I quaderni di

Agenda Digitale.eu

Maggio-agosto 2019

n. 0002

Agendadigitale.eu è una testata scientifica e giornalistica registrata al Tribunale di Milano

Dati di riferimento

Iscrizione ROC n. 16446
ISSN 2421-4167
Numero registrazione 1927, Tribunale di Milano

Editore: Digital360

Focus e ambito:

La rivista scientifica, i Quaderni di Agendadigitale.eu, pubblica fascicoli quadrimestrali in open access.

Lo scopo è creare un luogo per accompagnare i passi dell'Italia verso la necessaria rivoluzione digitale, con approfondimenti multidisciplinari a firma di esperti delle materie afferenti all'Agenda Digitale italiana ed europea

Submission e norme editoriali

Per effettuare una submission è necessario concordare prima un argomento e le misure precise contattando info@agendadigitale.eu.

Inviare un abstract di circa 500 caratteri alla testata, presentando l'articolo.

Le misure del testo finale saranno comprese tra 6mila e 20mila caratteri, salvo accordi per misure superiori.

I riferimenti bibliografici dovranno essere preparati in conformità alle regole dell'APA style, 6a edizione (si vedano le linee guida e il tutorial).

Gli autori sono invitati a tener conto degli articoli già pubblicati nella rivista e di citarli nel loro contributo qualora siano ritenuti di interesse per il tema trattato.

Comitato Scientifico e editoriale

Comitato scientifico

Presidente: Alessandro Perego**,** Politecnico di Milano

Membri del Comitato scientifico

Ottavio Di Cillo, università di Bari

Elena Valentini, Università Sapienza di Roma

Maurizio Ferraris, università di Torino

Paolo Ferri, Università Bicocca di Milano

Pietro Fiore, Università di Foggia

Stefania Fragapane, Università degli Studi di Enna Kore

Alfonso Fuggetta, Politecnico di Milano

Carlo Giovannella, Università Tor Vergata di Roma

Mariella Guercio, Università Sapienza di Roma

Mauro Lombardi, Università di Firenze

Mario Longo, Università del Salento

Roberto Maragliano, Università Roma Tre

Massimo Marchiori, Università di Padova

Berta Martini, Università di Urbino Carlo Bo

Carlo Medaglia, Università Unilink di Roma

Tommaso Minerva, Università degli studi di Modena e Reggio Emilia

Mario Morcellini, Università degli Studi di Roma "La Sapienza"

Giuliano Noci, Politecnico di Milano

Fabrizio Onida, Università Bocconi di Milano

Mario Pireddu, Università degli Studi della Tuscia

Franco Pizzetti, Università di Torino

Antonio Rafele, Università di Parigi (CEAQ- Université Paris Descartes La Sorbonne)

Francesco Sacco, Università Bocconi di Milano

Donatella Sciuto, Politecnico di Milano

Nicola Strizzolo, Università di Udine

Comitato di referaggio

Coordinatore: Luca Gastaldi, Polimi

Mauro Andreolini, sicurezza informatica, Unimore

Luca Baccaro, concorrenza, diritto comunicazioni elettroniche e dei media; studio legale Lipani Catricalà & Partner

Raffaello Balocco, IT e innovazione, Politecnico di Milano

Francesco Capparelli, privacy, cyber security, ecommerce, data management, identità digitale; studio legale ICT Legal Consulting

Ida Cortoni, media education e digital literacy; Dipartimento di Comunicazione e Ricerca Sociale, Sapienza Università di Roma

Giuseppe D'Acquisto, Autorità garante privacy, sicurezza e privacy

Daniela Di Donato, Docente di lettere, Dottoranda di ricerca presso Sapienza Università di Roma-Dipartimento di Psicologia dei processi di sviluppo e socializzazione, Collaboratrice del Crespi

Francesco Di Giorgi, diritto dell'informazione e della comunicazione, tutela dei consumatori, diritto delle comunicazioni elettroniche; Agcom

Leonella Di Mauro, data management, e-commerce, tutela del consumatore, diritto delle comunicazioni elettroniche; Agcom)

Gabriele Ferri, comunicazione e digitale, università Milano Bicocca

Luca Gastaldi: eGov, sanità, telecomunicazioni, procurement pubblico, design thinking, Smart Working, Politecnico di Milano

Maurizio Gentile, professore associato, Università di Roma LUMSA

Antonio Ghezzi: strategia, business model, startups, mobile, Politecnico di Milano

Nicola La Sala, registro degli operatori della comunicazione, fattura elettronica, industria4.0, editoria, cittadinanza digitale; Agcom

Emanuele Lettieri, sanità Politecnico di Milano

Maria Beatrice Ligorio, psicologia, università di Bari

Marika Macchi, economia, Unifi

Riccardo Mangiaracina: fatturazione elettronica, eCommerce, logistica e trasporti, export, Politecnico di Milano

Mirco Marchetti, Sicurezza informatica, unimore

Chiara Marzocchi, economia, Università di Manchester

Cristina Masella, Sanità, Politecnico di Milano

Davide Mula, sanità digitale, cyber security, privacy; Agcom

Simone Mulargia, internet and social media studies; Lumsa

Francesco Paoletti, docente di organizzazione aziendale e gestione delle risorse umane, Università degli Studi di Milano-Bicocca

Franco Pizzetti, diritto, privacy, università di Torino

Barbara Quacquarelli, scienze umane e formazione, università Milano Bicocca

Filippo Renga: turismo digitale, smart agrifood, finance and banking, mobile, Politecnico di Milano

Angelo Rovatti, tutela del diritto d'autore, diritti connessi, Diritto dei media; Agcom

Christian Ruggiero, sociologia del giornalismo e comunicazione politica; Dipartimento di Comunicazione e Ricerca Sociale, Sapienza Università di Roma

Franco Torcellan, Laboratorio RED del CISRE – Centro Internazionale di Studi sulla Ricerca Educativa Università Ca' Foscari Venezia

Angela Tumino: Internet of Things, logistica e trasporti, smart city, Politecnico di Milano

Simone Vannuccini, economia, SPRU

Indice del fascicolo

Giornalismo a tutela del dibattito democratico, ecco il nuovo ruolo

In un'epoca di ricerca del consenso e di bolle polarizzate, il giornalismo deve ripensare sé stesso e mettere al centro quello che può essere l'antidoto all'omogeneità e alle manipolazioni: il dissenso, la messa in discussione di idee e posizioni. Puntando alla conquista del "cittadino informato quanto basta". Vediamo come

Di **Bruno Mastroianni**, Dipartimento di Lettere e Filosofia dell'Università di Firenze

Vi presento il ***cittadino informato quanto basta***. Un interlocutore che con la rivoluzione digitale sta prendendo sempre più spazio e importanza nello scenario della comunicazione.

Il cittadino, cioè, che **partecipa al dibattito fino a un certo punto**, legge quello che gli capita sui suoi spazi online senza avere un vero metodo per la fruizione delle notizie, **agisce in rete senza avere numeri rilevanti** e senza essere un commentatore compulsivo. Ma che con i suoi like, le sue condivisioni, i suoi link inviati tramite le app di messaggistica **ha di fatto il potere di influenzare le sue cerchie ristrette**, quelle in cui ha più peso proprio perché basate su relazioni di vicinanza e affinità con i suoi contatti.

È sul cittadino informato quanto basta (d'ora in poi CIQB) che, nell'era dello strapotere degli algoritmi e della disinformazione, il **giornalismo** deve riuscire a fare presa, curando e offrendo **assieme all'informazione di qualità, anche occasioni di discussione produttive, pure a partire da un moto di dissenso**.

Occorre però un ripensamento e un riadattamento della funzione e del ruolo dei giornalisti, che **dovrebbero essere i primi ad adottare uno stile di comunicazione che inviti al pensiero critico e alla messa alla prova di ciò che si legge. Ci sta provando, ad esempio, il Wall Street Journal.**

Proviamo a capire perché è importante e quale sforzo è necessario oggi per informare correttamente.

Le nuove forme di propaganda e manipolazione

In un interessante articolo di ValigiaBlu.it sulle scorse elezioni in Brasile, Fabio Chiusi ha fatto un'analisi dei principali studi che si sono occupati delle strategie di disinformazione e manipolazione durante la campagna elettorale. Uno degli aspetti sottolineati è **l'impegno per far arrivare i messaggi proprio nelle chat di WhatsApp**, cioè in quegli spazi dove il CIQB scambia i suoi messaggi con le persone che gli sono vicine: segno che anche le modalità di propaganda e

manipolazione diventano sempre più raffinate nel cercare di arrivare fin dentro i luoghi di prossimità del cittadino medio.

Anche sulle piattaforme dei social network l'azione del CIQB si fa sentire e ha una certa efficacia: il funzionamento degli algoritmi, infatti, valorizza la segnalazione di contenuti a ciascuno in base alle interazioni degli altri con i quali è collegato, tanto che la maggior parte dei contenuti arriva nelle timeline proprio perché qualcuno vicino sta commentando, condividendo, dando attenzione a qualcosa.

Già nel 1994 **Mauro Wolf**, nel suo saggio pubblicato postumo, *Le discrete influenze* (Wolf, 1996), faceva un parallelo tra lo spazio pubblico mediatizzato e il concetto di sviluppo compatibile: **si chiedeva se l'espansione, la diffusione e l'evoluzione delle tecnologie di comunicazione sarebbero riuscite a procedere con il loro ritmo senza compromettere e distruggere l'ambiente sociale**. È una domanda ancora più attuale oggi, a venticinque anni di distanza, considerando proprio quanto **la disintermediazione e l'iperconnessione stiano riconfigurando drasticamente l'intero sistema sociale**, entrando nella vita di ciascuno e modificando il rapporto tra comunicazione, informazione e conoscenza: un cambiamento al cui centro c'è proprio il cittadino con i suoi atti di comunicazione online che incidono su di sé e chi gli sta intorno.

Sovraccarico di valutazioni e di discussioni

Proprio da questo occorre partire, considerando quanto la questione sia più relazionale e sociale che non puramente informativa. Siamo portati, infatti, a osservare il CIQB soprattutto dal punto di vista del *sovraccarico informativo* (*information overload*) in cui è inserito, che lo porta a una situazione di caos e di disordine (*information disorder*) in cui matura la disinformazione. Così tralasciamo, però, altre **dimensioni più relazionali del sovraccarico che non solo sono rilevanti, ma che sono di fatto le vere catalizzatrici del primo e dei suoi effetti più preoccupanti.**

Come scrivevamo qualche tempo fa su Agendadigitale.eu il CIQB è diventato, grazie all'*onlife* (Floridi, 2017), cioè alla vita connessa, **un piccolo personaggio pubblico**, che fa continuamente atti di comunicazione pubblica, ha una sua immagine pubblica ed è sottoposto a un continuo giudizio da parte di un pubblico, più o meno esteso, che lo segue. Questo porta a un ***sovraccarico valutativo***, cioè alla possibilità di essere visto, letto, raggiunto e quindi giudicato da altri costantemente. Proprio da questa situazione di esposizione pubblica continua deriva un ulteriore sovraccarico: quello di discussioni e confronti in cui si viene coinvolti. La condizione di discussione perenne diventa così un portato della connessione che, ampliando le possibilità e la facilità con cui le parole e i contenuti possono raggiungere chiunque in ogni momento, ha anche creato le condizioni per le quali **il continuo scambio diventa difficilmente sostenibile e fruibile.**

Il CIQB, insomma, non è semplicemente preda passiva di un *sovraccarico di informazioni* in cui viene raggiunto da contenuti più o meno attendibili e verificati, ma **attore che allo stesso tempo subisce ed è protagonista della dinamica,** impegnato com'è a difendere se stesso, le sue convinzioni, il suo buon nome in un *sovraccarico di valutazioni* che affronta in una continua forma di lotta in cui scambia parole e informazioni con altri, immerso in un *sovraccarico di discussioni* che contribuiscono a loro volta a aumentare disinformazione e manipolazioni.

Differenze inconciliabili e rifugio tra gli affini

A guardar bene, insomma, **il sovraccarico più importante dei tre citati è proprio l'ultimo, cioè quello delle discussioni**, perché è come se fosse la condizione in cui si sviluppano gli altri due: **è**

l'effetto dell'interconnessione che ha ridotto le distanze e ha aumentato le possibilità di comunicazione facendo sì che le differenze si incontrino molto più frequentemente finendo spesso in scontri privi di reali vantaggi (Mastroianni, 2017). Tale sovraccarico di incontri tra differenze non porta automaticamente gli effetti benefici che ci si aspetterebbe dal continuo confronto fra posizioni, ma genera spesso l'opposto: **il rifugio e la chiusura in cerchie omogenee e affini** (Quattrociocchi, Vicini, 2016) in cui trovare conferma delle proprie idee e tenere alla larga il dissenso.

Non è un caso che **il dibattito pubblico abbia un modo di procedere che predilige contrapposizioni e polarizzazioni.** Le formulazioni binarie inconciliabili (Cosenza, 2018) – pro/contro, con me/contro di me, vero/falso, giusto/sbagliato, degno/indegno – diventano la retorica prediletta nella comunicazione a tutti i livelli, dal discorso politico allo stile di diverse testate giornalistiche, fino ad arrivare alla comunicazione di certi brand che tendono a sfruttare la polarizzazione entrando in campo e prendendo posizioni forti su temi sociali, politici, culturali. **Fomentare la polarizzazione e lo scontro diventa così uno dei metodi più a buon mercato (e di fatto efficaci) per ottenere il consenso di chi è costantemente in preda alla lotta per la difesa di se stesso e delle sue convinzioni**: la "presa di posizione" diventa modo per chiamare a raccolta i cittadini che si identificano in quegli schieramenti.

Il dibattito ridotto

Quella della contrapposizione diventa una vera e propria forma di riduzione del dibattito pubblico. **Piero Dominici** fa una differenza fondamentale tra *semplificazione* e *riduzionismo*: la **semplificazione** è la capacità di saper evidenziare percorsi di significato sostenibili che non perdano il collegamento con la complessità in cui sono inseriti; **riduzionismo** significa invece scegliere di vedere un fenomeno riconducendolo a un solo elemento e considerando solo in alcune delle sue parti disgiungendole dall'insieme delle relazioni in cui sono inserite. **La semplificazione è necessaria e costruttiva** in una situazione di sovraccarico; **il riduzionismo, invece, è distruttivo**: pur attenuando il disagio per l'*overload*, fa perdere pezzi di realtà.

Il ruolo del giornalismo nell'era dell'autocomunicazione di massa

A questo punto, una delle domande fondamentali che deve porsi oggi chi ha il compito di informare in modo attendibile è **come inserirsi nel sovraccarico di discussioni in cui il CIQB non è solo una preda, ma un attore e protagonista che le fomenta e le alimenta**. Il diverso ruolo del CIQB, insomma, **richiama a pensare a un diverso ruolo anche del giornalismo**; a meno che il giornalismo non voglia ridursi anch'esso a cavalcare la polarizzazione assumendo posizioni in contrasto per chiamare a raccolta il consenso di chi già le condivide.

Nello scenario precedente, quello delle comunicazioni di massa, **il compito dei giornalisti era principalmente semplificare** (selezione e verifica delle informazioni nel sovraccarico) per permettere ai cittadini di essere più consapevoli e quindi il più possibile liberi, pur nei limiti delle loro possibilità. È stato da sempre questo il ruolo del *watchdog*, il cane da guardia della democrazia.

Oggi, nell'epoca della *autocomunicazione di massa* (Castells, 2009), in cui il sovraccarico è la dimensione in cui il cittadino vive e a cui contribuisce tra giudizi e discussioni con gli altri, **la stessa modalità è insufficiente**. **La selezione, infatti, viene prodotta dalla dinamica dell'engagement e degli algoritmi che premiano la circolazione dei contenuti tra affini, e la**

verifica (o meglio la non verifica) avviene da parte di ogni utente che si fa una sua propria idea di verità del mondo da se stesso (Fabris, 2017), spesso ridotta a contrasto tra le sue convinzioni e quelle di qualcun altro, aggravando la tendenza a **chiudersi in bolle di opinioni omogenee** all'interno delle quale trincerarsi.

In questo scenario, insomma, **il compito del giornalista, oltre a quello della semplificazione (che rimane sfida attuale e intatta)** deve assumere anche qualche connotazione in più, **se vuole mantenere la sua capacità di rendere i cittadini più liberi e consapevoli.**

È un compito che non può prescindere dalla dinamica delle discussioni continue.

Informare correttamente oggi non è più soltanto curare la qualità delle notizie, la loro tempestività, la confezione del contenuto, la diffusione, ma diventa anche e soprattutto una certa modalità di intercettare il CIQB proprio nella conversazione e nella discussione in cui è impegnato a proposito di quelle notizie e informazioni.

Il giornalismo, oggi, e più in generale la divulgazione del sapere, non possono prescindere dalla disintermediazione e dalla dimensione conversazionale dell'informazione; il che vuol dire avere la **capacità di entrare, partecipare, contribuire a quelle conversazioni** per produrre in esse e trarre da esse i benefici che derivano da una buona e sana informazione.

Gli audience voice reporters

È significativo ciò che ha annunciato recentemente il Wall Street Journal a proposito di una serie di cambiamenti che attuerà nella sua strategia di risposta e gestione dei commenti dei lettori. In base a una ricerca sulle interazioni più frequenti nei commenti agli articoli, **il quotidiano internazionale ha deciso di passare dalla semplice moderazione all'impegno per far emergere attivamente e valorizzare la voce dei lettori.**

La situazione che ha registrato nei suoi spazi è la presenza di commentatori assidui (un piccolo numero ma molto attivo) e commentatori meno frequenti. Gli appartenenti al primo gruppo **hanno mostrato di avere la tendenza a non leggere fino in fondo gli articoli e a essere più interessati a esprimere le proprie posizioni che a ingaggiare discussioni**. Dall'altra, è stato rilevato che i commentatori meno assidui tendono a essere più sensibili in caso di lettura da parte dei giornalisti: diversi di loro hanno detto di commentare poco proprio per la sensazione di non essere presi sufficientemente in considerazione.

Dall'analisi è risultato anche che il gruppo dei commentatori più frequenti fosse poco rappresentativo dei lettori del giornale rispetto al gruppo dei commentatori sporadici. Insomma, il quotidiano ha deciso di puntare sul secondo gruppo, quello che non solo mostra di ricercare una conversazione che sia veramente tale, ma che soprattutto **costituisce il pubblico più ampio**, più diversificato e anche più interessante per la crescita del giornale.

Come? Fondamentalmente seguendo tre criteri.

Il primo è quello della ***sostenibilità*:** per seguire bene le conversazioni ci vogliono energie, persone e tempo, pertanto il giornale ha deciso di predisporre la possibilità di attivare la discussione solo su alcuni contenuti per poterla curare al meglio.

Il secondo criterio è quello dell'***ascolto attivo***: in quegli spazi i lettori saranno incoraggiati a intervenire e saranno presi in considerazione da veri e propri "audience voice reporters", che non sono più solo dei moderatori, ma giornalisti con il compito di raccogliere e valorizzare gli spunti che provengono dalla conversazione dei lettori.

Il terzo criterio è quello del ***clima di sicurezza e di qualità della conversazione***: questi spazi saranno al sicuro da insulti, discorsi di odio e aggressioni verbali inutili, in modo che ciascuno possa intervenire liberamente con le sue opinioni senza temere di essere assalito da polemiche sterili.

Un'alternativa al sovraccarico di discussioni

È un esempio molto significativo che va in una direzione interessante e duplice: curare attivamente la qualità della conversazione e mettere i lettori nelle condizioni di esprimere la loro opinione ed essere ascoltati. In altre parole, si tratta di m**ettersi in una modalità relazionale e conversazionale offrendo un'alternativa alla vita sovraccarica di discussioni** che il lettore vive, incoraggiando chi desidera discutere in modo produttivo e non degenerato.

Si vedrà quali frutti porterà questa azione del WSJ, che per adesso ci dice qualcosa sulle strade che si potrebbero percorrere per **un giornalismo che, assieme all'informazione di qualità, curi e offra occasioni di discussione produttive**. Tra l'altro, la categoria di lettori che commentano raramente individuata nel quotidiano assomiglia proprio a quella del CIQB, che *interagisce quanto basta*, e che in effetti può e deve diventare sempre di più il centro delle attenzioni dell'attività giornalistica.

Gli spazi social abbandonati a sé stessi

Certo è che se si passa dagli spazi online controllabili dalle testate a quegli spazi senza un vero controllo che sono le piattaforme dei social network, il discorso si fa più complicato, ma questo non toglie che la strada intrapresa dal WSJ non possa essere di ispirazione, a cominciare magari proprio da quei criteri di sostenibilità, ascolto attivo e cura del clima della conversazione che il giornale newyorkese sta applicando.

Come ha fatto notare Pierluca Santoro, **le maggiori testate italiane si limitano a usare gli spazi social come "discariche" di link, con scarsissima interazione e cura della relazione con i lettori, tanto che alla fine la maggioranza dei commenti è di tipo negativo e aggressivo**, di fatto favorendo un clima che tiene lontano chiunque abbia voglia di discussioni costruttive o perlomeno civili.

Un primo ambito di azione insomma potrebbe essere individuato proprio in quei luoghi dove il campo lasciato al commento casuale non fa che alimentare le dinamiche di sfiducia e scoraggiare la partecipazione di chi, invece, rappresenta la parte più interessante dei lettori a cui rivolgersi. **E qui sorge il tema della sostenibilità**: quante energie e risorse è disposta una testata a impiegare per mettere in campo social media manager in grado di svolgere un lavoro simile a quello degli "audience voice reporters" del WSJ?

Mettersi alla prova davanti al lettore e valorizzare il dissenso

In altre parole, di fronte alla continua contrapposizione, cioè la formazione di schieramenti avversi intenti ad accaparrarsi il consenso dei lettori invitandoli a identificarsi in uno dei lati della polarizzazione, **esiste la possibilità di un giornalismo di contraddizione, capace di mettere alla prova quelle posizioni, quali che siano, e quindi di invitare a discuterle, valorizzando e incoraggiando il lettore a fare altrettanto** (di fatto è una strada che diversi stanno percorrendo, e con risultati rilevanti, per fare solo un esempio citato in questo articolo: ValigiaBlu).

Un giornalismo, insomma, che come *watchdog* della democrazia, in un'epoca di ricerca del consenso e di bolle omogenee polarizzate, metta al centro quello che può essere **l'antidoto all'omogeneità e alle manipolazioni: il dissenso, la contraddizione, la messa in discussione delle idee e delle posizioni.**

Ma come si fa a **valorizzare il dissenso** in un mondo in cui l'intera dinamica porta a resistere ed evitare le differenze? Vengono in aiuto gli altri due criteri applicati nella strategia del WSJ: l'ascolto attivo e la cura del clima della discussione.

La strada che si può davvero percorrere è quella di iniziare con il dare il buon esempio: dovrebbero essere i giornalisti stessi i primi ad adottare uno stile di comunicazione che inviti al pensiero critico e alla messa alla prova di ciò che si legge.

Intanto in ciò che scrivono: indicando il più possibile le fonti, esplicitando ciò che proviene dalle proprie opinioni e ciò che invece è frutto di fatti o di evidenze oggettive, arrivando magari anche ad ammettere di non avere sufficienti elementi per poter dire qualcosa di definitivo. Un giornalismo molto più di domande e dubbi che di certezze e tesi, un giornalismo che spiega il suo metodo mentre lo applica, mostrando il percorso che compie mentre divulga e informa. **Un giornalismo che si mette alla prova di fronte al lettore e lo invita a fare altrettanto.**

Il dissenso come antidoto alle manipolazioni

Tutto ciò va costruito favorendo che il dissenso possa emergere e mettere alla prova i contenuti giornalistici, ricevendo in cambio ascolto e risposta. Questa sarebbe la vera cura delle discussioni online: non solo evitare di fomentare contrapposizioni scomposte (che dovrebbe essere il minimo), ma valorizzare attivamente e prendere in considerazione le parti produttive e significative del dissenso.

Sopire le contrapposizioni sterili non vuol dire togliere la parola al pubblico, al contrario: come nella strategia messa in atto dal WSJ significa dare più voce e valorizzare chi davvero vuole esprimere il suo punto di vista, anche quando critico. Se ci si pensa bene, si tratta di mettere al centro il valore del dissenso, del pluralismo e della diversità, opponendolo al consenso facile, alla riduzione a una posizione contro l'altra, che deriva dalla contrapposizione polarizzata. È un lavoro in direzione di un dibattito che non perde i suoi legami con la complessità.

E qui occorre ancora una volta rimettere al centro il nostro interlocutore prevalente, cioè **il CIQB, considerando che, proprio per le sue caratteristiche intrinseche, non sarà sempre in grado di esprimere il suo dissenso in modo elegante e composto.** Anzi, c'è da aspettarsi che, proprio perché pressato dal sovraccarico di valutazioni e discussioni, il modo di presentare il suo punto di vista avrà elementi aggressivi e poco funzionali alla discussione.

Pretendere che il nostro cittadino sia in grado da solo di sostenere, promuovere o condurre dibattiti costruttivi, sarebbe a dir poco ingenuo. È qui che ancora una volta l'azione di chi informa dovrebbe

supplire riuscendo a trarre da una selva di parole inadatte pensieri che hanno senso, riconoscendo le istanze e ignorando le parti polemiche.

Un'azione di ascolto attivo (Sclavi, 2003) che andrebbe fatta sempre: **il dissenso, infatti, ha un valore anche quando non espresso con tutti i crismi**, perché intervenire a raccogliere domande e argomenti validi anche quando sono affogati in mezzo a espressioni aggressive può dare occasione di fornire risposte che si rivolgono alla moltitudine silenziosa di cittadini informati quanto basta disposti a ragionare e a confrontarsi (Gheno, Mastroianni, 2018).

Nella dinamica dei social network è infatti più difficile avere un controllo a monte dei flussi di interazione, ma si può fare molto a valle, di fronte alle diverse tipologie di commenti degli utenti. **Si tratta di compiere un lavoro di scelta e di valutazione intelligente delle istanze a cui dare seguito e di quelle da ignorare e da lasciar cadere.** È un'attività faticosa e dispendiosa, che però può contribuire a costruire il clima della conversazione, proprio come il passaggio dalla semplice moderazione all'ascolto della voce dei lettori.

Non è tutto odio ciò che polemizza

Facciamo un esempio concreto per capire di cosa potrebbe trattarsi. Mi è capitato, di fronte all'ennesimo delitto di cui si è macchiato un migrante che ha confessato la sua colpevolezza, di imbattermi in due commenti a proposito della notizia sul caso:

Commento A: "Rispediamoli tutti a casa!"

Commento B: "Ha confessato: perché dovremmo spendere i soldi per fargli anche il processo? Dovrebbero mettergli il cemento ai piedi e buttarlo a mare!"

Apparentemente, i due commenti si somigliano in quanto ad aggressività e violenza. In realtà, a una valutazione più attenta, che sappia mettere al centro il valore del dissenso e della discussione, il commento A è diverso da B: il primo non ha alcun elemento di interesse, si tratta di pura espressione d'odio fine a se stesso; il secondo invece, in mezzo a una serie di formulazioni scomposte, contiene una questione fondamentale, quella del **perché nelle nostre democrazie facciamo processi anche a chi confessa un crimine.**

Una risposta al commento B, se data con le opportune modalità, potrebbe essere l'occasione per parlare non tanto al commentatore (che probabilmente rimarrebbe nella sua posizione polarizzata) **quanto a quell'insieme di lettori silenziosi che da quell'intervento non solo sarebbero portati a riflettere sull'importanza del tema,** ma potrebbero avere anche la sensazione che quello spazio non è lasciato a se stesso e in preda alle parole in libertà di chiunque.

La custodia del dibattito nella disintermediazione

Si tratta insomma di quella strada intrapresa da un certo giornalismo che dimostra costantemente di accettare conflitti e contraddizioni occupandosene invece che solleticare le contrapposizioni tanto per ottenerne benefici in termini di consenso. Un giornalismo che coltiva l'alleanza con il CIQB e che lo incoraggia a fare un passo in più di riflessione e discussione, mentre scoraggia chi, più rumoroso, alimenta solo scontri e litigi privi di vera utilità per una migliore informazione.

A ben vedere, è proprio **quel ruolo di garante e custode di un dibattito vero e plurale** che ormai non può essere più solo giocato negli spazi mediatici classici, anche se connessi in rete, ma che deve entrare in qualche modo nelle pieghe della vita interconnessa del CIQB tanto quanto stanno tentando di entrarvi le azioni della propaganda a caccia di consenso.

Una strada, insomma, per rispondere a quelle azioni di manipolazione che stanno puntando sempre più alla dimensione delle micro-interazioni online, sia sui social network che negli spazi ancora meno aperti della messaggistica privata dove, se non è lo stesso cittadino a fare qualcosa, maturando egli stesso degli anticorpi alla propaganda polarizzata, difficilmente basterà adottare contromisure generalizzate.

BIBLIOGRAFIA

Manuel Castells, *Comunicazione e potere*, Università Bocconi Editore, Milano, 2009.

Giovanna Cosenza, *Semiotica e comunicazione politica*, Laterza, Roma-Bari, 2018.

Piero Dominici, *For an inclusive innovation. Healing the fracture between the human and the technological in the hypercomplex society*, "European Journal of Futures Research" (2018) 6:3.

Maurizio Ferraris, *Postverità e altri enigmi*, ilMulino, Bologna, 2017.

Luciano Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017.

Vera Gheno, Bruno Mastroianni, *Tienilo acceso. Posta, commenta, condividi senza spegnere il cervello*, Longanesi, 2018.

Walter Quattrociocchi, Antonella Vicini, *Misinformation. Guida alla società dell'informazione e della credulità*, FrancoAngeli, Milano, 2016.

Bruno Mastroianni, *La disputa felice. Dissentire senza litigare sui social network, sui media e in pubblico*, Cesati, 2017.

Marinella Sclavi, *Arte di ascoltare e mondi possibili. Come si esce dalle cornici di cui siamo parte*, Bruno Mondadori, Milano, 2003.

Mauro Wolf, *Le discrete influenze*, in "Problemi dell'informazione", n.4 dicembre 1996.

Scuola, quali competenze per costruire il mondo che vogliamo

Di fronte alla diffusione del digitale e alle radicali innovazioni della produzione, la sfida per i sistemi educativi si pone nei termini dell'eguaglianza delle opportunità e si traduce nella promozione di competenze adeguate per il cittadino e il lavoratore del futuro. Ecco perché le scelte prese oggi sono fondamentali

Di **Annalisa Buffardi**, Ricercatrice, Indire - Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa

A fronte delle nuove opportunità offerte dalle tecnologie digitali, i**l ruolo della scuola** non deve essere soltanto quello di accompagnare i giovani a comprendere il funzionamento delle macchine e dei nuovi sistemi: la scelta che le istituzioni pubbliche devono compiere oggi, come sempre, è quella d**i accompagnare i giovani a comprendere e a potenziare le proprie capacità ideative e realizzative, a immaginare il futuro "intelligente" e "sostenibile",** ad abilitare il cambiamento reso possibile dalle tecnologie digitali.

Una mission, quella della **istituzioni educative, a tutti i livelli,** costellata da sfide importanti e impegnative, ma il cui obiettivo, fondamentale, è quello di **fornire le lenti per una prospettiva che guardi al futuro e favorire la pluralità degli sguardi.**

Superare la paura delle tecnologie per coglierne i vantaggi

Oltre dieci anni fa, nel discutere della prima generazione di nativi digitali, John Gorham Palfrey e Urs Gasser (2008) evidenziavano **il valore delle scelte pubbliche nell'orientare le modalità prevalenti di uso del web**, e quindi il modo in cui i "nostri figli e nipoti vivranno la loro vita".

La **paura,** scrivevano gli studiosi, è **il vero grande ostacolo che può limitare il potenziale delle tecnologie**, riducendone la visione delle opportunità a vantaggio dei rischi. Il dibattito sulla diffusione dei nuovi mezzi ha visto nella sua prima fase, e ripropone ancora oggi, visioni apocalittiche opposte a scenari integrati, ma è sempre più chiaro che le "disposizioni" di istituzioni quali scuola, famiglia, mercato e stato guidano il modo in cui le tecnologie sono e saranno utilizzate, e, come scriveva anche Sonia Livingstone nel 2009, "in effetti sono proprio queste a far si che, per esempio, gli insegnanti scelgano di rimpiazzare la stampa con tecnologia informatica".

Le tecnologie digitali offrono nuove opportunità, sul fronte della diffusione delle informazioni, dell'apertura delle conoscenze, della partecipazione. La diffusione dei nuovi mezzi di produzione digitali sembra inoltre orientare verso ciò che Gershenfled (1999) ha definito "democratizzazione dei processi di produzione". Tuttavia, la diffusa partecipazione è funzione delle possibilità di scelta individuali. **Il ruolo delle istituzioni formative e in primis della scuola pubblica è centrale nell'accompagnare le giovani generazioni a comprendere non solo e non tanto il funzionamento tecnico delle nuove macchine e dei nuovi sistemi digitali.**

Immaginare il futuro: visioni per il mondo che vogliamo

La trasformazione culturale e tecnologica orienta verso **una dinamica economica e produttiva** che mette in primo piano **il valore delle idee, le competenze digitali, la contaminazione di ambiti,** settori, professionalità, lo spirito di iniziativa e **la capacità di cogliere le diverse opportunità** offerte dalle più immediate possibilità di produzione e di realizzazione. Cambiamenti che coinvolgono con forza il mondo della formazione, ai diversi livelli di istruzione, sul versante organizzativo e metodologico-didattico. La digitalizzazione dei processi economici accompagna e nutre **una visione imprenditiva che restituisce ai giovani la promessa di poter trasformare le proprie idee in progetti.**

Al centro di tale promessa risiede un nucleo di abilità, definibili nell'area dell'imprenditorialità e delle competenze digitali e che comprendono alcune tra le cosiddette **soft skill**. Tale promessa si fonda, dunque, innanzitutto, sulla **capacità delle istituzioni formative di promuovere e formare un nucleo di competenze** - imprenditoriali, digitali, soft skills - **necessarie per l'innovazione** e per gestire le sfide che il cambiamento porta con sé, rinnovando il proprio modello didattico a partire dalla cultura di rete, ormai diffusa a livello culturale e sociale. Dai modelli di "apertura" che la caratterizzano al pensiero creativo connettivo che può tradursi in pratiche innovative.

Networking e making rappresentano due aspetti, resi possibili dalla diffusione dei nuovi mezzi, che caratterizzano la cultura contemporanea, che mettono in scena un diffuso orientamento a logiche di rete, all'ideare, al progettare, al fare, in una dimensione di connessione tra individui, oggetti, tecnologie (Buffardi, Savonardo 2019).

Il più facile accesso alle conoscenze, ai dati e alle tecnologie di fabbricazione digitale apre scenari in cui la logica del pensiero connettivo (de Kerckhove 1997) si traduce nel "fare creativo connettivo".

Innovazione e nuova imprenditorialità

Le dinamiche di trasformazione in atto richiamano, anche nelle agende politiche europee e mondiali, la spinta ad **incoraggiare le innovazioni nella direzione della «crescita intelligente basata sulla conoscenza e della sostenibilità»** e per il rilancio economico e produttivo, come si legge nella Strategia Europea 2020 o nell'**Agenda 2030 per lo sviluppo sostenibile**.

Il tema dell'imprenditorialità si colloca efficacemente in questa cornice e lascia intravedere scenari in cui sia potenzialmente possibile ideare, progettare e realizzare prodotti e servizi in grado di rispondere a nuovi bisogni emergenti.

La spinta all'innovazione incontra nuove definizioni che non restano confinate in un singolo ambito ma attraversano l'area sociale, culturale, economica, imprenditoriale. E il caso, ad esempio, della **green economy** che, sulla scia della cultura ecologica e trainata da nuove scoperte scientifiche e tecnologiche, coinvolge settori tradizionali come l'agricoltura. Analogamente, il concetto di "**qualità della vita**", affermatosi tra gli anni Sessanta e Settanta in relazione alla consapevolezza che il benessere e lo sviluppo sociale non potevano essere il risultato tout court della crescita economica, sembra oggi trovare una declinazione operativa, ad esempio nei nuovi modelli collegati al concetto di **smart city**. Nel riconoscere la necessità di un adeguamento alle esigenze dell'uomo e alla cultura del benessere le stesse tecnologie divengono "smart technologies".

Una transizione che si colloca e si riflette in opportunità e spinte per **una nuova imprenditoria in cui creatività, tecnologia, conoscenza e ricerca risultano profondamente intrecciate.** A partire dalla diffusione del web 2.0, degli user generated content e del digital making, la cultura della partecipazione apre scenari che rendono possibile non solo esprimere opinioni, posizioni favorevoli o contrarie, o promuovere mobilitazioni di consenso-dissenso pubblico. La progressiva diffusione delle tecnologie per la produzione, dentro questa cornice culturale, amplia le possibilità di partecipazione alla possibilità effettiva di dare forma alle idee e di modellare le cose (Gershenfeld 1999), di creare con gli altri.

La nuova disponibilità di accesso all'informazione, ai dati, alla ricerca scientifica, alle tecniche e alle tecnologie di produzione promette una più diffusa partecipazione alla definizione delle vie del cambiamento, uno scenario in cui potenzialmente il più facile accesso a strumenti e conoscenze sembra ampliare le possibilità di contribuire alle scelte, di pensare e progettare soluzioni, prodotti, servizi per rispondere alle mutate esigenze contemporanee.

Divari culturali e digitali

Un tema che richiama, insieme a nuove opportunità, anche **nuovi divari** tra chi è capace di partecipare alla visione del cambiamento e chi ne è escluso, e che coinvolge il ruolo del sistema educativo nello sviluppo delle competenze necessarie per partecipare alle sfide della società contemporanea.

La sempre più diffusa disponibilità di tecnologie per la fabbricazione, associata alle caratteristiche di networking che definisce l'ambiente digitale, nel **combinare il valore connettivo della rete con le radicali innovazioni della produzione, valorizza la partecipazione, la creatività, l'imprenditività negli scenari di sviluppo sociale, culturale ed economico-produttivi**. Elementi che rappresentano fattori significativi di attenzione per le politiche educative nel contesto della formazione dei «giovani che cambieranno il mondo» (Wagner 2013).

«**Capacitare l'entrepreneurship**» nei ragazzi, come rileva Andrea Strano (2015) richiamando l'approccio di Sen e Nussbaum vuol dire, nei contesti educativi e formativi, i**ndividuare le vie di un ampliamento degli spazi di libertà e di agency individuale,** per andare verso la promozione di processi di innovazione e al contempo verso un ampliamento delle possibilità individuali di ideazione e realizzazione di progetti professionali e di vita. «Non si tratta soltanto di qualificare con competenze tecniche i nostri studenti, bensì si tratta di avvicinare una cultura del lavoro capace di interpretare i nuovi paradigmi del lavoro e dell'innovazione all'interno di una dimensione educativa e formativa delle nostre scuole».

Capacitare entrepreneurship vuol dire formare nelle persone le competenze e le capacità generative per un ampliamento dei loro spazi di libertà, per un potenziamento della capacità di vedere il proprio futuro e di esprimere con scelte concrete la propria direzionalità realizzativa, sapendo cogliere tra le diverse opportunità del contesto quelle che si ritengono di valore per sé.

Capacitare entrepreneurship significa, dunque, **collocarsi strategicamente nei segmenti di connessione tra mondo della formazione e mondo del lavoro**, riqualificando percorsi di apprendimento attraverso la progettazione di architetture formative capaci di integrare diversi contesti e di rafforzare il dialogo tra Università, Imprese e Istituzioni, definendo così nuovi modelli pedagogici basati su azioni multidisciplinari, competenti e generativi.

Uno scenario in cui "The world we want" (Kingwell, 2001), il mondo che vogliamo "creare" è tendenzialmente aperto alle possibilità creative e partecipative. Di chiunque abbia accesso consapevole alle tecnologie e alla conoscenza. Di chi abbia l'opportunità di individuare scelte possibili per i propri percorsi di vita.

Su questi fronti, la principale sfida per i sistemi educativi si pone nei termini dell'eguaglianza delle opportunità e si traduce nella **promozione di competenze adeguate per il cittadino e il lavoratore del futuro.**

Parafrasando Palfrey e Gasser, «le scelte che stiamo facendo oggi condizioneranno il mondo che i nostri figli e nipoti potranno costruire». Laurent Alexandre (2017) discutendo gli sviluppi dell'**Intelligenza Artificiale** come motore dell'innovazione e la parallela necessità di «coltivare cervelli biologici» per evitare la loro sconfitta definitiva nella battaglia con le tecnologie, afferma che, in ogni caso, quegli sviluppi non verranno «da un laboratorio di una delle nostre vecchie e collaudate istituzioni. L'IA è nelle mani dei giovani che affermano con candore di voler rendere il mondo un posto migliore. Quanto meno ai loro occhi».

BIBLIOGRAFIA

Alexandre, L. 2017, *La guerre des intelligences. Comment l'Intelligence Artificielle va révolutionner l'éducation*, Jean Claude Lattès (trad. it. La guerra delle intelligenze. Intelligenza artificiale *contro* intelligenza umana, Torino, EDT, 2018).

Buffardi A., Savonardo L. 2019, *Culture digitali, innovazione e startup. Il modello Contamination Lab* Milano, Egea.

de Kerckhove, D. 1997, *Connected Intelligence. The Arrival of The Web Society*, Toronto, Sommerville.

Gershenfeld, N. 1999, *When Things start to Thin*k, New York, Henry Holt, (trad. it. *Quando le cose iniziano a pensare. Come gli oggetti intelligenti rivoluzieranno le nostre v*ite, Milano, Garzanti, 1999).

Kingwell, M. 2001, *The World We Want: Virtue, Vice, and the Good Citizen.* Canada, Penguin.

Livingstone, S. 2009. *Children and the Internet. Great Expectations, Challenging Realities*, Cambridge, Polity Press.

Palfrey J., Gasser, U. 2008, *Born Digital. Understanding the First Generation of Digital Natives*, New York, Basic Books.

Strano, A. 2015. «Capacitare entrepreneurship per l'attivazione professionale dei giovani», Formazione e Insegnamento. *Rivista Internazionale di Scienze dell'Educazione e della Formazione,* 13-1.

Wagner, T. 2013, *Creating Innovators: the Making of Young People Who Will Change the World*, NewYork, Scribner/Simon & Schuster.

Bambini troppo soli davanti agli smartphone: ecco che cosa può fare la scuola

Lo smartphone in sé non è uno strumento nocivo per bambini e ragazzi, ma è sbagliato lasciarli troppo soli davanti agli schermi. Per questo la scuola deve intervenire e fare da bussola, fornendo indicazioni e modelli diversi da quelli offerti dai genitori. Vediamo in che modo

Di **Daniela Di Donato**, Docente di lettere, Dottoranda di ricerca presso Sapienza Università di Roma-Dipartimento di Psicologia dei processi di sviluppo e socializzazione, Collaboratrice del Crespi

Spesso i bambini o i ragazzi sembrano molto soli davanti agli schermi dei loro smartphone. È questa solitudine a non essere sana, non l'uso dei dispositivi digitali in sé. Per questo è indispensabile che **la scuola si assuma la responsabilità e l'incarico di educare all'uso della rete e al suo non uso**, che dia bussole per scegliere, che faccia qualcosa di diverso da quello che possono e riescono a fare i genitori o l'ambiente familiare.

Questa mia riflessione parte da un episodio accaduto poco tempo fa.

Sono in treno e accanto a me si siede un bambino, che avrà quattro o cinque anni. Abbassa il tavolino e ci sistema uno smartphone acceso. **Si sintonizza su youtube e sceglie dei brevi video di tre/quattro minuti: sono cartoni animati di Barbie**. Non ne finisce uno: si interrompe più o meno a metà e passa al video successivo. Sa come cercare, conosce le principali funzioni per orientarsi nella lista dei materiali che il social gli propone (infatti salta alcuni video perché effettivamente non sono con Barbie protagonista), mette in pausa quando gli chiedo di spostarsi perché devo andare in bagno.

Sua madre è seduta due file più giù, con un bambino molto piccolo, che piange in braccio a lei ed è evidente che lo smartphone ha il compito di distrarre il mio compagno di fila, per consentirle di sedare con qualche coccola il fratellino minore. Il mio piccolo compagno di viaggio non ha le cuffiette, e questo lo rende un po' molesto, ma mentre lo sbircio mentre tiene gli occhi fissi sullo schermo dello smartphone e i suoi video, **mi chiedo se sia giusto che la madre gli abbia dato quell'oggetto da manovrare, da solo, per distrarlo.**

Bambini e smartphone: il ruolo della scuola

Poi mi ricordo che quando noi si stava davanti alla televisione, dicevano che era quella la nostra baby sitter. Una priorità invece mi è molto chiara: quale dovrebbe essere il ruolo della scuola, la sua responsabilità nel fornire una diversa educazione all'uso dei media digitali rispetto a quanto riescano a fare i genitori.

Perché la forza della scuola è la sua socialità e la media literacy va educata in un contesto sociale.

Quello che più colpisce, pensandoci, sono i tanti **bambini intrattenuti da schermi in pizzeria**, mentre cenano con la famiglia o nel passeggino, mentre aspettano accanto ai genitori che sostano in fila oppure in volo o sull'autobus. **Non ne ho visti invece (non in pubblico) guardare uno schermo insieme ad un adulto.**

Come ho già accennato, infatti, non è tanto l'uso degli smartphone in sé a essere malsano, quanto il suo utilizzo in solitudine**. Le competenze più complesse vanno educate a scuola perché è lì che possono essere predisposti ambienti di apprendimento dove le tecnologie digitali hanno uno spazio studiato**, progettato e ben inserito in una visione didattica contemporanea.

I quattro livelli di apprendimento di Bateson

Nel suo libro *Verso un'ecologia della mente*, Gregory Bateson ha proposto la classificazione di **quattro livelli di apprendimento.**

Al livello zero ha messo l'apprendimento semplice o meccanico, fondato essenzialmente sulla reazione stimolo-risposta.

Al livello uno si trova invece **l'apprendimento che dà origine alla formazione di abitudini, derivanti dall'esperienza e dall'addestramento**, come quello di tipo scolastico tradizionale, in cui l'insegnante stabilisce che cosa l'allievo deve imparare e definisce i ritmi, la quantità e la qualità dell'insegnamento. A questo livello interviene un cambiamento nella risposta agli stimoli, mediante la correzione degli errori di scelta in un insieme di alternative.

Arrivati al livello due, finalmente **l'apprendimento è connesso al cambiamento del modo in cui le azioni e le esperienze sono suddivise in base al contesto delle relazioni**: il soggetto fornisce risposte adeguate agli stimoli provenienti dall'esperienza e modifica le risposte in base al contesto. **Qui "apprende ad apprendere"**, ma lo fa ancora meccanicamente, acquisendo abitudini cognitive adatte alla soluzione dei problemi.

La parte più difficile arriva al livello tre, dove nascono **funzioni di valutazione complesse**, come la coscienza di esistere, di conoscere, di apprendere, di dare senso all'esperienza. È a questo livello che **il soggetto "impara a imparare"** consapevolmente e intenzionalmente, liberandosi dalle abitudini cognitive e diventando disponibile a uscire dal proprio io per confrontarsi con il pluralismo delle possibili verità.

Ecco lo smartphone va utilizzato a scuola per lavorare sui livelli due e tre, secondo me. La consapevolezza e la scelta, quella che il bambino sembrava esercitare in modo meccanico mentre col dito scorreva sullo schermo la lista dei video da guardare. **Per uscire dalle routine addestrate nelle abitudini familiari o legate al gruppo dei pari** (soprattutto per gli adolescenti) dobbiamo **rompere delle abitudini**: aiutare ciascuno studente a entrare in quegli stessi schermi con uno scopo, che non sia far passare il tempo o intrattenersi mentre qualcuno fa qualcos'altro. Ce la possiamo fare? Ce la possiamo fare.

I docenti devono avere il coraggio e nutrire quello spirito pioneristico, che dovrebbe essere proprio di qualsiasi educatore, che si muove alla scoperta dell'altro per costruire con lui una relazione, che è nuova ogni giorno. **Mi sembra che i tempi siano maturi per scendere dalle cattedre (per chi ci sale, naturalmente) e affiancare i nostri studenti in questo viaggio verso una maturità digitale**,

che ormai è ora di far affiorare in ogni spazio utile, in ogni luogo collegiale, in ogni discorso educativo, in ogni occasione di formazione e autoformazione.

Per farlo, occorre che docenti e studenti escano dalla *comfort zone*: i docenti devono tenere a bada la paura, che dicono di avere, verso un uso dei dispositivi mobili personali a scuola; gli studenti dovrebbero modificare le loro abitudini legate allo smartphone, **che prevedono un uso spesso limitato a chat, fruizione video e pubblicazione foto, talvolta in maniera compulsiva**. Se riuscissimo anche a coinvolgere le famiglie in questo percorso, forse, potremmo collaborare e agire come co-educatori, ma si può cominciare anche da soli. Niente scuse.

Bibliografia

Gregory Bateson, *Verso una ecologia della mente*, Adelphi, Milano, 1976

BONAIUTI, Giovanni; RICCIU, **Roberto. Mobile devices to increase attention and improve learning. Form@re** - Open Journal per la formazione in rete, [S.l.], v. 17, n. 1, p. 190-203, apr. 2017. ISSN 1825-7321.

Chi ha paura dei robot? La sfida si vince rimettendo l'uomo al centro

Intelligenza artificiale e automazione prospettano enormi ripercussioni su mondo del lavoro e attività produttive. Serve guardare al rapporto uomo-macchina in ottica di complementarità, spostando il focus su processi che valorizzino le potenzialità dell'intelligenza umana. Evitando il rischio di ridurle o comprimerle

Di **Mauro Lombardi**, Scienze per l'Economia e l'Impresa, Università di Firenze

L'avanzata irreversibile della tecnologia intellettuale deve indurre a concentrarsi sulla complementarietà, e non sul conflitto, tra l'uomo e la macchina: occorre innanzitutto **porre *l'uomo al centro* del processo di transizione** e quindi ideare strumenti idonei a **valorizzare potenzialità che l'intelligenza umana possiede**, evitando il rischio di ridurle o comprimerle.

Questo significa anche che **il focus strategico non può più essere il lavoro come totem, bensì le persone** sostituite o "spiazzate" dalla rivoluzione avviata.

Esaminiamo di seguito gli scenari che si aprono, la posta in gioco e gli shift da intraprendere per governare il passaggio.

Le caratteristiche della dinamica tecno-economica in atto

L'automazione così come viene rappresentata nella forma estrema che si sta realizzando - **Intelligenza Artificiale** + **robot** - viene "narrata" come la "fiaba del lupo cattivo", la cui funzione catartica è quella di liberare la nostra fantasia di uomini-in-formazione alle prese con le grandi contraddizioni della realtà (Bruno Bettelheim, 2013).

Il "lupo cattivo" è la sintesi immaginifica di tre peculiarità della dinamica innovativa odierna: generalità, trasversalità e presenza di agenti artificiali con abilità cognitive.

La dinamica tecno-economica ora in pieno dispiegamento ha infatti precise caratteristiche:

- data la rappresentazione digitale di processi e prodotti (***"digital twin"***), **è teoricamente possibile inserire ovunque sistemi di software che si auto-organizzano grazie all'interazione tra flussi informativi**. Siamo quindi di fronte a tecnologie di portata generale.
- **Algoritmi che evolvono sulla base di tali flussi possono influenzare e modificare i processi decisionali** e le attività fisiche ed intellettuali. In un mondo iperconnesso, la giustapposizione e l'integrazione tra flussi di informazione non "riflette" solo la realtà, bensì può "generarla" attraverso le azioni più o meno indotte su entità viventi e oggetti inanimati. **Siamo pertanto in presenza di meccanismi che operano in modo trasversale, cioè in un mondo fisico-cibernetico**, laddove il secondo aggettivo va interpretato alla luce

della definizione data da Wiener nella "Cibernetica: o controllo e Comunicazione negli Animali e nelle Macchine".

- Sistemi di algoritmi che si auto-organizzano ed evolvono sono in grado non solo di eseguire funzioni puramente meccaniche e ripetitive, bensì di **svolgere vere e proprie funzioni cognitive**: estrarre pattern da **masse crescenti di dati**, estrapolare tendenze, delineare opzioni alternative: **dal governo del traffico urbano e della diffusione di epidemie, alla definizione di scenari strategici mediante modelli di simulazione.**

Su questa base si generano processi dinamici e trend globali, che assumono forme estremamente diversificate, a seconda dei contesti economico-territoriali, delle culture in essi presenti, del grado di reattività strategica degli agenti socio-economici e istituzionali.

Quando reale e digitale interagiscono

La storia umana è ricca di episodi relativi a popoli e comunità, per non dire di vere e proprie grandi civiltà, che non hanno compreso adeguatamente le rivoluzioni tecno-economiche dei loro tempi, a causa di fenomeni collettivi di *lock-in* cognitivi, cioè di chiusura culturale verso le sfide poste da cambiamenti tecnico-scientifici e dai connessi mutamenti sociali e geo-economici (Diamond, 2005). **In sostanza, l'attaccamento a modelli mentali inappropriati è alla radice di numerosi arretramenti di fiorenti civiltà**. Naturalmente la storia umana è ricca anche di esempi di società e comunità capaci di metabolizzare nuovi input scientifico-culturali e addirittura di essere stesse protagoniste di vere e proprie rivoluzioni di paradigmi tecnico-scientifici, salvo poi essere incapaci di captare segnali di cambiamenti epocali, dopo alcune generazioni.

Anche la storia del nostro Paese è stata interessata da traiettorie sussultorie di questa natura e morfologia. Naturalmente tutto questo assume caratteri parossistici durante i periodi di grande trasformazione, come quello odierno, incentrato sulle **interazioni multi-dimensionali tra la sfera reale e la sfera informativa**, che costituiscono appunto componenti fondamentali del mondo fisico-cibernetico in cui siamo entrati. **E' logico infatti che ciò accada laddove prevalgono assetti economico-produttivi fortemente radicati in saperi e competenze tradizionalmente accumulate *on site*** e fonti di successo grazie ad appropriati modelli manageriali per un ambiente competitivo molto differente rispetto a quello odierno.

Lo scenario tecno-economico attuale ha alla base una discontinuità negli input tecnico-scientifici che occorrono per modellare output a partire da nuovi materiali (progettati a scala nano-molecolare) fino alla scala ordinaria e globale, cioè **modelli di prodotti e servizi da proiettare nel mondo iperconnesso**. Emerge chiaramente che esiste un potenziale di trasformazione che comprende molte dimensioni dei contesti economico-sociali.

Trasformazioni così estese e profonde non possono dispiegarsi senza l'operatività di *soft infrastructures*: Centri di Ricerca, schemi culturali aperti, nuove regolamentazioni, strutture interattive Università-Industria, strategie formative di nuova concezione, politiche strategiche in ambito industriale e fiscale. **Conseguenza inevitabile delle grandi trasformazioni è la creazione di un insieme variabile e ignoto (all'inizio) di asimmetrie culturali, economiche, sociali, di potere di mercato**.

Chi poteva ad esempio immaginare, nelle prime fasi della diffusione di Internet, la **concentrazione oligopolistica di GAFA (Google, Amazon, Facebook, Apple)**, divenute potenze economiche mondiali, di cui il caso relativo **Cambridge Analytica** è solo una pallida espressione, pur nella sua rilevanza ai fini dei processi politici USA. Pensiamo allora ad un'altra serie di elementi:

- grazie alla tecnica CRISPR-Cas9 **è possibile intervenire sul DNA** in funzioni di *editing* cioè modificarne segmenti.
- Vi sono **dispositivi in grado di realizzare reti wireless**, anche a lunga distanza, attraverso la luce come strumento di trasmissione delle informazioni.
- Vi è possibilità di **creare modelli dinamici integrati**, rappresentazioni complete multi-scala di processi e prodotti, mediante i quali controllare da remoto in *real time* motori di aereo, locomotive, case, ponti e infrastrutture, intere aree territoriali, insieme all'analisi chimico-ambientale e alla stima della probabilità di eventi indesiderati (inquinamento, probabili attentati, azioni belliche, fenomeni climatici anomali, ecc.).

I tecno-pessimisti: non c'è speranza per il lavoro

Tutto questo ha imponderabili ripercussioni sul mondo del lavoro e sullo svolgimento delle attività economico-produttive del mondo reale. E' pertanto logico che, a seconda delle assunzioni di fondo e della metodologia impiegata, gli studiosi finiscano per sviluppare analisi e interpretazioni contrapposte. **Da un lato abbiamo i *tecno-pessimisti***. Gordon, famoso economista statunitense, vede un trend di lenta diminuzione della capacità propulsiva delle innovazioni di questi decenni, con effetti depressivi sull'economia americana e internazionale. **Peter Thiel, inventore di PayPal e venture capitalist molto importante, non appare ottimista** sui cambiamenti introdotti dall'informatica nell'intervista a Tom Simonite (Technology Review, Febbraio 2015), durante la quale parla di "tecnologia a doppio senso". Soprattutto nell'ultimo capitolo di un suo libro (Thiel, 2016) sfida il senso comune secondo cui il mondo convergerà verso un plateau di sviluppo simile alla vita di oggi dei Paesi ricchi: "Il futuro come il presente". Thiel ricorda che la storia è piena di incredibili avanzamenti seguiti da collassi, che oggi sarebbe un collasso globale, per evitare il quale occorre "pensare a nuove cose che rendano il futuro non solo differente, bensì migliore –da zero a 1". Il punto essenziale è pensare per noi stessi, "perché solo guardando il nostro mondo nuovo, libero e strano come era per i nostri antenati che l'hanno visto all'inizio, possiamo ricrearlo e conservarlo per il futuro".

Un altro studioso, **l'economista Tyler Cowen** (2017) dal confronto con precedenti rivoluzioni industriali non vede emergere motivi di speranza, perché ogni volta si sono presentati enormi problemi sociali, economici e politici. Oggi questi potrebbero ripresentarsi su scala molto più ampia che in passato e la capacità di risposta ad essi appare del tutto inadeguata. Nel libro del 2013 Cowen prefigura uno scenario con due classi in America: una *extremely skilled élite* e tutti gli altri.

Larry Summers, professore emerito ad Harvard e con precedenti alte cariche politico professionali (Ministro del Tesoro con Clinton, direttore del National Econmic Council con Obama), dopo aver sostenuto la tesi della *secular stagnation* (Summers, 2016), nel 2013 in una conferenza al Bureau of Economic Institute ha affermato a proposito dell'automazione come causa della perdita di posti di lavoro: "Fino a pochi anni or sono non pensavo che la questione fosse complicata: i luddisti sbagliano e coloro che credono nella tecnologia e nel progresso tecnologico sono nel giusto. Ora non sono più completamento sicuro".

Due studiosi di fama internazionale, **Brynjolfsson e McAfee**, nel loro bestseller del 2011 sottolineano la tendenza all'accelerazione della dinamica tecnologica e il parallelo trend, ma in direzione inversa, verso la **diminuzione dei posti di lavoro**. Di qui "*the race against the machine*", che però va rifomulata nel senso che "*the key to winning the race is not to compete* against *machines but to compete* with *machines*", cioè nello sviluppare le capacità che i computer non hanno, quali intuizione e creatività, mentre sono molto più bravi nelle operazioni ripetitive, nei calcoli numerici, nello scoprire e associare pattern di dati.

In un successivo volume (2014) non esitano a ritenere che lo sviluppo di "**macchine che pensano**" sia incredibilmente positivo e possa contribuire a risolvere molti problemi umani, anche se sottolineano il rischio di uno **"*spread*" crescente tra *winners* (star e superstar) possessori di capitale fisico, finanziario e elevato capitale umano e *loosers* (tutti gli altri)**. Fenomeni come la polarizzazione socio-economica, unita alla potenziale abbondanza, alla varietà e all'aumento della qualità di molte componenti delle nostre vite costituiscono uno dei paradossi della nostra era.

Ancora più pessimista è **Martin Ford** (2015), che paventa uno scenario dove IA e l'"esplosione robotica" potrebbero portare a una "**tempesta perfetta**", dovuta a disoccupazione tecnologica e impatto ambientale su scala planetaria come tendenze parallele che si rafforzano reciprocamente, a meno che l'evoluzione tecnologica non sia diretta in modo da riconoscere e attenuare le implicazioni in termini di occupazione e distribuzione del reddito.

I tecno-ottimisti: meno lavoro, più tempo a disposizione

L'inventore e futurista **Ray Kurzweil** (2005) ritiene che alla fine di questo secolo si svilupperà in pieno un'intelligenza biologica molto più potente di quella umana a partire dal 2030, senza che ciò significhi la fine dell'intelligenza biologica, arricchita dalla presenza di **nanobots in grado di incrementare le potenzialità di ampie parti del nostro corpo**. Alla domanda "**Avremo un futuro senza lavoro umano se l'automazione assorbirà molte attività e professioni?**" Kurzweil risponde: "dipende da come definiamo il lavoro. Dobbiamo cambiare il nostro modo di pensare come dovrebbero essere le nostre vite. Attualmente è pienamente adottato un modello economico per cui la gente lavora, ottiene denaro e poi compra ciò di cui ha bisogno. Possiamo rovesciare il modello e ipotizzare che venga dato tutto il **reddito sufficiente per garantire a ciascuno di scegliere come spendere il proprio tempo**. Si lavorerà di meno e si impiegherà il tempo disponibile per approfondire le proprie passioni. Perché non chiamarle lavoro? Una volta che non dobbiamo lavorare per vivere, possiamo iniziare a vivere per lavorare". Questa tesi sarebbe la realizzazione di quello che lo studioso di problemi del lavoro **Benjamin Hunnicut** (2013) definisce "*Forgotten American Dream*" e il capovolgimento del *great reversal* realizzato nella storia umana (Hunnicut, 2006).

Il sociologo **Peter Frase** (2016) delinea invece quattro scenari: due paradisiaci e due infernali. Il suo messaggio principale è che "*the future is not bright nor gloomy. It's what we wake of it*". Non si può conoscere il futuro, ma il suo procedere lento e sconvolto da sussulti più o meno violenti dipende dalla nostra capacità di creare il mondo in cui vogliamo vorremmo vivere.

Non nutre preoccupazioni invece **Autor** (2015), che distingue tra polarizzazione occupazionale e quella salariale, le quali sono influenzate da fattori diversi. Le sue stime lo portano a ritenere che **la polarizzazione non durerà a lungo**, perché si tratta di un fenomeno ricorrente e vi sono **complementarità uomo-macchina**, il cui sviluppo dipende dall'elaborazione di strategie di investimento in capitale umano.

E' chiaro che autorevoli studiosi e specialisti divergono ampiamente circa gli scenari odierni e futuri concernenti gli effetti dell'automazione, né potrebbe essere altrimenti, date le loro assunzioni di partenza e risultati non univoci di analisi empiriche. Gli orizzonti di breve e di lungo termine sono soggetti all'azione di molti fattori e processi, tali da escludere la possibilità di effettuare previsioni con un grado di approssimazione molto stretto.

Guardando ad esempio alla produttività negli USA, nonostante il rilevante impiego delle nuove tecnologie, è previsto per i prossimi anni un ulteriore **rallentamento dall'1,8% all'1,4%**, distante

dal 2,4% del decennio precedente (MGI, 2018). Questi dati non preoccupano **Byrnjolfsson** (2018), ottimista perché il divario tra aspettative e le rilevazioni empiriche è dovuto al fatto che **le nuove tecnologie richiedono lo sviluppo di complementarità e co-invenzioni**, quindi occorre tempo e sostenere costi al di là di quelli previsti. Di conseguenza si sono generate false aspettative, sono insorte difficoltà nel misurare gli effetti, perché probabilmente quelli positivi sono concentrati in alcuni ambiti produttivi e non sono generalizzati, infine vi è una elevata probabilità che l'implementazione delle innovazioni richieda tempo.

Una convergenza di fondo con questa tesi è di fatto espressa da **Arntz** (2016), secondo il quale le stime circa la quota di attività-professioni a rischio di automazione non possono non divergere sia dai risultati già ottenuti che da quelli attesi per tre motivi:

- il processo di adozione delle nuove tecnologie è necessariamente lento.
- E' necessario, oltre all'investimento in capitale materiale, quello nella modificazione delle dotazioni conoscitive delle persone.
- **Saranno create nuove attività e professioni**, che non possono essere ipotizzate in questo momento, perché molto dipende da come nascono le conoscenze sulla base dei meccanismi di interazione tra domini conoscitivi differenti, posseduti da molteplici imprese e centri di ricerca.

AI e robot, le nuove sfide economiche sociali

Comunque sia, però, IA, Automazione e tutte le altre nuove tecnologie pongono una serie di **grandi sfide economico-sociali** ("*moonshot societal challenges*) (MGI, 2018), dal momento che, anche se solo una parte minima delle occupazioni (5%) sarà forse completamente automatizzata, quasi tutte saranno influenzate dai processi innovativi. **Bisogna inoltre tenere presente che le dinamiche effettive saranno condizionate da una serie di fattori**, a loro volta dipendenti dai contesti: tipologie dei mercati del lavoro, caratteristiche quantitative e qualitative dell'offerta di lavoro, norme sociali prevalenti, adattatività di individui e sistemi di imprese.

In effetti, quello che possiamo dire con una certa fondatezza è che **un'ampia parte della popolazione dovrà modificare profondamente la propria dotazione conoscitiva e le competenze**. Riteniamo allora logico concentrare l'attenzione sui problemi e le sfide generali al fine di elaborare strategie appropriate.

La prima assunzione da cui partire è che siamo in una fase di transizione tecno-economica e sociale di grande portata. Un'implicazione immediata di ciò è il prodursi di **molte e profonde asimmetrie**: cognitive, sociali, economiche, di potere, a causa dell'ampliarsi dei divari tra le possibili traiettorie di evoluzione, implicite nel potenziale tecnico-scientifico in dispiegamento, e gli assetti socio-economici consolidatisi nel tradizionale e del tutto differente *frame*, ovvero in uno schema strutturale prototipico (struttura-funzione-performance) progettato a varia scala nei modelli di impresa, dell'organizzazione sociale, dei processi formativi.

Si tratta quindi di uno *shift* multi-dimensionale complesso verso un "nuovo mondo", dove si sovrappongono e intersecano processi e agenti (individuali e collettivi), che oggi devono pensare e agire in un mondo iperconnesso, con **flussi informativi** in incessante evoluzione. **Variabilità e incertezza divengono, pertanto, proprietà determinanti degli orizzonti decisionali, al cui interno evolvono intelligenza umana e intelligenza artificiale**, a causa dell'esistenza di un meccanismo propulsivo basilare: la "tecnologia intellettuale" di produzione (Bell, 1973), cioè la codificazione della conoscenza teorica incorporata nelle macchine.

Macchine con funzioni cognitive

Quello che cambia radicalmente rispetto al passato non è l'uso della conoscenza, bensì "l'applicazione della conoscenza e dell'informazione a dispositivi che generano, elaborano e comunicano conoscenze e informazioni in cicli di feedback cumulativi tra innovazione e usi dell'innovazione" (Castells, 2010, p. 31). Ecco perché questa volta può essere differente: **IA, Machine Learning, robotica avanzata e robotica evolutiva** vanno oltre attività e funzioni elettro-meccaniche, **svolgendo anche funzioni cognitive**, come affermato all'inizio. La tecnologia intellettuale tende ad entrare profondamente anche nell'universo simbolico degli umani, nel processare informazioni e influenzarne il linguaggio e i processi cognitivi. Non si tratta più del passaggio dall'economia a base agricola a quella industriale e terziaria, bensì della **trasformazione dell'intelaiatura essenziale delle attività umane**, oggi sostenute e alimentate da sistemi di algoritmi in continua evoluzione e approfondimento.

Risiede in questo mutamento di fondo la causa dell'enorme divario che si apre tra l'immenso spazio della conoscenza e la limitata razionalità umana (Simon, 1979). La conseguenza più rilevante è la transitorietà della propria dotazione conoscitiva e delle competenze possedute da ciascuno, perché l'universo informativo in continua espansione cambia tendenzialmente il contenuto di ogni tipo di attività lavorativa (*task*), con il **rischio di rendere obsolete figure e funzioni tradizionalmente considerate solide.**

In questo scenario emergono due probabili trend, di cui è arduo delimitare preventivamente i confini, che sono variabili: **sostituzione di certi lavori e professioni**; cambiamenti delle attività delle persone tramite una **modificazione delle dotazioni conoscitive e delle competenze**, in modo da metterle in condizioni di effettuare **attività che le macchine non sono in grado di svolgere** perché non ne hanno le capacità e –presumibilmente- non l'avranno in un futuro più o meno lontano. Dobbiamo allora inquadrare il problema con uno frame concettuale basato su sfide con cui misurarsi alla luce di una migliore comprensione di quello che sta accadendo, preparando il terreno e gli strumenti per affrontare eventualità al momento ignote oppure conosciute in modo ambiguo e confuso.

L'uomo al centro della rivoluzione tecno-economica

Se l'automazione è in grado di inglobare sia **funzioni di routine non cognitive** che **funzioni non di routine cognitive**, anche se in misura non totalizzante, la traiettoria obbligata di intervento, se non si intende assecondare processi di asservimento dell'uomo alla macchina e di progressivo indebolimento delle capacità intellettuali umane, è quella di **promuovere un sistematico e generale processo di acculturazione rispetto all'universo fisico-digitale**, il che non significa semplicemente imparare a usare oppure a programmare, bensì **riorganizzare le sequenze formative con nuovi principi e metodi**, alla luce delle conquiste della fisica, delle **scienze cognitive**, della filosofia della mente, della logica computazionale e così via.

Investire in processi di formazione permanente

Come viene ampiamente argomentato in recenti Rapporti dell'Aspen Institute (Future of Work Initiative, Automation and a Changing Economy, Aprile 2019) e della Brooking Institution (Automation and Artificial Intelligence, Gennaio 2019, a cura di M Muro, R. Naxim, J. Whiton), occorre adottare una strategia multi-dimensionale, che prenda in considerazione precise direttrici di azione:

1) cospicui investimenti, sia pubblici che privati, in **processi di formazione** a tutti i livelli e lungo tutto l'arco della vita. Si tratta di una direzione opposta a quella scelta dagli Usa e da molti altri Paesi occidentali, dove sono diminuiti gli interventi e i progetti sia delle imprese che delle istituzioni.

2) Invenzione di nuovi e tra loro **complementari meccanismi per favorire processi di acculturazione e reinserimento** tramite strumenti di sostegno economico, assistenziale (erogazione di servizi innovativi) e orientamento verso nuove potenzialità.

In sostanza, **il descritto processo di transizione richiede una rete di sicurezza integrata**, strategicamente orientata e gestita secondo criteri di razionalità adattativa ed efficacia costantemente valutata. Anche in questo caso le tendenze degli ultimi decenni vanno in senso opposto, con un pronunciato declino in ciascuna delle direttrici.

3) **Creazione di nuovi strumenti di cooperazione socio-economica**. E' necessario creare le basi per superare chiusure individualistiche e falsamente identitarie, favorendo lo sviluppo di una **progettazione sociale delle trasformazioni**. Il termine non deve spaventare: negli stessi documenti dell'Aspen Institute e della Brookings Institution sono introdotti temi in passato tabu per la cultura manageriale americana: **la necessità di far partecipare le persone alle decisioni delle imprese**, condividendo la consapevolezza dei cambiamenti e dei percorsi per il superamento delle difficoltà. L'espressione "nuove forme di cooperazione socio-economica" significa anche e soprattutto far sì che **intere fasce di popolazione possano essere coinvolti in dinamiche di apprendimento**, senza essere abbandonati di fronte alle sfide dell'IA e dell'automazione. **Lo sviluppo di una cultura adattativa richiede originali modelli di condivisione sociale di competenze, valori e orizzonti evolutivi.** Per questa via è possibile ridurre le asimmetrie di varia natura, più volte sottolineate per enfatizzare le interdipendenze tra livelli conoscitivi, reddito, ruolo sociale, partecipazione democratica.

A questo punto è opportuno rispondere ad un interrogativo: perché queste sfide sono basilari? La ragione della risposta affermativa è la seguente. Esse vertono e innovano tre pilastri del modello di società prevalso nella seconda metà del '900: **sono poste al centro le persone** e la loro funzione; viene stimolata la **rigenerazione dei presupposti dell'appartenenza sociale degli individui**; è perseguita la **valorizzazione su nuove basi degli esseri umani come "animali sociali"**. Il punto di arrivo di queste riflessioni è chiaro: se non sapremo dare risposte efficaci alle sfide, verranno meno i fondamenti delle stesse società e il futuro dipende da come riusciremo a modellarlo in base a scelte consapevoli della posta in gioco.

Bibliografia

Autor D.A., 2015, Why Are There Still So Many Jobs? The History and Future of Workplace Automation, The Journal of Economic Perspectives, Vol. 29, No. 3 (Summer 2015), pp. 3-30

Bell D., 1973, The Coming of Post-Industrial Society, Basic Books

Bettelheim B., 2013, Il mondo incantato. Uso, importanza e significati psicoanalitici delle fiabe, Feltrinelli

Brynjolfsson E., McAfee A., 2011, The race against the machine, Digital Frontier Press

Brynjolfsson E., McAfee A., 2014, The Second Machine Age, Norton Company

Castells M., 2010, The Rise of Network Society, Whiley-Blackwell

Frase P., 2016, Four Futures. Life after Capitalism, Verso Books

Cowen 2013, The Average is Over, Penguin Books

Cowen T., 2017, Industrial Revolution Comparisons Aren't Comforting, Bloomberg Blog, february

Diamond J., 2005, Collapse. How Societies choose to Fail or Succeed, Viking

Frase P., 2016, Four Futures: the Life After Capitalism, Verso Press

Kefee Conversation with Ray Kurzweil, Singularity Hub (https://singularityhub.com/2016/08/11/ray-kurzweil-the-future-offers-meaningful-work-not-meaningless-jobs/

Hunnicutt B-K., 2013, Free Time: The Forgotten American Dream. Temple University Press

Hunnicutt B-K., 2006, The History of W estern Leisure, in Rojek et al., cit

Ford M., 2015, Rise of the robots: technology and the threat of a jobless future, Basic Books

Kurzweil R., 2005, The Singularity is Near, Viking

MGI (McKinsey Global Institute), 2018, AI, Automation and the Future of Work, Ten Things to solve for, June

Rojek C., Shaw S.M., Vea A. J., 2006, A Handbook of Leisure Studies, Palgrave McMillan

Simon H.A., 1979, Rational Decision Making in Business Organizations, The American Economic Review, Vol. 69, No. 4, pp. 493-513

Summers L., 2016, Secular Stagnation, Foreign Afairs, February

Thiel P. with Blake Masters, 2014, Zero-to-One, Crown Business, New York

Wiener N, 1948, Cybernetics: or Control and Communication in the Animal and the Machine, MIT Press

Libra di Facebook ovvero la crisi della democrazia

Chi sarà a "battere la moneta" globale nel cyberspazio? Chi verificherà l'identità della persona che effettua una transazione? Libra, che rischia di trasformarsi nel porto franco del riciclaggio, lancia una seria sfida alle Autorità e richiama la necessità di tornare a definire limiti e regole democratiche condivise

Di **Norberto Patrignani**, Politecnico di Torino

Le cosiddette valute digitali sono già da qualche anno sotto lo scrutinio di tutte le autorità finanziarie del pianeta ma il **lancio di Libra** da parte di Facebook apre molti interrogativi più ampi e forse, paradossalmente, lancia una importante **sfida proprio alle autorità internazionali, chiamate a regolamentare dal punto di vista finanziario, fiscale e penale qualcosa di molto sfuggente**: chi sarà a "*battere la moneta*" globale nel cyberspazio? Chi verificherà l'identità della persona che effettua una transazione? Se dei problemi per la **privacy** si è già ampiamente discusso, cominciano infatti a emergere anche gli allarmi degli esperti di riciclaggio (Gaiullo e Mincuzzi, 2019), che definiscono molto elevato **il rischio che Libra crei un meccanismo perfetto per criminali e evasori fiscali.**

Ma i dubbi e gli interrogativi su Libra non finiscono qui. Come spiegherò di seguito, l'annuncio del lancio della criptomoneta di *Facebook* potrebbe rappresentare anche l'ultima mossa nella gigantesca partita a scacchi tra USA e China.

O**ppure l'ennesimo slittamento della società globale verso un mondo dominato unicamente dal mercato e dalle tecnologie connesse**, lasciando indietro i due pilastri della storia dell'umanità: la definizione di regole condivise tramite regole democratiche e la preparazione delle prossime generazioni tramite l'educazione.

Serve, insomma, una riflessione molto ampia su molti aspetti.

Libra: è ancora Usa vs China?

L'ultima mossa di Facebook va nella direzione di integrare in un unico ambiente *social netwok*, *chat*, *pagamenti* e *transazioni finanziarie*. Ma nel mondo esiste già una cosa simile creata da uno dei "titani del Web", *Tencent*, con la sua *WeChat*, il più grande *social network* della Cina, con miliardi di utenti e con il suo sistema di pagamenti *WeChatPay*. Integrare *WhatsApp* con *Libra* assomiglia molto all'applicazione offerta da *Tencent*. Ma **se in Cina il contesto permette al governo un controllo capillare sui cittadini, in altri paesi la fusione del business bancario con altri settori dell'economia non è così semplice**: sapere cosa compro è ben diverso dal sapere con quali risorse lo compro.

I rischi di conflitti e monopoli sono altissimi. Forse *Facebook* sta cercando di diversificare il suo business che, basato sulla pubblicità, è molto condizionabile dagli utenti e dagli inserzionisti? E se i

servizi attualmente gratuiti diventassero a pagamento? Avere direttamente accesso alle transazioni, anzi controllarle, non faciliterebbe il compito? Inoltre, dopo lo scandalo *Cambridge Analytica*, anche la necessità d**i curare la reputazione o distrarre i *policy maker*** con altre mosse diventa urgente. Oppure stiamo assistendo all'emergere di una nuova guerra fredda in versione "USA - Cina", stavolta tutta giocata sul dominio del cyberspazio?

Verso il dominio del mercato e delle tecnologie connesse

Controllare e garantire le transazioni di miliardi di persone su scala globale è un compito molto più complesso rispetto al tradizionale raggio d'azione delle autorità di vigilanza finanziarie, tipicamente localizzato. **La sede fisica di questa nuova iniziativa è la Svizzera (Reuters, 2019) e quindi la sua autorità di sorveglianza sui mercati finanziari, FINMA (Swiss Financial Market Supervisory Authority), si trova di fronte ad compito non semplice**. Eppure proprio l'amministratore delegato di *Facebook* aveva recentemente chiesto ai *policy maker*, ai governi, di regolamentare la rete: "*...abbiamo bisogno di un ruolo più attivo dei governi e dei regolatori*" (Zuckerberg, 2019).

I problemi tecnici legati alla progettazione e gestione di tale sistema complesso sono enormi: pensiamo solo ai requisiti normativi (*compliance*) richiesti attualmente alle banche. Oppure, visto che i fondatori dell'iniziativa sono imprese private soggette a fallimento, **cosa succede alla "riserva" di *Libra* in caso di problemi?** Rischiamo di introdurre un altro esempio di interessi privati che, in caso di problemi, si trasformano in costi per la collettività?

Una riflessione sulla democrazia

Ma una riflessione più profonda riguarda la democrazia stessa: seppur criticabili in molti aspetti, in molti paesi del mondo le autorità di regolamentazione sono designate da rappresentanti eletti democraticamente. Chi eleggerà le *authority* bancarie del *cyberspazio*?

Certamente avere la possibilità di effettuare acquisti e transazioni con un semplice dispositivo online in molti paesi in via di sviluppo è un'opportunità. Infatti molte società high-tech si stanno focalizzando proprio in quei paesi dove sistemi di pagamento sono poco disponibili e nello stesso tempo la telefonia mobile ha superato quella fissa, offrendo servizi non solo a privati ma anche a piccole imprese senza un conto bancario. E l'opportunità esiste davvero in quanto può appoggiarsi su una base di partenza di oltre due miliardi di utenti della popolare *social network*.

Questo è il punto cruciale: **per accedere al sistema di pagamenti non è più necessario un conto bancario ma basta un account su *Facebook*.** Il nuovo sistema potrebbe anche fornire servizi di credito o micro-credito come quelli introdotti già dal 1983 dalla *Grameen Bank* del Premio Nobel per la Pace 2006 Mohammad Yunus. Le differenze tra la proposta globale lanciata da Facebook e quelle locali tipo *social lendin*g o prestiti *peer-to-peer* sono evidenti: il ruolo delle comunità locali nella definizione di relazioni di fiducia.

Nell'annuncio di *Libra* stessa sono annunciate molte promesse: "*... creare una nuova opportunità per un'innovazione responsabile dei servizi finanziari.*" Ma **un'innovazione responsabile richiede anche il coinvolgimento delle comunità**, evitando il rischio di introdurre ulteriori forme di dipendenza.

E non si tratta solo di dipendenza economica. La possibilità di premiare chi guarda la pubblicità con valuta digitale spendibile in acquisti, permetterebbe a chi gestisce la piattaforma di avere due

business paralleli: quello degli inserzionisti che pagano per esporre i loro prodotti e quello degli utenti del *social network* che pagano una percentuale sui loro acquisti. Il rischio di innescare un circolo che si autoalimenta è altissima, più pubblicità guardo, più guadagno, più spendo, ...con rischi di diventare *shopaholic*, dei veri maniaci dello shopping.

In una fase dell'Antropocene dove dobbiamo tutti affrontare urgentemente **i rischi del cambiamento climatico**, possiamo permetterci un aumento esponenziale dei consumi, dei trasporti?

Tornare alle regole condivise

Diventa urgente aprire una riflessione sul subdolo slittamento della società globale verso un mondo dove le regole sono dettate unicamente dal mercato e incorporate in tecnologie poco trasparenti. Il mercato e le tecnologie saranno pure importanti, ma **quando si arriva a toccare in profondità le regole di convivenza forse è meglio riprendere il controllo definendo dei limiti e delle regole democratiche condivise**. Si aprono nuovi scenari che richiedono a tutti un grande salto evolutivo. Problemi globali, come il cambiamento climatico, richiedono una visione di interdipendenza da parte di tutti.

La rete è un ottimo esempio: come diceva Rodotà, s**enza una "costituzione" rischia di diventare il Far West del XXI secolo (Rodotà, 2007)** e forse è arrivato il tempo per definire e approvare un Internet Bill of Rights che regolamenti le attività economiche sulla rete, incluse le valute virtuali.

Bibliografia

- Gaiullo R., Mincuzzi A. (2019), *Libra, controlli solo virtuali. Cresce il rischio riciclaggio*, IlSole24Ore, 23 Giugno 2019.

- Reuters, (2019), *Swiss regulator says in contact with initiators of Facebook's Libra*, reuters.com, June 18, 2019.

- Rodotà S. (2007), Una carta dei diritti del Web, Repubblica, 20 Novembre 2007.

- Zuckerberg M. (2019), The Internet needs new rules. Let’s start in these four area, Washington Post, 30 March 2019.

Internet ergo sum, la grande illusione del tecno-capitalismo

Non fermarsi mai. Non pensare, non studiare. Copia e incolla invece di ragionamento. Sono i paradigmi intorno ai quali la digital transformation articola il totalitarismo moderno che promette massima libertà. Annullandola. Da Marcuse a Gallino, un'analisi delle dinamiche della "industrializzazione della felicità"

Di **Lelio Demichelis**, Docente di Sociologia economica Dipartimento di Economia- Università degli Studi dell'Insubria

Digital transformation, quarta rivoluzione industriale, Industria 4.0, Intelligenza artificiale, IoT, smart? In realtà siamo dentro a una ulteriore tappa di una lunghissima ***rivoluzione industriale*** così come di una lunghissima *modernità* – **il *tecno-capitalismo*, come lo definiamo e costituito sempre e comunque da *accelerazione* delle macchine e del tempo**; di *divisione* del lavoro, dell'individuo e della sua *vita* e poi di *integrazione/connessione/sussunzione* degli uomini nella mega-macchina tecnica e capitalistica; di *mobilitazione totale* delle masse (ieri nelle guerre e oggi nell'economia globalizzata e nella fabbrica-rete), grazie all'*adattamento* e alla *coincidenza* di ciascuno nel e con il proprio ruolo/funzione di competitore, *di leone e di gazzella* nella savana del mercato.

Tecnocapitalismo, la grande narrazione

E quindi, le *grandi narrazioni* otto-novecentesche (le ideologie politiche) non sono morte, come sostenevano i post-modernisti – così come non è *finita la storia* nel 1989 - ma sono state sostituite da una nuova e globale *grandissima narrazione*: quella della *volontà di potenza* della tecnica e del feticismo per l'innovazione *a prescindere*, coniugata alla ***volontà di potenza* del mercato capitalistico**, per l'accrescimento infinito dell'apparato tecnico e del mercato e quindi del profitto del capitale. Il tutto sempre **rimuovendo ogni *principio di responsabilità* per la biosfera e per le generazioni future**, la terra e gli uomini essendo stati ridotti a merci e insieme a *miniera* (Heidegger) da sfruttare al massimo della estrazione di valore, siano esse *risorse naturali* come il petrolio o *risorse umane*.

Una *grandissima narrazione*, egemone e dominante, fatta di retoriche individualistiche, libertarie-anarco-capitaliste ma soprattutto di fascinazione/innamoramento per tutto ciò che è tecnica e *comunitarismo tecnico*. Agendo sul *doppio movimento psicologico* degli uomini, quello che li porta da un lato a cercare la *differenziazione dagli altri* e quello, dall'altro lato, della ricerca di una *appartenenza/integrazione/coincidenza* con un gruppo/comunità, il sistema di potere attivando ora l'uno ora l'altro e possibilmente insieme (*infra*). Tutto questo utile a *produrre* l'integrazione funzionale ma *libera* di ciascuno nel sistema tecno-capitalista, cioè nella *società amministrata* (Horkheimer e Adorno) o nel ***totalitarismo della società industriale avanzata* (Marcuse).**

L'uomo funzionale: rovesciato l'imperativo kantiano

Perché sempre più il ***tecno-capitalismo*** non è un *mezzo* a disposizione dell'uomo ma - rovesciando l'imperativo kantiano - è l'uomo a essere divenuto *mezzo per* il funzionamento e *parte* della mega-macchina (appunto, la sua ibridazione/sussunzione totale nell'apparato), incessantemente *spinto* a *produrre* (merci, valore, emozioni, condivisione, dati), a *consumare* (anche il *low cost* serve a questo) e oggi a *innovare* (sempre *prescindendo* dalla utilità dell'innovazione), alla sua massima prestazione/produttività e creatività.

È la *società adescante* secondo Neil Postman; è **il *capitalismo delle emozioni* e l'*industrializzazione della felicità***; è la *società della prestazione*; è il neoliberalismo come *biopolitica* secondo Michel Foucault, che governa e orienta e guida la vita dell'uomo nella direzione voluta dal tecno-capitalismo (il neoliberalismo inteso come *filosofia politica* per *far adattare incessantemente* la società e gli individui alle *esigenze* della rivoluzione industriale – secondo Walter Lippmann). Tutto per rendere l'uomo sempre più *funzionale* - cioè sempre più integrato/sincronizzato/accelerato e connesso e quindi *mobilitabile* (*mobilitabile perché connesso*) e soprattutto **perfettamente *identificatosi/coincidente* – con il *funzionamento* dell'apparato tecnico e capitalista**.

Per cui anche la scuola non deve essere luogo dove costruire un *pensiero critico* - ovvero dove acquisire una *conoscenza* capace di essere la *cassetta degli attrezzi intellettuali* per capire il mondo in cui si vive - ma solo una *fabbrica fordista-tayloristica (ma in just in time) di competenze* per il sistema. *Competenze*, appunto, per *far funzionare* la macchina tecno-capitalista, **ciascuno ibridandosi con la tecnica** e funzionando come la tecnica/algoritmo gli dice di funzionare. E non *conoscenze* che sarebbero utili invece per capire il *senso* di questo processo e immaginare un pensiero *divergente* e *dissidente* o almeno *critico/riflessivo/consapevole* per poter *governare* i processi di innovazione senza esserne, come oggi, *governati* inconsapevolmente.

I rischi della "didattica delle competenze"

Tutta (o quasi tutta) la scuola modellandosi non solo secondo ***ordine e disciplina* (Salvini)**, ma anche o soprattutto (ma è un'altra forma di *ordine e disciplina*) secondo la ***didattica delle competenze* promossa dal neoliberalismo**, dove *imparare a imparare* non è la forma pedagogica virtuosa e umanistica (virtuosa perché umanistica) per aiutare l'individuo a costruire la propria *individuazione* mediante la *conoscenza*, ma è (appunto) la ***biopolitica disciplinare*, neoliberale e tecnica per farlo *coincidere al meglio e on demand* con le *esigenze* della rivoluzione industriale** (in proposito rimandiamo all'ottimo libro di Mauro Boarelli, *Contro l'ideologia del merito*; ma anche a *La tirannia della valutazione* di Angélique del Rey e a *Funzionare o esistere?* di Miguel Benasayag). **Coincidendo/adattandosi, l'uomo è sempre meno soggetto/individuo** e sempre più (Adorno) è il *prodotto/oggetto del sistema che lo produce*. Anche mediante la *didattica delle competenze* – come con il marketing, l'industria culturale, la società dello spettacolo, il pathos per la tecnica e l'innovazione, il *non ci sono alternative*.

C'era una volta la "new era" tecnologica

Dunque, nessuna *new era* grazie alla tecnologia di rete, anche se questa era la promessa/favola/storytelling dei guru/teologi/visionari dell'innovazione degli anni '90. Nessuna riduzione della fatica del lavoro e dei tempi e dei ritmi di lavoro grazie alla tecnica (come appunto promesso in quegli anni), ma esattamente il contrario: **lavoro h24, ritmi accresciuti come accresciuta è la fatica (anche lo stress è fatica)**.

Mentre la rete è divenuta (un'altra eterogenesi dei fini; un'altra utopia divenuta distopia; o un'altra *profezia che non-si-auto-avvera*) la nuova ***organizzazione scientifica del lavoro in forma di folla/sciame-lavoro disseminato***. Con in più e peggio: sovrapposizione di tempi di lavoro e tempo di vita e insieme flessibilità totale e precarizzazione della vita, *estrazione di valore dal pluslavoro collettivo*, soprattutto ***ibridazione/sussunzione* totale dell'uomo nella mega-macchina/sistema tecnico e insieme trionfo della *finzione totale* e della sua *spettacolarizzazione***. Con la **totale e totalitaria *dipendenza* dell'uomo dalla tecnica e una *alienazione reale da sé dell'uomo***, *ma ben mascherata* dallo stesso sistema feticistico ed estraniante che la produce e riproduce incessantemente.

Il '900 è stato sicuramente un secolo di grande progresso scientifico, ma anche (secondo lo scrittore William Golding), *il secolo più violento della storia dell'umanità*. Oggi divenendo il secolo più violento e dis-umano non solo verso/contro gli uomini ma verso/contro la biosfera, nella massima potenza del conflitto della *tecno-sfera* contro la *bio-sfera*. Ma facciamo finta di niente, la nostra *dis-umanità* verso uomini e ambiente rasenta il più irresponsabile *cupio dissolvi*. Viviamo circondati dalla/integrati nella tecnica, *ma siamo incapaci* (Gino Strada) *di progredire sul piano etico* – anche perché, aggiungiamo, **per il tecno-capitalismo l'*etica* come la *responsabilità* sono un *intralcio* al dispiegamento illimitato della propria *volontà di potenza***. Quindi da eliminare.

Viviamo conseguentemente in una sorta di ***sadomasochismo collettivo e insieme molecolare/individuale*** e più facciamo del male (agli altri e alla biosfera) - e quindi *ci* facciamo del male - più *crediamo* di *godere*, magari *consumando* o *divertendoci* e *vetrinizzandoci/mercificandoci*. È un **falso *principio di piacere* confuso con il *principio di prestazione*** (dalla *industrializzazione della felicità* al capitalismo dell'emotività), creati per noi (il biopotere che produce biopolitica/tanatopolitica) dal tecno-capitalismo per evitarci di dover o poter fare i conti con il *principio di realtà*; e soprattutto con il *principio di responsabilità* (Hans Jonas) verso le generazioni future e la biosfera. Ovvero, ancora Adorno, il sistema *produce* anche in questo modo l'uomo *di cui ha bisogno* per funzionare al massimo del plusvalore per sé.

La tecnica ci fa *credere* che lo smartphone sia un *giocattolo* mentre è una macchina di produzione di dati, ma soprattutto la *forma* e la *norma* di *normalizzazione* di ciascuno nella *società amministrata/totalitaria* che si chiama rete - e il Progresso diventa inevitabilmente Regresso e l'Utopia si capovolge in *Retrotopia* (Bauman).

La società di massa? E' in rete

Se dunque siamo dentro alla *modernità* di tecnica e capitalismo e se la sua logica (*suddividere* lavoro, vita, individuo, realtà, spazio, tempo, per ottenere la massima *integrazione* di tutti nel proprio sistema organizzativo/produttivo/valoriale) si conferma anche oggi nella fabbrica-rete, allora ***dobbiamo* applicare i termini e i concetti della *modernità* e della *rivoluzione industriale* per descrivere *anche* questa sua ultima fase**. Modernità e rivoluzione industriale che non vivono di cesure (prima, seconda, terza, quarta rivoluzione industriale – queste sono retoriche fuorvianti che mascherano l'*uniformità e la unidimensionalità* delle *forme* e delle *norme* di *normalizzazione/normazione sociale* di tecnica e capitalismo), ma è un *processo* che dura da tre secoli, sempre diverso ma sempre uguale - dalla fabbrica degli spilli di Adam Smith alla catena di montaggio al capitalismo delle piattaforme/fabbrica-rete.

Iniziamo allora dal concetto otto-novecentesco di *società di massa*. E dalla **definizione che ne dava Luciano Gallino** nel suo *Dizionario di Sociologia*, pur riconoscendo che il termine presenta comunque molte ambiguità: la *società di massa* è "quella società, non necessariamente capitalistica,

in cui *la popolazione partecipa su larga scala alle attività di produzione, distribuzione e consumo di merci e servizi*, nonché a qualche forma di attività politica e culturale, anche in veste di consumatrice della cultura di massa" (corsivi nostri). Agli elementi indicati da Gallino, Giovanni Borgognone aggiungeva "le tendenze all'omologazione delle identità e dei comportamenti, all'indebolimento dei legami familiari e comunitari e all'atomizzazione sociale".

Dovrebbe essere dunque evidente (anche se imbarazzante da ammettere, dopo trent'anni di ideologia e di pedagogia **neoliberale-individualistica**), che anche oggi ci troviamo in una *società di massa*, organizzata (*amministrata*) grazie alla rete, cioè alla tecnica, dove tutto è e deve essere automatico/automatizzato, dal lavoro al pensiero. **La *popolazione* – fattore chiave di ogni biopolitica e insieme oggetto di ogni forma di *amministrazione* tecnico-economica – è oggi nella realtà virtuale**, che è lo *spazio* della società di massa, o meglio il nuovo *nomos* non più della terra o del cielo, ma del virtuale (parafrasando Carl Schmitt); e più di ieri *partecipa su larga scala alle attività di* ***produzione, distribuzione e consumo di merci e servizi*****, h24, senza più distinzione tra tempo di vita e di lavoro.**

Tutti isolati ma connessi. Grazie alla rete

In verità da tempo **siamo passati da una società di *massa concentrata* a una società di *massa individualizzata*, cioè ad una *massa di individui***. Se già Hitler e Goebbels avevano capito "che per mezzo della radio potevano essere coordinati ed effettivamente massificati una quantità incomparabilmente maggiore di uomini che non nelle spianate di Norimberga" (Anders) – oggi tutto è ulteriormente potenziato (la *massificazione degli individui isolati/separati, solistici* diceva Anders) grazie alla rete. Per cui, ancora Anders, **siamo in una società di massa che non ha più bisogno di *sostanzialità fisica*, perché i singoli sono comunque, anche oggi via rete, *completamente livellati*** pur essendo separati/isolati dagli altri ma connessi grazie alla rete.

La massa quindi, ieri e ancor più oggi, *è diventata una qualità di milioni* (oggi miliardi) *di singoli, non più la loro concentrazione*. Dove l'atomizzazione prodotta dalla società di massa non è un problema ma è perfettamente funzionale alla costruzione di una massa molto più *funzionale* di quelle del passato (ancora tecnica e capitalismo: *individualizzazione/suddivisione* e poi *totalizzazione/integrazione*). E sempre Anders aveva già analizzato **una nuova forma di *lavoro a domicilio* molto simile al *lavoro esternalizzato/on demand di folla-sciame/lavoro diffuso o disperso*** di oggi, scrivendo: "gli interessi del sistema conformistico" – e ogni società di massa *è* un *sistema conformistico/conformante e insieme attivante/adescante* – "sostengono e promuovono il lavoro a domicilio in modo esplicito. E ciò perché hanno il massimo interesse a nascondere che il loro è già un sistema totale (e con ciò *un sistema di totale privazione di libertà*). E riescono in questo *disperdendo gli incarichi di lavoro*, cioè assegnandoli a singoli come lavoratori a domicilio" e oggi tali (*diversamente a domicilio*) sono **i lavoratori autonomi/free-lance/imprenditori di se stessi, i riders di Foodora e gli autisti di Uber e i professionisti uberizzati**, **ma anche i consumatori che consumano via Amazon** (che svolgono un *lavoro di consumo*) o tutti noi che generiamo dati *lavorando* appunto davanti al pc o con lo smartphone (forma massima di lavoro ancor più *a domicilio*, addirittura *peripatetico* – ma soprattutto *alienato e alienante da se stessi e dalla propria vita*).

Il concetto di mobilitazione totale

Un secondo concetto otto-novecentesco che tracima nel nuovo secolo è quello di *mobilitazione totale*. Anch'esso legato alla rivoluzione industriale e alla modernità, anch'esso generato dal sistema tecno-capitalista per *creare* l'uomo e la società di cui ha bisogno per sostenere il proprio

accrescimento infinito e la propria volontà di potenza. Allo stesso tempo, *amministrandone* la vita in modo totalitario.

Non fermarsi mai. Non oziare. Non perdere tempo. Non pensare, non approfondire, non studiare. Copia e incolla invece di ragionamento (e oggi internet come *la più grande fotocopiatrice della storia*, secondo Franklin Foer). **Superficialità invece di conoscenza. Efficienza invece di efficacia. Irresponsabilità invece di responsabilità** (avendo perduto il *senso del fare*, tutti mobilitati a *fare prescindendo dal pensare*).

Mobilitazione totale e quindi: **Ernst Jünger**. Mobilitazione che avviene *quando tutte le parti del sistema vengono attivate e soprattutto integrate/connesse e sincronizzate in vista della realizzazione di uno scopo*. Che allora (anni Trenta), perJünger era in primo luogo quella bellica: "Così, anche **l'immagine della guerra come di un'azione armata sfuma sempre più nell'immagine ben più ampia di un gigantesco *processo di lavoro***. Accanto agli eserciti che si affrontano sui campi di battaglia sorgono *eserciti di nuovo tipo, l'esercito dei trasporti, dell'approvvigionamento, dell'industria degli armamenti: in generale, l'esercito del lavoro*. (…) Per dispiegare energie di questa misura non è più sufficiente armare il braccio che porta la spada: è necessario essere *armati* fino nelle midolla, fino nel più sottile *nervo vitale*.

Porre in essere quelle energie è il compito della mobilitazione totale, di un atto cioè attraverso il quale è possibile, *impugnando un unico comando* su di un quadro di controllo, far confluire la *rete d'energie – tanto ramificata e diffusa – della vita moderna, nella grande corrente dell'energia bellica*" (corsivi nostri). Una *mobilitazione totale* che non tanto viene *eseguita*, "quanto piuttosto essa stessa *si esegue*: in pace e in guerra è l'espressione di una *misteriosa e cogente esigenza*, a cui *siamo sottomessi da questo vivere nell'epoca delle masse e delle macchine*.

Il web, nuovo inconscio collettivo

Si perviene così al risultato che ogni singola vita diventa sempre più inequivocabilmente una *vita di operaio*…". E nel libro *L'operaio*, Jünger aggiungeva: "questa mobilitazione totale distrugge tutto ciò che ostacola questa mobilitazione. **Dietro i processi di trasformazione tecnica, quali appaiono in superficie, traspaiono una diffusa distruzione e una costruzione del mondo in forme diverse**; [ma] entrambe procedono in una determinata direzione" e questa *forma dell'operaio* "mobilita, senza distinzioni, l'intera condizione umana". Ebbene, se questa è la *mobilitazione totale* (tanto simile – nel suo *eseguirsi sulla base di una misteriosa ma cogente esigenza* - al concetto di autopoiesi, dove **il *soggetto ordinatore è oggetto dell'ordine da esso stesso prodotto*** – oppure, *usando* Ferraris, **questa *cogenza* è imposta dal web come nuovo *inconscio collettivo***), questa è la condizione normale, normata, normalizzata della vita umana in tempo di rete e di globalizzazione. *Che mobilita distruggendo, che distrugge mobilitando* (ancora: **dalla *distruzione creatrice* alla *disruption***). Irresponsabilmente, ma in mobilitazione totale: che è a sua volta una delle forme peggiori di alienazione.

La *mobilitazione totale* si integra quindi (è possibile solo) con la *società di massa* (meglio ancora: con la *società in forma di folla/sciame* – cioè "**insiemi di unità autopropulsive unite solamente da una *unità meccanica* che si manifesta replicando schemi di condotta simili e muovendosi in direzione analoga**" - Bauman), attivandosi reciprocamente e generando una nuova forma di *società (auto)amministrata* (ma sempre sotto il *comando*, ormai introiettato del sistema tecno-capitalista), evoluzione o involuzione di quella *società amministrata* criticata dai francofortesi.

Aggiungeva ancora Zygmunt Bauman: "Per gli individui di oggi, l'unico scopo di essere in movimento è restare in movimento. Se un tempo il cambiamento era un'operazione pensata in vista di certe esigenze, un mezzo per un fine, è invece un fine in se stesso per gli individui di oggi, i quali si aspettano di vederlo *continuare perpetuamente* (…) **Sono in movimento perché in movimento devono stare. Si muovono perché non possono fermarsi.** Come le biciclette, stanno dritti solo quando corrono. Ed è come se seguissero il precetto di Lewis Carroll: "**Qui, vedi, per star fermi bisogna correre più che si può**" (in *Adorno e la globalizzazione*, MicroMega, novembre 2003).

Mobilitazione totale ("Non siamo in guerra, ma siamo mobilitati più che in ogni altro tempo" – concorda Ferraris), dove ciascun membro della *massa individualizzata* e dell'*organizzazione totalitaria della sua mobilitazione* è attivato (**dal marketing e dall'organizzazione del lavoro, dai social e dalle community, dal *dover condividere* e dal *dovere di essere sempre connessi***) a mobilitarsi, ciascuno incorporando/introiettando (*la misteriosa e cogente esigenza*) il *dovere* di mobilitarsi, oggi **connettendosi in rete, per produrre, consumare, innovare, generare dati**. Permettendo alla mobilitazione di *eseguirsi*. E nessuno si ribella, nessuno cerca alternative per uscire da questa totale dis-umanizzazione/post-umanizzazione/alienazione.

Digital transformation, da soggetti a oggetti della mega-macchina

E se la tecnica veniva accusata di essere *spaesante* (Heidegger) è vero piuttosto che **il tecno-capitalismo è il primo totalitarismo moderno** (ed è *vincente* proprio per questo) che si fonda sull'esaltazione dell'individuo atomizzato e solistico nella sua assoluta libertà (appunto, *contano solo gli individui, la società non esiste*), nel suo narcisismo e nel suo pigmalionismo. **Il tecno-capitalismo è quindi diverso dai totalitarismi del Novecento che invece annullavano/azzeravano l'individuo nella massa** (*privando l'individuo del proprio io*, come sottolineava Hannah Arendt): perché assoggetta/subordina/sussume l'individuo a sé, **lo trasforma da soggetto in oggetto/parte funzionale della sua mega-macchina**, ma lo fa in nome della libertà dell'individuo, *esaltando il suo io*, per assoggettarlo meglio - **nessuno opponendosi a un sistema che *promette* la massima libertà.**

Geniale, dal punto di vista biopolitico e ideologico e di costruzione di un sistema totalitario. Il tecno-capitalismo individualizza/personalizza, separa e isola, de-socializza, **per poi produrre esso stesso le forme di compensazione emotiva per far sentire l'individuo meno solo**. Un individuo frantumato e suddiviso, messo al lavoro in mobilitazione totale, monade alienata ed egoista/narcisista nella realtà reale ma portato poi a far parte *felicemente* di un social, di una community, di una comunità nazionale (il populismo/sovranismo), di una comunità di lavoro, tutto basato su quella parola magica che si chiama ***condivisione***.

Ancora il *doppio movimento della psicologia umana*, messo a profitto per il capitale e per costruire il *totalitarismo della società tecnologica avanzata*. Con tutti che aderiscono liberamente all'organizzazione, *sciogliendo/azzerando se stessi come soggetti* ma in nome di una promessa di *massima soggettivazione*. È - appunto - il totalitarismo perfetto.

Remo Bodei: la tecnica produttrice di ordine e disciplina

Come scriveva Remo Bodei, per Jünger (e diversamente da Heidegger) "**la tecnica diventa, essa stessa, produttrice di ordine, di disciplina, di compattezza**. Proprio perché la tecnica non produce alcun effetto di *spaesamento* o di *spersonalizzazione*, ma al contrario un forte senso di

appartenenza alla comunità - gerarchicamente concepita secondo il modello dell'esercito – uomini e macchine possono non solo coesistere, ma crescere simbioticamente". *Coincidere*. Secondo il modello ieri dell'esercito, per Jünger; oggi secondo quello dell'impresa. **Per Heidegger, comunque la potenza della tecnica – *che incalza, trascina, avvince l'uomo* – "è cresciuta a dismisura e oltrepassa di gran lunga la nostra volontà, la nostra capacità di decisione, perché non è da noi che procede"**; eppure "i risultati della tecnica, il suo progresso sempre più veloce vengono *ammirati* da un pubblico vastissimo". Ciò che allora è inquietante "è che non siamo ancora capaci di raggiungere, attraverso un *pensiero meditante*, un confronto adeguato con ciò che sta realmente emergendo nella nostra epoca", cioè lo strapotere della tecnica (e del capitalismo).

La via di uscita: de-coincidenza/dissidenza. Ma sarà così?

Nella *società di massa* e nella *mobilitazione totale*, **ciascuno deve *sciogliere se stesso* nella massa, nell'organizzazione che mobilita e che lo attiva**, deve essere *funzionale per* e *congruo* (Anders) *con* il funzionamento del sistema. **Deve farsi *utile e docile* (Foucault)**. Deve *identificarsi/coincidere* con ciò che lo mobilita e con ciò che gli offre compensazioni emotive di comunità e di felicità via consumismo, dopo averlo deprivato/alienato anche di relazioni umane e di responsabilità/consapevolezza.

Ciascuno deve cioè praticare solo *un pensiero calcolante* (tecnica e capitalismo, di nuovo e la loro *razionalità calcolante/strumentale*) *e non meditante* (Heidegger); deve farsi prima *appendice delle macchine* e ora *ibridarsi con la tecnica*. **Deve cioè *coincidere* con la tecnica e con il sistema di mercato** (questo volevano e vogliono i neoliberali e gli anarco-capitalisti della Silicon Valley: far *coincidere* mercato e tecnica con la società, e viceversa), deve *ibridarsi/sussumersi* con il sistema post-umano tecno-capitalista e con il suo immaginario/industria culturale-spettacolare.

Ma se questo è vero, ed è vero, allora la libertà dell'individuo (quella vera, non quella fabbricata e venduta dal sistema), va cercata proprio *de-coincidendo* e *dis-alienandosi* dalla logica irrazionale e dal pensiero calcolante e competitivo del sistema. **La libertà dell'individuo va cercata *dis-adattandosi* da un sistema che ci chiede solo di *adattarci/coincidere* con le sue esigenze**. E poiché la rivoluzione industriale è incessante, incessante deve essere anche il nostro *adattamento* e il nostro *coincidere*. Ma *adattarsi/coincidere/ibridarsi/sussumersi* è negarsi come individui, come *soggetti*. *Adattarsi* significa infatti alienarsi (asservimento volontario? conformistico?) da un *pensiero meditante*, che invece ci chiede *di non restare attaccati in maniera unilaterale ad un'unica rappresentazione* (Heidegger, ancora) della realtà.

Ad aiutarci a *de-coincidere* e a *dis-adattarci* dall'apparato, dalla massa, dalla mobilitazione totale, recuperando una capacità di libertà e di pensiero, c'è l'ultimo, bellissimo libro del filosofo-sinologo François Jullien che scrive: "De-coincidenza è un concetto in grado di esprimere la vocazione dell'arte ma anche – in primo luogo – dell'esistenza. Se de-coincidere implica l'uscita dall'adeguamento a un sé, dal proprio adattamento a un mondo, allora significa propriamente *esistere* (…) che rimanda letteralmente al *tenersi fuori*: ciò significa in primo luogo fuori dall'adeguamento-adattamento che, cumulandosi, ostruiscono; che, saturandosi, non lasciano spazio per il futuro e per inventarsi. (…) **Di conseguenza, è tramite la de-coincidenza che si sviluppa la libertà**", ossia "aprendo una breccia nella normalità acquisita (nella sua funzionalità ammessa), insomma **osando uno scarto (…) per far emergere l'esistenza**".

La porta stretta: allontanarsi dai processi

L'uomo così *dis-adattandosi*, cioè uscendo dalla massa ("dal gruppo e dal gregariato" e, aggiungiamo: dal neoliberalismo e dal determinismo tecnico che producono massificazione e *coincidenza*), "prendendo le distanze dalla totalizzazione e dall'integrazione che fanno mondo", quindi *scartando* dalla mobilitazione che invece chiede adattamento e *coincidenza* (o altrimenti: funzionalità, congruità, conformazione). **"La coincidenza mantiene nell'adeguamento" - è l'adeguatezza, certo, ma è anche la paralisi, la conformità, l'impasse: la morte di ogni iniziativa e di ogni accenno di cambiamento**. Mentre è solo dalla *de-coincidenza* (che è un *processo*, non un atto singolo) – disfacendo continuamente la *coincidenza/funzionalità* acquisita o fatta acquisire/introiettare – "che procede il fenomeno stesso della vita in quanto è vivente", *arrischiandosi al di fuori del proprio adattamento*. In quanto rinnovamento/distacco da ciò che è abitudine/coincidenza, la *de-coincidenza* e il *dis-adattamento* (che sono l'*essenza vera* – per Jullien - della vita umana e della libertà) sono cosa tutta diversa dalla ***distruzione creatrice/disruption*** **e dalla *mobilitazione totale*, che producono invece la totalitaria *coincidenza/identificazione* di tutti con l'insieme.**

Il problema – *e che problema!* - è che il tecno-capitalismo è esso stesso produttore incessante di *de-coincidenza*. Come di illusioni di libertà, di *esistenza*, di creatività. Certo è una *de-coincidenza* illusoria perché funzionale alla *attivazione* eteronoma del lavoro umano, della *massificazione individualistica*, della *mobilitazione* di tutti nella produzione/consumo. **Il totalitarismo tecno-capitalista *de-coincide* incessantemente se stesso** (attraverso la competizione e la *distruzione creatrice/disruption* come *forme* e *norme* della sua *volontà di potenza/accrescimento*) e ciascuna delle sue *parti* da se stesse ma non dall'apparato (è la *flessibilizzazione* incessante del sistema), uomini compresi. Tutto per far meglio *coincidere* ciascuna parte a sé e con sé come apparato; e *mobilitare* ciascuno alla sua massima capacità di *coincidenza con il sistema de-coincidente* (la sua *dynamis* lo richiede), così come *individualizza* per *integrare* meglio ciascuno nel proprio sistema.

Perché allora vi sia vera *de-coincidenza* (e la riflessione di Jullien è decisamente affascinante) e (aggiungiamo) *dis-alienazione* – e quindi **libertà, soggettività, autonomia dell'uomo** - occorre soprattutto **imparare a *de-coincidere* dalla falsa ma affascinante *de-coincidenza* e *dis-alienazione* incessantemente prodotta dal sistema per la propria riproducibilità (e coincidenza/adattamento) infinita**.

De-coincidere, ovvero e altrimenti, con José Saramago: "non puoi sapere chi sei se non esci da te stesso"; e "non ci vediamo" – cioè non possiamo conoscere noi stessi – "se non ci allontaniamo da noi stessi". **Così come non vediamo i processi (soprattutto tecnici) in cui siamo inseriti se non ci allontaniamo da essi, guardandoli criticamente. Per *governarli consapevolmente*.**

Bibliografia di riferimento

Adorno T.W. (2010), *La crisi dell'individuo*, Diabasis, Reggio Emilia

Arendt H. (2004), *Le origini del totalitarismo*, Einaudi, Torino

Bartolini P. – Consigliere S. (2019), *Strumenti di cattura. Per una critica dell'immaginario tecno-capitalista*, Jaca Book, Milano

Bauman Z. (2018), *Retrotopia*, Laterza, Roma-Bari

Bauman Z. (2008), *Consumo, dunque sono*, Laterza, Roma-Bari

Benasayag M. (2019), *Funzionare o esistere?*, Vita e pensiero, Milano

Boarelli M. (2019), *Contro l'ideologia del merito*, Laterza, Roma-Bari

Bodei R., *Introduzione* a Adorno T. W. (2006), *Il gergo dell'autenticità*, Bollati Boringhieri, Torino

Borgognone G., *voce*: *Società di massa*, in Bobbio N., Matteucci N., Pasquino G. (2004), *Il Dizionario di Politica*, Utet, Torino

Chicchi F. (2017), *La società della prestazione*, Ediesse, Roma

Codeluppi V. (2007), *La vetrinizzazione sociale*, Bollati Boringhieri, Torino

Davies W. (2019), *Stati nervosi*, Einaudi, Torino

Davies W. (2016), *L'industria della felicità*, Einaudi, Torino

Del Rey A. (2018), *La tirannia della valutazione*, Elèuthera, Milano

Demichelis L. (2018), *La grande alienazione. Narciso, Pigmalione, Prometeo e il tecno-capitalismo*, Jaca Book, Milano

Demichelis L. (2017), *Sociologia della tecnica e del capitalismo*, FrancoAngeli, Milano

Ferraris M. (2015), *Mobilitazione totale*, Laterza, Roma-Bari

Galimberti U. (2018), *Nuovo Dizionario di Psicologia*, Feltrinelli, Milano

Gallino L. (2007), *Il lavoro non è una merce*, Laterza, Roma-Bari

Gallino L. (1993), *Dizionario di Sociologia*, Utet, Torino

Heidegger M. (2006), *L'abbandono*, il Melangolo, Genova

Horkheimer M. (1979), *La società di transizione*, Einaudi, Torino.

Jullien F. (2019), *Il gioco dell'esistenza. De-coincidenza e libertà*, Feltrinelli, Milano

Jünger E. (1985), *La mobilitazione totale*, ne: Il Mulino nr. 301, il Mulino, Bologna

Jonas H. (1990), *Il principio responsabilità*, Einaudi, Torino

Marcuse H. (1993), *L'uomo a una dimensione*, Einaudi, Torino

Rosa H. (2015), *Accelerazione e alienazione*, Einaudi, Torino

Saramago J. (2015), *Il racconto dell'isola sconosciuta*, Feltrinelli, Milano

Zagrebelsky G. (2015), *Liberi servi*, Einaudi, Torino

L'impronta ambientale dell'ICT: ecco l'impatto dei nostri device sul Pianeta

Depauperamento di risorse non rinnovabili, riscaldamento globale, inquinamento: la rivoluzione digitale, con i suoi Pc, dispositivi elettronici e infrastrutture ICT, ha un impatto sull'ambiente che molti di noi neanche immaginano. Una panoramica su tutte le problematiche connesse

Di Giovanna Sissa, Università degli Studi di Genova, DITEN

I dispositivi ICT che circondano la nostra vita, in modo visibile o invisibile, ad uno sguardo superficiale **possono apparire come privi di effetti sull'ambiente**. Quando si accende un computer o uno smartphone non si vede fumo, né polvere, non c'è cattivo odore. Non si osserva, si annusa, si tocca o si percepiscono inquinamento o calore. **Nessuna sensazione soggettiva è però più sbagliata.**

I tre principali impatti dei device sull'ambiente

I computer, siano desktop, laptop o server, gli smartphone e i tablet come i router o tutti i dispositivi del settore telecomunicazioni, i sensori e attuatori connessi ad Internet dell'universo IoT, come tutti i dispositivi ICT, grandi o piccoli, individuali o collettivi, usati in cloud o in locale, **hanno effetti sull'ambiente che si possono raggruppare in tre categorie principali.** Contribuiscono;

- al **riscaldamento** globale,
- **all'inquinamento**
- al **depauperamento delle risorse limitate** (quali ad esempio alcuni minerali).

Qualche considerazione generale può quindi servire a inquadrare il problema ambientale, anche per quanto riguarda il settore ICT:

- Le **emissioni di gas serra** (spesso definite CO2 equivalenti) sono responsabili del riscaldamento globale;
- L'inquinamento è responsabile del **degrado dell'ambiente** derivante da uso di sostanze che contaminano acqua, aria o suolo;
- **L'uso indiscriminato di risorse** – come ad esempio molti minerali – che sono limitate sul pianeta (anche se presenti in grande quantità) è **insostenibile** per il futuro del pianeta.

Costruire un dispositivo ICT richiede una notevole quantità di combustibili fossili, materiali (anche tossici), minerali rari, acqua. Una parte dell'impatto ambientale si ha nell'estrazione delle materie prime e nella fabbricazione dei componenti, che comporta anche un forte utilizzo di energia elettrica.

I dispositivi finali vengono trasportati per lunghe distanze, in imballaggi consistenti che andranno poi smaltiti. Server, computer, monitor, data center, infrastrutture di comunicazione e relativi sottosistemi **consumano una grande quantità di energia nel loro funzionamento**: l'incremento della richiesta energetica contribuisce al riscaldamento globale. Inoltre lo smaltimento a fine vita ha un forte impatto ambientale: può essere inquinante e pericoloso.

Quanto pesa l'ICT sull'ambiente?

Depauperamento di risorse non rinnovabili, riscaldamento globale, inquinamento: questi termini indicano aspetti diversi dell'impatto ambientale: non sono sinonimi e non sono intercambiabili. Hanno ovviamente punti di contatto e correlazioni, che si possono sintetizzare nell'idea che ogni dispositivo artificiale lascia sulla terra un'impronta che descrive gli effetti che tale dispositivo ha avuto nel corso di tutta la sua vita sull'ecosistema.

Computer, dispositivi elettronici e infrastrutture ICT consumano quantità significative di elettricità, mettendo un pesante fardello sulle nostre reti elettriche e contribuendo alle emissioni di gas serra. Nel 2008 l'ICT ha contribuito per il 2% delle emissioni globali di CO2, nell'ultimo decennio tale contributo è triplicato e si stima che nel 2040 si arriverà al 14% (a fronte di un contributo del 20% del settore trasporti, sostanzialmente stabile nel tempo). **Ad aumentare il proprio impatto sono soprattutto gli smartphone, dato il tasso di crescita e la rapidità di sostituzione**. Ma come si arriva a queste quantificazioni?

Gli indicatori

Esistono vari indicatori che fanno capo alla cosiddetta ***Footprint Family***, ovvero alla famiglia di indicatori che si basano sul concetto di impronta, a sua volta legato al concetto di **appropriazione delle risorse naturali.** Senza entrare nei dettagli delle definizioni o metriche che le scienze ambientali hanno elaborato – definizioni e metriche che non è immediato applicare all'ICT - ci concentriamo sull'**Impronta Ecologica** (*Ecological Footprint*) e sull'**Impronta di Carbonio** (*Carbon Footprint),* due indicatori che monitorizzano aspetti diversi e complementari l'uno con l'altro.

L'**impronta ecologica** è un indicatore complesso utilizzato per valutare il consumo umano di risorse naturali rispetto alla capacità della Terra di rigenerarle. L'impronta ecologica **misura l'area biologicamente produttiva di mare e di terra necessaria a rigenerare le risorse consumate da una popolazione umana e ad assorbire i rifiuti prodotti**. Utilizzando l'impronta ecologica è possibile stimare quanti "pianeta Terra" servirebbero per sostenere l'umanità, qualora tutti vivessero secondo un determinato stile di vita.

La **carbon footprint** (letteralmente, "impronta di carbonio") è un parametro che viene utilizzato per **stimare le emissioni gas serra** (d'ora in poi GHGs – GreenHouse Gases) causate da un prodotto, da un servizio, da un'organizzazione, da un evento o da un individuo, espresse generalmente in *tonnellate di CO2 equivalente*. Tale parametro può essere utilizzato per la determinazione degli impatti ambientali che le emissioni hanno sui cambiamenti climatici di origine antropica. La produzione di energia elettrica, particolarmente rilevante nella fase d'uso dell'ICT, viene espressa in termini di GHGs.

Life Cycle Assessment

Gli impatti ambientali devono essere considerati lungo l'intero ciclo di vita. Nell'ambito dei processi produttivi, ogni unità di prodotto genera un impatto lungo la sua intera filiera, di cui il cliente finale è in qualche modo il "responsabile" in quanto causa della domanda di quel bene medesimo. Il Life Cycle Assessment, è la metodologia per individuare e quantificare **i carichi ambientali complessivi di un prodotto "from cradle to grave" (dalla "culla alla tomba")**.

Il ciclo di vita del prodotto è costituito da varie fasi: l'estrazione di materie prime, la produzione, il trasporto, l'utilizzo del prodotto e il suo fine vita.

La produzione di dispositivi ICT è ad alta intensità energetica e materiale; i combustibili fossili utilizzati per realizzare un computer desktop tradizionale pesavano circa 10 volte il peso del desktop stesso. **Questo rapporto per i dispositivi ICT è alto rispetto a molti altri beni materiali artificiali**: per un'automobile o un frigorifero, ad esempio, il peso dei combustibili fossili utilizzati per la produzione è all'incirca uguale al loro peso.

Perché l'uso delle materie prime dovrebbe essere relativamente alto per i dispositivi a semiconduttore? La spiegazione fondamentale sta nella **termodinamica.** I microchip e molti altri prodotti high-tech sono forme di materia estremamente bassa ed entropicamente organizzate. Poichè vengono fabbricati usando materiali di partenza ad entropia relativamente alti, è naturale aspettarsi che sia necessario un **notevole investimento di energia e materiali di processo per la trasformazione in una forma organizzata**.

Il costo dell'hardware discende proprio dai *processi hi-tech lunghi,* per la trasformazione dalle materie prime ai componenti del computer (e da essi alle parti del computer e poi all'oggetto finale). Il costo di un computer dunque è costituito solo in minima parte dal valore delle materie prime che lo costituiscono. Il suo valore è costituito dai componenti hi-tech al suo interno, ovvero dall'hardware e, in misura sempre più crescente, dal software. Almeno fino a quando il computer è in esercizio.

Quando viene dismesso (sia esso ancora funzionante o meno) e diventa "rifiuto" il suo valore decresce drasticamente, perché **l'unica componente che ne rimane è l'hardware**. Può essere recuperata, nella migliore delle ipotesi, qualche scheda o componente – dipende dall'economicità e dai margini di guadagno possibili.

Mediante il riciclo si possono, dopo una serie di processi di trattamento, recuperare le materie prime secondarie [1] che lo compongono, da riutilizzare nuovamente nella produzione. Se la struttura interna dei dispositivi ICT è complessa, il recupero, mediante riciclo, delle materie prime secondarie è proporzionale alla complessità nella fase di costruzione; questo rende **il corretto smaltimento un processo multifase, lungo e costoso.**

Il trattamento del computer come rifiuto elettronico è dunque un processo articolato, costoso che, se non fatto in sicurezza, può essere anche inquinante e pericoloso.

Il fine vita ha un forte impatto ambientale: i componenti e più in generale i dispositivi ICT, contengono molte sostanze tossiche e se gettati nelle discariche o non trattati adeguatamente provocano all'ambiente e alla salute danni irreparabili.

eWaste

E-waste è un termine informale che indica i prodotti elettronici quando sono prossimi alla fine del loro ciclo di vita ed è uno dei segmenti della filiera dei rifiuti solidi che cresce più rapidamente. **In Europa cresce del 3%-5% l'anno, tre volte più in fretta dei rifiuti in generale.**

Il numero di dispositivi ICT è aumentato in modo vertiginoso in paesi come Cina e India, dove centinaia di milioni di nuovi utenti hanno trasformato il mondo ICT, sia lato consumer che producer.

Già nel 2006, si stimava che in Europa erano stati prodotti 8-12 milioni di tonnellate di rifiuti elettronici. I rifiuti elettronici rappresentano oggi una porzione di tutti i rifiuti solidi urbani: è circa la stessa percentuale degli imballaggi in plastica, ma i rifiuti elettronici sono molto più pericolosi e crescono, come si è detto, a un tasso elevatissimo. Ma i paesi in via di sviluppo hanno moltiplicato la loro produzione di rifiuti elettronici in modo molto più elevato.

C' è inoltre un lato oscuro, formalmente vietato, e ancora con molte zone d'ombra: **lo smaltimento non a norma, scorretto, mal tracciato, o illegale verso paesi del terzo mondo** dove intere regioni o città, ad esempio dell'Africa, sono diventate discariche a cielo aperto in cui ambiente e salute delle persone sono compromesse.

In parallelo alcune zone del mondo non coinvolte fino a poco tempo fa nel settore ICT diventano improvvisamente epicentro di nuove sfide tecnologiche, come nel caso delle *server farm* dedicate al mining dei bitcoin. **Nuove problematiche, di tipo ambientale, si affiancano così alle preesistenti.**

L'Europa e i RAEE

I rifiuti elettronici nella normativa normativa internazionale e nazionale sono associati anche ai rifiuti di apparecchiature elettriche come WEEE (Waste Electrical & Electronic Equipment), che in Italia vengono chiamati RAEE (**Rifiuti di apparecchiature elettriche ed elettroniche**). I dati, come la legislazione, sono riferiti ai RAEE nel loro complesso. Sono suddivisi in cinque gruppi, di cui il *Gruppo 4* comprende i dispositivi ICT. Non è immediato dunque conoscere le percentuali effettive di smaltimento a norma dei dispositivi ICT e ancora meno delle singole tipologie di dispositivo.

L'Unione Europea ha introdotto due atti legislativi specifici:

- la direttiva sui rifiuti di apparecchiature elettriche ed elettroniche (**direttiva WEEE**)
- la direttiva sulla restrizione dell'uso di determinate sostanze pericolose nelle apparecchiature elettriche ed elettroniche (**direttiva RoHS**).

La prima direttiva WEEE (direttiva 2002/96/CE), entrata in vigore nel febbraio 2003, ha definito la creazione di **sistemi di raccolta** in cui i consumatori restituiscono i loro WEEE gratuitamente, mirando così ad aumentare il riciclo dei WEEE e/o il riutilizzo. Nel dicembre 2008, la Commissione europea ha proposto di rivedere la direttiva al fine di affrontare il rapido flusso di rifiuti in aumento e la nuova direttiva WEEE 2012/19/UE ed è entrata in vigore il 14 febbraio 2014.

La legislazione dell'UE che limita l'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche (Direttiva RoHS 2002/95/CE) è entrata in vigore nel febbraio 2003: prevede che **metalli pesanti e ritardanti di fiamma siano sostituiti con alternative più sicure**. La direttiva è stata poi rivista (RoHS 2011/65/UE) ed è entrata in vigore il 3 gennaio 2013.

L'idea guida è **responsabilizzare le industrie del settore**, invitandole a **progettare in maniera ecocompatibile**, limitando l'utilizzo degli inquinanti. I principi di **design for the environment** prendono in considerazione già nella fase di progettazione gli aspetti ambientali e i costi correlati alla gestione dei beni a fine vita, per facilitare smaltimento e riciclo dei prodotti.

Per promuovere l'introduzione di una progettazione che tenga conto dell'ambiente devono essere gli stessi **produttori** di apparecchiature hi-tech a pagare i costi della raccolta, recupero e smaltimento, senza accollare tout court i costi aggiuntivi al consumatore.

La prospettiva di doversi fare carico economicamente della gestione del fine vita dovrebbe responsabilizzare le industrie e indurle a produrre apparecchiature meno pericolose e più facili da smaltire o recuperare. L'idea ispiratrice è sintetizzabile con "chi inquina paga".

Si cerca di far desistere il consumatore dalla "**tentazione del cassonetto**", delegando al produttore la responsabilità economica dello smaltimento e imponendo ai distributori il principio del "vuoto a rendere".

La riduzione degli impatti ambientali viene ridotta anche grazie a:

- la definizione di **obiettivi minimi di riuso**, riciclo e recupero dei WEEE;
- l'introduzione dell'**obbligo della raccolta differenziata** per i WEEE;
- l'introduzione del **divieto di smaltimento in discarica** dei WEEE che non siano preventivamente stati sottoposti a trattamento.

Attuazione della normativa Europea negli Stati membri

La direttiva WEEE (con la sua complementare RoHS), secondo il principio di sussidiarietà, stabilisce i requisiti generali cui ogni Stato membro europeo deve attenersi nell'adottare le proprie regole di applicazione; a esso sono lasciate le modalità logistiche e organizzative. Di conseguenza **ci sono sistemi diversi nei vari Stati membri**. Alcuni (come il Belgio, la Svezia, la Danimarca o i Paesi Bassi) avevano già una normativa e un sistema organizzativo per il WEEE prima che la direttiva entrasse in vigore. Tali sistemi riflettevano le diverse situazioni e filosofie nazionali e hanno dovuto adeguarsi alla direttiva. Altri Paesi membri hanno invece sviluppato una regolamentazione e un sistema di gestione per conformarsi alla direttiva.

Ci sono **due modelli di sistema di gestione: quello collettivo e quello competitivo.**

Il sistema nazionale collettivo (o monopolio) è un sistema nazionale responsabile di raccolta, riciclo e relativo finanziamento a livello nazionale. Al primo modello si ispirano gli Stati elencati, che avevano già prima un proprio sistema di gestione WEEE.

Il sistema della "competitive clearing house" invece è un quadro di riferimento nazionale in cui più partner (produttori, riciclatori e organizzazioni che si occupano di rifiuti) erogano servizi. Il governo assicura che ci sia un registro dei produttori e definisce dei meccanismi di allocazione e monitoraggio. Un ente nazionale di coordinamento garantisce la corretta allocazione delle quote sul territorio. Il principale motivo per l'adozione di questo modello è evitare una situazione di monopolio e diminuire i costi. Specialmente gli stati più grossi hanno optato per questo secondo modello e in tali stati, fra cui l'Italia, molti soggetti sono entrati nel meccanismo del trattamento RAEE.

Obsolescenza: reale o indotta?

Perché la filiera dei rifiuti dell'ICT è fra quelle in maggior crescita? Una ragione consiste nel fatto che la durata dei prodotti è in diminuzione, poiché i prodotti diventano obsoleti a causa di obsolescenza prematura (a volte programmata) o di smaltimento premature (di un prodotto funzionante).

Una grande parte dei prodotti viene sostituita anche se sono ancora funzionanti per varie ordini di ragioni: fattori emotivi e sociali, fattori materiali, funzionali psicologici ed economici influenzano congiuntamente la durata del prodotto, in interazione con l'innovazione dei produttori e le strategie di mercato e le possibilità e gli ostacoli alla riparazione e aggiornabilità.

Dal punto di vista ambientale ed economico, la riduzione della durata del prodotto è allarmante. La produzione consuma risorse preziose con un'impronta ambientale elevata, e dopo una vita relativamente breve, lo smaltimento delle merci spesso inquina l'ambiente a causa della mancanza di riciclo o approcci *from cradle to grave* adeguati. **La tracciabilità della filiera - dalla dismissione al trattamento finale - e la quantificazione dei processi di smaltimento sono importantissimo**. Gli impianti per il corretto trattamento del rifiuto elettronico sono ad alta innovazione e costosi.

Inoltre, c'è un dibattito acceso su "obsolescenza pianificata o programmata", in particolare sulla sua definizione e sui relativi impatti. Nel settore ICT il software gioca un ruolo importantissimo, come vedremo in seguito. C'è **scarsa fiducia** dei consumatori: uno studio di un'associazione di consumatori francese ha rilevato che il 92% degli intervistati ritiene che i prodotti elettrici o di alta tecnologia sono deliberatamente progettati per non durare.

Conclusione

Fin qui abbiamo analizzato le responsabilità ambientali dei dispositivi dell'universo ICT nelle fasi di inizio e fine vita. La fase di uso è responsabile delle emissioni di gas serra e dunque contribuisce al riscaldamento globale e lo fa in maniera considerevole e crescente data la pervasività di Internet. Oltre all'uso dei dispositivi connessi, quali appunto computer e smartphone, anche i data center, e tutti gli apparati relativi al funzionamento di Internet hanno un peso.

Nella seconda parte affronteremo dunque l'impatto dell'ICT nella fase d'uso, cercando anche di quantificarne gli aspetti più eclatanti – come l'uso enorme di energia nei sistemi di criptomoneta - per passare poi ad analizzare le soluzioni innovative su cui la ricerca sta lavorando per mitigare tali effetti e come le tendenze del settore ICT si colleghino anche agli impatti ambientali, talvolta in modi imprevisti.

BIBLIOGRAFIA

- Lotfi Belkhir, Ahmed Elmeligi, (2018). Assessing ICT global emissions footprint: Trends to 2040 & recommendations, Journal of Cleaner Production, Volume 177, Pages 448-463, https://doi.org/10.1016/j.jclepro.2017.12.239

- Durand, Pascal (2017). “REPORT on a Longer Lifetime for Products: Benefits for Consumers and Companies.” (2016/2272(INI)), Committee on the Internal Market and Consumer Protection, Rapporteur: Pascal Durand.
- GeSI (2015). Global e-Sustainability Initiative, "#SMARTer2030-ICT Solutions for 21st Century Challenges. Accent.

- GeSI (2012) BCG SMARTer2020, 2012. SMARTer2020: the Role of ICT in Driving a Sustainable Future
- United Nations (2015). UN Department of Economic and Social Affairs: http://www.un.org/en/development/desa/population/theme/trends/index.shtml
- OECD (2010). *Greener and smarter – ICTs the environment and climate change*. Paris, France: OECD.
- G. Sissa (2008). Il computer sostenibile, Franco Angeli editore, Milano
- Gesi Group (2008). *Smart 2020: Enabling the low carbon economy in the information age*
- Kuehr, R., & Williams, E. (2003). *Computers and the environment: Understanding and managing their impacts*. Dordrecht, The Netherlands: Kluwer Academic Publisher.
- Williams, E. D., Ayres, R. U., & Heller, M. (2002). The 1.7 kilogram microchip: energy and material use in the production of semiconductor devices. Environmental Science & Technology, 36, 5504–5510. doi:10.1021/es025643o

1. Materia Prima Seconda (o Secondaria): quando non sono più necessari ulteriori trattamenti perché le sostanze, i materiali e gli oggetti ottenuti possono essere usati in un processo industriale o commercializzati come materia prima secondaria. ↑

Gli effetti del cyberbullismo su vittime e carnefici: tutte le sfaccettature del fenomeno

Nuove escalation e scenari per gli attacchi tra ragazzi sferrati con il supporto delle tecnologie. Più diluito il confine tra vittima e carnefice. Non solo: anche gli "spettatori" sono coinvolti in dinamiche negative che possono protrarsi a lungo termine. Un'analisi del panorama alla luce degli studi più recenti

Di Ivan Ferrero, Psicologo delle nuove tecnologie

Quando parliamo di **cyberbullismo** non possiamo non parlare dei suoi effetti, e nell'analisi delle conseguenze tendiamo a focalizzarci su chi subisce il gesto. Tuttavia sono sempre più le ricerche che ci indicano che **le conseguenze di questo fenomeno coinvolgono anche chi commette il gesto**, e non solo: **anche chi assiste ne viene colpito.**

Il cyberbullismo si rivela spesso la **naturale estensione di un bullismo che sta già avvenendo offline**. In questo caso i ragazzi coinvolti si conoscono, ed esiste un gruppo a conoscenza del fenomeno, anche se non tutti vi hanno partecipato direttamente (né come attori e né come spettatori).

Questo fa del cyberbullismo un fenomeno che va al di là della semplice, e ormai superficiale, distinzione tra vittima e carnefice. Le ricerche infatti ci indicano che il Cyberbullismo è un fenomeno di gruppo, per il quale è necessario andare oltre le distinzioni a cui il bullismo tradizionale ci ha abituati. Il tema del Cyberbullismo è ormai entrato nel nostro immaginario collettivo, permeando il tessuto del nostro sociale.

Il costante abbassamento dell'età in cui **le nuove generazioni hanno accesso ad uno smartphone indipendente dal controllo dei loro genitori** comporta la costante crescita di questo fenomeno. **La varietà di formati offerta da una miriade di applicazioni e di piattaforme comporta inoltre il ramificarsi e il differenziarsi di questo fenomeno**.

Se infatti fino a qualche anno fa aveva ancora senso parlare di un Cyberbullismo generalizzato, **ultimamente sono nate numerose sfaccettature spesso così differenti l'una dall'altra, che ognuna di loro merita un'analisi ad hoc.** In questo articolo quindi tratterò quel **Cyberbullismo che avviene tra ragazzi adolescenti che si conoscono tra loro**.

Cyberbullismo: solamente effetti immediati?

I mass media ci hanno abituato a pensare a questo fenomeno come ad un qualcosa di immediato, fulmineo, per il quale le persone coinvolte reagiscono sulla scia dell'impulsività, del trasporto emotivo del momento. Nell'immaginario collettivo abbiamo la scena di un ragazzo che riceve all'improvviso un messaggio particolarm**ente negativo, seguito dai commenti di altri ragazzi, e quindi decide di compiere un gesto estremo.** Nulla è più lontano dalla realtà. **Questa forma di Cyberbullismo si sviluppa nel tempo**, spesso a partire dal bullismo tradizionale, in cui **il ragazzo è fatto bersaglio per settimane, forse anche mesi**, prima che i suoi persecutori decidano di aumentare l'effetto del loro gesto e **spostare il tutto online**.

Inoltre la percentuale dei ragazzi che decidono di compiere l'estremo gesto, per quanto tragica, rimane comunque molto contenuta: **la maggior parte dei ragazzi fortunatamente trova la forza per reagire alla pressione.** Tutto questo comporta che i nostri ragazzi porteranno il fardello di questa esperienza per settimane, mesi, in alcuni casi anche per anni, quindi **anche molto tempo dopo che il gesto si è esaurito.** In particolare possiamo classificare gli effetti in: breve termine, medio termine, lungo termine.

Gli effetti a breve/medio termine del Cyberbullismo

Gli effetti a breve/medio termine del **Cyberbullismo** sono davanti agli occhi di tutti, complici i mass media che si focalizzano sullo scoop del momento: questi ultimi hanno fretta di mostrarci la notizia dell'ultimo minuto e rincorrono la novità, quindi tendono a mostrarci il Cyberbullismo nei suoi effetti più immediati.

Tra questi troviamo:

- Improvviso e drastico mutamento dell'umore verso il versante negativo
- Abbandono della vita sociale
- Abbandono della scuola
- In alcuni casi auto-reclusione
- In alcuni casi gesti estremi quali tentato suicidio, oppure un suicidio che tragicamente riesce

Un altro effetto molto importante e preoccupante è l'inversione del ruolo vittima-carnefice.

Molte ricerche testimoniamo che **un ragazzo bullizzato ha un'alta probabilità di diventare a sua volta un bullo**, ovviamente non nei confronti del suo vecchio carnefice. Più in generale, i ragazzi che hanno sono stati bersaglio hanno un'alta probabilità di sviluppare forme aggressive quali linguaggio violento, atteggiamenti violenti nei confronti di altre persone, e comportamenti vandalici.

In particolare, **i ragazzi che hanno subìto sia forme di bullismo tradizionale che forme di bullismo online hanno il doppio di probabilità di sviluppare simili atteggiamenti devianti**, come ci testimonia una ricerca presentata alla P**ediatric Academic Societies 2016 Meeting** nell'aprile 2016 a Baltimora, portando una percentuale del 38% tra quei ragazzi indagati che erano stati vittime sia della forma offline che della forma online del bullismo. **Una percentuale allarmante, se consideriamo che spesso il bullismo online è una naturale estensione di un bullismo che sta già avvenendo offline.**

E' anche un chiaro segnale di un fenomeno che è anche un problema per la società, non solamente per i ragazzi direttamente coinvolti e per il gruppo dei loro vicini. Ciò che spesso non viene preso in considerazione è l'ampio spettro degli effetti a lungo termine.

Gli effetti a medio/lungo termine del cyberbullismo

Il cyberbullismo è un trauma a tutti gli effetti, per cui è come tale che dobbiamo analizzarlo se vogliamo comprendere meglio gli strascichi nel corso degli anni successivi all'evento. E se parliamo di un trauma i cui effetti possono protrarsi per lunghissimo tempo non possiamo non pensare al **Disturbo da Stress Post-Traumatico** (PTSD, ossia Post Traumatic Stress Disorder). In

uno **studio condotto da Megan Ranney per la Hasbro Children's Hospital** è infatti emerso che la violenza tra ragazzi, Cyberbullismo e il PTSD sono strettamente intrecciati e correlati.

Nel suo studio effettuato su 353 adolescenti, Ranney ha rilevato che il 46.5% dei ragazzi che avevano avuto accesso al reparto emergenze dell'ospedale, riportavano episodi di violenza tra pari, e sempre tra questi 353 ragazzi un altro 46.7% riportava eventi di Cyberbullismo.

Nel dettaglio dei sintomi:

- 23.2% presentava i segni del PTSD
- 13.9% presentava i sintomi della depressione
- 11.3% riportavano pensieri suicidari

Una situazione che, se non trattata tempestivamente e con professionalità (un percorso di psicoterapia e, se occorre, anche consultando uno psichiatra), può provocare dei tangibili mutamenti nella nostra struttura cerebrale, minando a sua volta nei ragazzi colpiti la capacità di reagire a future situazioni simili, in un circolo vizioso che fa scivolare l'individuo verso il basso.

Gli effetti del bullismo tradizionale e del cyberbullismo possono anche rimanere latenti per molti anni a seguire, e sfociare in età adulta o pre-adulta. In una ricerca longitudinale condotta da su 7.000 bambini partendo dai 12 anni fino ai 18 anni, ha rilevato che tra coloro che avevano riportato di essere state vittime di bullismo:

- Il 12.3% presentava i sintomi della depressione
- Il 16% riportò segni di ansia
- Il 14% dichiarò di avere praticato autolesionismo nell'ultimo anno

Siamo di fronte a delle percentuali molto importanti, se consideriamo che questi effetti erano presenti anche 8 anni dopo l'evento scatenante. Possiamo spingerci anche più in là: una ricerca condotta da **Audrey Tyrka, del Dipartimento di Psichiatria e Comportamento Umano della Warren Alpert Medical School della Brown University, Providence**, e i suoi collaboratori nel 2014, ha scoperto che eventi e situazioni di forte stress e ansia in età infantile possono provocare cambiamenti nei mitocondri del DNA che accelerano l'invecchiamento dell'individuo. Sebbene la ricerca sia stata condotta su un campione molto ristretto di individui, ossia 290 adulti, i suoi risultati ci offrono un ulteriore campanello di allarme circa fenomeni quali bullismo e Cyberbullismo.

Bulli online: imparare ad avere paura

Ogni stato d'animo umano può essere appreso. Di più: **ogni stato d'animo umano può essere rinforzato** mediante un'esposizione tale per cui ad un certo punto il soggetto si crea un'anticipazione dello stato d'animo stesso. **E' lo stesso effetto che i ricordi hanno nel rievocare in noi sensazioni ed emozioni, anche dopo anni che l'evento in sé si è esaurito.**

Il cyberbullismo, a differenza del bullismo tradizionale, colpisce all'improvviso e in silenzio, tanto che **spesso la vittima ne viene a conoscenza quando ormai il fenomeno è già in corso.** Inoltre **la natura virale e di scala del fenomeno** genera nella vittima una sensazione di impotenza: il ragazzo in questione sente di non avere alcun controllo, si sente in balìa degli eventi, non potendo fermare il flusso delle ricondivisioni e dei commenti negativi.

E' questa perdita della sensazione di controllo che "insegna" al ragazzo a rimanere costantemente sul chi va là: in ogni momento, ogni notifica può essere l'ennesima derisione di qualche compagno. Il ragazzo quindi impara ad avere paura, e nel tempo impara anche a prepararsi ad avere paura, cosa che alimenta questa sensazione. La conseguenza è lo sviluppo di un orientamento verso questo stato d'animo che finisce per influenzare ogni aspetto della vita dell'individuo.

La persona diventa sempre più sensibile alla paura e tutto ciò che ad essa è legato, e perde sempre più sensibilità nei confronti degli aspetti positivi di un evento oppure una relazione. Il risultato è un ragazzo, poi adulto, che non sarà in grado di rispondere positivamente alle situazioni di stress, e che farà molta fatica a provare emozioni positive, non importa la situazione di vita che sta vivendo.

Inoltre nel corso degli anni il fortissimo orientamento verso la paura influenzerà i ricordi, e non solo: le emozioni che viviamo influenzano anche in che modo noi apprendiamo i nuovi eventi. Noi letteralmente filtriamo ogni nostra situazione di vita alla luce dell'emozione dominante in quel momento. E se la paura è l'emozione dominante di un individuo, allora possiamo immaginare quali profonde implicazioni avrà nella crescita e nella vita adulta.

L'abuso emotivo sullo stesso livello dell'abuso fisico?

Sebbene il cyberbullismo possa esprimersi in molteplici modi e configurazioni, nel vissuto della vittima troviamo gli stessi elementi: **denigrazione, intimidazione, esclusione, umiliazione**. Questi elementi possono protrarsi per giorni, settimane, forse anche per mesi oppure anni. Stiamo quindi parlando di vero e proprio abuso emotivo, che presenta conseguenze che vanno ben al di là dell'evento in sé.

A tal proposito una ricerca condotta nel 2015 da **David Vachon, del Dipartimento di Psicologia della McGill University**, e collaboratori, si è avvalsa dei dati di ricerche condotte negli ultimi 20 anni presso un Summer camp con ragazzi tra i 5 e i 13 anni, e li ha incrociati con i rilevamenti effettuati su 2.300 ragazzi dello stesso Summer camp. I risultati sono molto chiari: **abuso fisico e abuso emotivo** provocano gli stessi effetti, che sono equivalenti, trasversali, universali. Questi effetti sono i comportamenti devianti già citati sopra.

Non solo effetti psicologici. Fino ad ora ci siamo concentrati sugli effetti psicologici del cyberbullismo, cosa peraltro abbastanza ovvia, trattandosi di un fenomeno prettamente "virtuale". Tuttavia questo non deve trarci in inganno, poiché questa particolare forma di bullismo provoca effetti a lungo termine anche nell'organismo della vittima. **Oltre ai già citati mutamenti cerebrali e nel DNA, dobbiamo anche considerare quelli che potremmo definire "effetti indiretti".** Un ragazzo che tenta il suicidio lo fa adottando una pratica fortemente deleteria per il suo corpo, sia essa l'ingestione di una sostanza altamente tossica, oppure autolesionando il proprio corpo in modo da ottenere l'effetto estremo.

Sono tutte pratiche che lasciano nel corpo del ragazzo segni spesso indelebili. Allo stesso modo, un ragazzo che assume comportamenti devianti come conseguenza del disagio provocato da un atto di cyberbullismo danneggia gli altri attraverso i suoi comportamenti violenti e non solo: corre il rischio di esporre anche se stesso a comportamenti che possono portarlo a conseguenze molto estreme.

Cyberbullismo, le conseguenze per gli "spettatori"

Il cyberbullismo, più del bullismo tradizionale, gode di una fluidità dei ruoli: come la vittima può facilmente diventare un futuro bullo, così il bullo può diventare la futura vittima di atti di bullismo, anche in età adulta. **Inoltre vari studi hanno dimostrato che le stesse tensioni psicologiche vissute dalla vittima vengono vissute anche dai bulli.** Spingendoci ancora più in là, alcune ricerche hanno rilevato che questi effetti si espandono anche alla cerchia degli amici dei ragazzi direttamente coinvolti nel fenomeno, sia che quei ragazzi abbiano assistito all'atto, sia che ne siano solamente a conoscenza.

Varie ricerche infatti ci dicono che **dove si verifica un atto di cyberbullismo anche la classe intera ne risente**, sia emotivamente che nel **rendimento scolastico**.

Inoltre **le tecniche di intervento che si sono rivelate più efficaci nelle scuole sono quelle che lavorano sull'intera classe** senza operare forti distinzioni di ruolo: la maggior parte delle volte infatti la forma di Cyberbullismo qui trattata si configura come un pensiero del gruppo che tende ad estromettere l'elemento considerato più debole oppure che mina la sopravvivenza del gruppo stesso, nel quale il bullo si rivela essere la mano longa di questo pensiero collettivo.

Un fenomeno che coinvolge tutti noi. Il Cyberbullismo quindi è molto più di un diverbio tra due ragazzi. E' molto più di un gesto: è un pensiero di gruppo che individua l'elemento da estromettere, ne pianifica l'estromissione, individua chi concretizzerà il gesto, e lo porterà a compimento. Per cui nessuno deve esserne escluso, sia in fase di prevenzione che di intervento. Essendo tutti i ragazzi partecipanti, in un modo o nell'altro, nello strutturare i nostri progetti non dobbiamo dimenticarci di nessuno. Siamo alla presenza di un fenomeno che coinvolge tutti, e le cui conseguenze individuali, relazionali, sociali, coinvolgono tutta la società in cui vivono i ragazzi.

-

Bibliografia

Alex Tendler, Shlomo Wagner. Different types of theta rhythmicity are induced by social and fearful stimuli in a network associated with social memory. *eLife*, 2015; 4 DOI: 10.7554/eLife.03614

American Academy of Pediatrics. (2016, April 30). Combination of face-to-face and online bullying may pack a powerful punch: Victims of multiple forms of bullying have more than twice as likely to show aggressive behaviors such as verbal hostility, physical fighting and damaging property. *ScienceDaily*. Retrieved April 22, 2019 from www.sciencedaily.com/releases/2016/04/160430100241.htm

David D. Vachon, Robert F. Kruger, Fred Rogosch, Dante Cicchetti. Assessment of the Harmful Psychiatric and Behavioral Effects of Different Forms of Child Maltreatment. *JAMA Psychiatry*, 2015 DOI: 10.1001/jamapsychiatry.2015.1792

Jamie L. Hanson, Ahmad R. Hariri, Douglas E. Williamson. Blunted Ventral Striatum Development in Adolescence Reflects Emotional Neglect and Predicts Depressive Symptoms. *Biological Psychiatry*, 2015; 78 (9): 598 DOI: 10.1016/j.biopsych.2015.05.010

Jason N. Doctor, Lori A. Zoellner and Norah C. Feeny. Predictors of Health-Related Quality-of-Life Utilities Among Persons With Posttraumatic Stress Disorder. *Psychiatr Serv*, 62:272-277, March 2011 DOI: 10.1176/appi.ps.62.3.272

Lucy Bowes, Dieter Wolke, Carol Joinson, Suzet Tanya Lereya, Glyn Lewis. **Sibling Bullying and Risk of Depression, Anxiety, and Self-Harm: A Prospective Cohort Study.** *Pediatrics* Oct 2014, 134 (4) e1032-e1039; **DOI:** 10.1542/peds.2014-0832

Marieke Jepma, Tor D. Wager, **Conceptual Conditioning: Mechanisms Mediating Conditioning Effects on Pain, Psychological Science,** September 17, 2015; DOI: 10.1177/0956797615597658

Megan L. Ranney, John V. Patena, Nicole Nugent, Anthony Spirito, Edward Boyer, Douglas Zatzick, Rebecca Cunningham. **PTSD, cyberbullying and peer violence: prevalence and correlates among adolescent emergency department patients**. *General Hospital Psychiatry*, 2015; DOI: 10.1016/j.genhosppsych.2015.12.002

T Lau, B Bigio, D Zelli, B S McEwen, C Nasca. Stress-induced structural plasticity of medial amygdala stellate neurons and rapid prevention by a candidate antidepressant. *Molecular Psychiatry*, 2016; DOI: 10.1038/MP.2016.68

Responsabilità dell'hosting provider: luci e ombre della giurisprudenza

Le disposizioni Ue e nazionali sulle responsabilità degli hosting provider in merito alla pubblicazione di contenuti illeciti sono inadeguate all'evoluzione delle piattaforme digitali. Ecco perché la giurisprudenza, si è trovata a elaborare in modo spesso disarmonico. Una panoramica sulle sentenze e gli interrogativi aperti

Di **Ernesto Apa**, partner, Portolano Cavallo
e **Filippo Frigerio**, associate, Portolano Cavallo

E' stato molto sottovalutato negli ultimi tempi la questione riguardante **i caratteri del regime di responsabilità degli *internet service provider***, e in particolare dei cosiddetti "*hosting provider*", in relazione ai contenuti caricati su tali piattaforme dagli utenti.

Questione che sta montando nelle aule dei tribunali, ma non - come dovrebbe - sulle pagine dei media (distratti dall'analogo dibattito sulla **direttiva copyright).**

Hosting provider attivo, le sentenze

Negli scorsi anni, il Tribunale di Roma ha definito i caratteri del cosiddetto *hosting provider* attivo **con tre sentenze in materia di diritto d'autore**, emanate nel 2016 (rispettivamente *Break Media*[1], confermata in appello l'anno seguente[2], *Kit Digital France*[3] e *Megavideo*[4]).

L'*hosting* attivo è una figura di creazione giurisprudenziale, che sfugge all'applicazione dell'esenzione di responsabilità prevista dalla direttiva comunitaria sull'e-commerce[5] a causa dello svolgimento di specifiche attività ancillari nell'ambito della fornitura del servizio. È importante sottolineare come tali attività prescindano dalla conoscenza dei contenuti caricati dagli utenti, bensì siano, da un lato, esclusivamente funzionali a una migliore fruizione del servizio da parte degli utenti medesimi e, dall'altro, **destinate ad aumentarne l'attrattività e la conseguente redditività**. Il Tribunale di Roma ha, inoltre, individuato una serie di elementi rivelatori del carattere "attivo" dell'*hosting provider* (nella sostanza confermati dalla pronuncia *Vimeo*[6] del gennaio 2019), quali **l'impiego di sistemi automatizzati di filtraggio dei contenuti e l'accostamento di pubblicità a detti contenuti.**

Nel 2015, si era espressa **in senso opposto** la Corte d'Appello di Milano nel caso *RTI/Yahoo!*[7], seguita dal Tribunale di Torino con le decisioni *DeltaTV/YouTube*[8] nel 2017 e *DeltaTV/Dailymotion*[9] nel 2018.

In particolare, **queste due corti hanno sancito l'irresponsabilità dell'*hosting provider* fino al momento in cui quest'ultimo non riceva una segnalazione qualificata che lo renda in tal modo edotto della presenza di un contenuto illecito** specificamente individuato a mezzo del proprio URL. L'*hosting provider* diviene responsabile per i contenuti ospitati sulla propria piattaforma secondo il regime ordinario di responsabilità per fatto illecito qualora riceva detta segnalazione qualificata oppure manipoli i contenuti medesimi.

Nel dibattito è intervenuta pochi mesi fa la decisione della **Corte di cassazione** che ha annullato con rinvio la decisione *RTI/Yahoo!* della Corte d'Appello di Milano[10].

Dobbiamo chiederci quale sia la portata innovativa della pronuncia del Supremo Collegio.

Il quadro giuridico europeo

L'art. 14 della direttiva e-commerce definisce l'*hosting provider* come il fornitore di un servizio "*consistente nella memorizzazione di informazioni fornite da un destinatario del servizio*". Per promuovere la libera circolazione dei servizi digitali nell'ambito dell'Unione europea, **il legislatore ha previsto che, in presenza di determinate circostanze, il prestatore di questo servizio non sia responsabile delle informazioni che memorizza su richiesta del destinatario del servizio**, salvo che quest'ultimo non agisca sotto il controllo o l'autorità del prestatore.

In alternativa, **tale esenzione di responsabilità viene meno qualora il prestatore sia effettivamente a conoscenza dell'illiceità o della manifesta illiceità del contenuto**, **oppure** nel caso in cui, venuto a conoscenza di un fatto che rende illecito il contenuto, **non si attivi immediatamente per rimuoverlo o per disabilitarne l'accesso.** Nel recepire la normativa europea a mezzo del D.lgs. n. 70 del 2003, il legislatore italiano ha previsto che l'effettiva conoscenza dell'illiceità del contenuto, che determina l'insorgere dell'obbligo di rimozione per mantenere l'esenzione di responsabilità, può derivare anche dalla comunicazione dell'autorità giudiziaria o amministrativa.

L'intento del legislatore europeo è stato quello di creare **un quadro giuridico teso ad assicurare la libera circolazione dei servizi della società dell'informazione tra gli Stati membri**, imponendo il divieto agli Stati membri di imporre ai prestatori sia un obbligo generale di sorveglianza delle informazioni sia un obbligo di ricercare attivamente fatti o circostanze relativi ad attività illecite. Nel recepire la normativa europea, il legislatore italiano ha previsto che il *provider* sia tenuto a comunicare, su richiesta dell'autorità giudiziaria o amministrativa, i dati che consentano l'identificazione dell'utente che ha commesso un illecito sul servizio.

Inoltre, la legge italiana sancisce un **obbligo di attivazione, generalmente *ex post*, da parte del fornitore del servizio**, allo scopo di raggiungere un equilibrio, per quanto delicato, tra le esigenze di tutela dei prestatori dei servizi della società dell'informazione e gli interessi dei fruitori di tali servizi.

Normative inadeguate all'evoluzione digitale

Le disposizioni appena richiamate mostrano oggi tutti i segni del tempo. In questo senso, non è difficile intuire come il mondo dei servizi *online* sia profondamente cambiato rispetto a com'era nel 2000/2003: in particolare, in quegli anni servizi come YouTube, Facebook, Twitter, Instagram, WhatsApp, etc. non erano nemmeno immaginabili. Di conseguenza, **la giurisprudenza è stata chiamata ad affrontare temi radicalmente nuovi,** elaborando in modo spesso disarmonico i concetti fissati dalla normativa sull'e-commerce, proprio alla luce del carattere così dinamico della materia in oggetto.

I commentatori si sono interrogati sulle **modalità concrete che devono essere seguite per segnalare i contenuti oggetto di violazione**, sul **livello di dettaglio richiesto** per ritenere effettivamente informato il *provider* e, infine, sul **dovere di diligenza** richiesto nell'analizzare (e processare) le richieste di rimozione provenienti dal titolare del diritto che si assume leso.

La posizione della Corte di cassazione

La Corte di cassazione fornisce risposta a parte di questi interrogativi. La Corte ha confermato, sulla scorta del citato Tribunale di Roma, l'esistenza della figura dell'*hosting provider* attivo, ossia di quel soggetto che svolge attività che esulano da un servizio di ordine meramente tecnico, automatico e passivo. Ulteriormente, i Supremi giudici hanno individuato i cosiddetti "indici di interferenza", ovverosia quelle specifiche condotte che si traducono in "*attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione*". La Cassazione ha, pertanto, individuato una deviazione in taluni servizi rispetto al modello di *hosting provider* di matrice europea; **questo determina l'inapplicabilità dell'esenzione di responsabilità sancita nella direttiva e-commerce e il riconoscimento della responsabilità** se sono integrati tutti gli elementi della responsabilità aquiliana *ex* art. 2043 e ss. c.c.

Rovesciando questi criteri si individuano anche i caratteri dell'***hosting provider* passivo**, cioè quello che può beneficiare dell'esenzione di responsabilità di cui alla normativa e-commerce, prevedendo però specifici obblighi di intervento e segnalazione al ricorrere di determinate circostanze.

In aggiunta ai principi sopra richiamati, **la Suprema Corte ha precisato che chiunque può segnalare la presenza di un contenuto illecito al *provider* e quest'ultimo deve fornire un riscontro**. In particolare, secondo quest'orientamento, tale segnalazione può essere inoltrata con qualunque mezzo, pertanto **non è richiesta una lettera formale di diffida in senso tecnico**. Le regole di diritto comune stabiliscono che opera una presunzione di conoscenza del destinatario di una comunicazione ove questi sia stato reso edotto dell'esistenza di un fatto specifico in forma orale o scritta. Come correttamente precisato dal Supremo collegio, l'assenza di una comunicazione formale al *provider* rende più complessa la prova dell'effettiva conoscenza, che resta sempre a carico del segnalante.

In ogni caso, **la segnalazione deve essere idonea a consentire al *provider* di individuare il contenuto della violazione**. Ancorché la Corte di cassazione non abbia preso posizione circa la necessità per il titolare del diritto di fornire l'URL per individuare il contenuto, i Giudici hanno chiaramente suggerito che la comunicazione deve porre il prestatore nelle condizioni di "*identificare perfettamente*" i contenuti.

Una volta ricevuta la segnalazione, il *provider* deve processarla con la diligenza richiesta dalla natura del servizio che offre e compiere una scelta circa il carattere illecito o meno del contenuto. Ciò significa che il *provider* è chiamato a operare una valutazione del contenuto segnalato (e successivamente identificato) e a provvedere alla sua **immediata rimozione nel caso in cui il contenuto sia manifestamente illecito. Qualora residui un dubbio e il contenuto appaia solo potenzialmente illecito, il *provider* è tenuto a inoltrare la segnalazione all'autorità giudiziaria o amministrativa.** Quest'ultima operazione, ancorché astrattamente possibile, si presenta in concreto non priva di insidie, specialmente in relazione a determinate tipologie di contenuti, e impone alla piattaforma digitale di operare un bilanciamento che, forse, non era affatto previsto nello spirito della direttiva e-commerce.

Contenuti a carattere diffamatorio

Se, come si è visto, **per i contenuti in violazione del diritto autorale altrui la giurisprudenza è oramai abbastanza consolidata** nel ritenere sufficiente una segnalazione dettagliata da parte del

titolare dei diritti, i giudici hanno deciso in maniera diametralmente opposta nel caso di **contenuti a carattere diffamatorio**. In particolare, in due distinte occasioni, il Tribunale e la Corte d'appello di Roma hanno rigettato le domande, indirizzate a due differenti *provider*, avanzate da due soggetti che sostenevano di essere stati diffamati da alcune dichiarazioni presenti *online*[11]. I Giudici hanno concluso che i contenuti in oggetto non si presentavano come manifestamente illeciti e, di conseguenza, non era mai sorto alcun obbligo in capo all'ISP di agire e di rimuovere l'accesso al contenuto asseritamente diffamatorio per il solo fatto della segnalazione.

Inevitabilmente, **laddove l'ordine di rimozione provenga invece da un'autorità giudiziaria o amministrativa, il *provider* non sarà chiamato a operare alcuna valutazione**, bensì a provvedere all'immediata rimozione del contenuto.

In conclusione, qual è lo spazio lasciato al dibattito? Se è vero, come è stato dimostrato, che i Supremi giudici hanno confermato la figura dell'*hosting provider* attivo, i caratteri – o i cosiddetti "indici di interferenza" – di questo servizio sembrano puntare verso un soggetto che ha preso conoscenza dei contenuti in maniera diretta e non automatizzata. Sotto questo punto di vista, la recente decisione lascia aperti molti interrogativi, che – è ragionevole attendersi – occuperanno le corti italiane per molto tempo a venire.

BIBLIOGRAFIA

1. Trib. Roma, 27.04.2016, n. 8437, in *DeJure*. ↑
2. Corte d'appello di Roma, 29.04.2017, n. 2833, in *DeJure*. ↑
3. Trib. Roma, 05.05.2016, n. 9026 in *DeJure*. ↑
4. Trib. Roma, 15.07.2016, n. 14279 in *DeJure*. ↑
5. Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») ↑
6. Trib. Roma, 10.01.2019, n. 639. ↑
7. Corte d'appello di Milano, 07.01.2015, n. 29. ↑
8. Trib. Torino, 07.04.2017, n. 1928. ↑
9. Trib. Torino, 24.01.2018, n. 342. ↑
10. Cass., I sez., sent. 19.03.2019, n. 7708. ↑
11. Trib. Roma, 22.06.2018 in *Rivista di diritto dei media*, 2018, 3 e App. Roma, 19.02.2018, n. 1065 in *Rivista di diritto dei media*, 2018, 2. ↑

Una piramide per valutare e gestire il cyber risk, ecco i vantaggi

Una strategia per aumentare la resistenza agli attacchi di un sistema informatico a partire da una classificazione "a piramide" del sistema basata sui possibili attacchi ed al rischio che essi generano. Obiettivo: individuare quali strumenti utilizzare per valutare e gestire il cyber risk

Di **Fabrizio Baiardi**, Università di Pisa

Una **struttura a piramide** per classificare i sistemi Ict di una organizzazione e scegliere lo **strumento migliore per minimizzare i rischi.**

Partendo dalla valutazione del rischio che un sistema genera, la soluzione utilizza una classificazione dei sistemi visualizzata, appunto, come una piramide con più livelli che prende in considerazione tre aspetti:

- quello puramente **tecnico** del tipo di attacco e dell'attaccante,
- quello puramente **economico** sui costi e benefici economici dell'organizzazione proprietaria,
- i possibili **costi sociali.**

[infografica id="62578" class="attachment-full infoImg infoImg-contain-width infoImg-contain-width-transform hide"]

Fig. 1. La piramide dei sistemi informatici

Sistemi ICT ai livelli più alti richiedono una valutazione ed una gestione più sofisticata per meglio resistere ai cyberattacchi che li coinvolgono [1, 2]. L'adozione di una piramide evidenzia che il numero di sistemi che richiedono soluzioni più sofisticate diminuisce all'aumentare del livello della piramide. Tuttavia, la crescente diffusione di sistemi informatici nell'**industria 4.0** sta erodendo la base della piramide.

Individuare i possibili attaccanti e le loro strategie è fondamentale per valutare e gestire il rischio. In particolare, la valutazione deve scoprire non solo le **vulnerabilità del sistema** ma soprattutto i percorsi degli attaccanti. Un percorso è una sequenza di attacchi che permette ad un attaccante di ampliare i propri privilegi e controllare un numero crescente di risorse fino a quelle che sono il suo obiettivo. **La gestione del rischio deve individuare un insieme di contromisure che modificano il sistema**, in modo permanente o temporaneo, e bloccano uno o più percorsi eliminando le vulnerabilità che abilitano gli attacchi nei percorsi. **Bloccare percorsi diversi con le stesse contromisure è una strategia fondamentale per minimizzare i costi della sicurezza.**

La necessità di predire e bloccare i percorsi di attacco rende la valutazione e gestione del rischio un processo diverso dalle soluzioni attualmente più diffuse e che coprono solo alcuni passi dell'intero processo. Questo processo è diverso dall'analisi delle vulnerabilità, che deve scoprire le vulnerabilità di un sistema ma non i percorsi che esse permettono [3]. È anche diverso da un

penetration test che non può garantire la scoperta di tutti i percorsi. Esistono attualmente sul mercato **numerosi strumenti che supportano alcuni passi del processo**. Un numero ridotto di strumenti più innovativi permette l'automazione completa della scoperta dei percorsi e la scelta delle contromisure da adottare.

La piramide della cybersecurity

Consideriamo inizialmente i soli **benefici ed impatti economici** per il proprietario del sistema. Se usiamo questa metrica possiamo classificare i sistemi utilizzando due metriche tra loro ortogonali.

La prima metrica la più semplice, classifica un sistema in base all'impatto sui processi dell'organizzazione del controllo illegale del sistema da parte di terzi. Questa metrica dovrebbe essere una percentuale ma, per semplicità, useremo una **classificazione binaria**. Di conseguenza, i processi dell'organizzazione possono continuare o dover essere interrotti in base al controllo dell'attaccante sul sistema target. Assumiamo che abbiano un impatto sui processi di un'organizzazione anche quei sistemi per cui esistono vincoli legali verso terzi. Ad esempio, il GDPR introduce dei **vincoli sulla protezione delle informazioni personali e sulla gestione di eventuali perdite di dati**. Un attacco a sistemi che trattano informazioni di questo tipo si ripercuote sempre sui processi dell'organizzazione.

La seconda metrica distingue i sistemi che meritano un attacco di tipo mirato (vedi box in basso) per il ritorno economico da quelli che verranno invece coinvolti solo in attacchi di massa**. Ciò che caratterizza questi ultimi sistemi è che le loro risorse più preziose sono quelle informatiche**, mentre le informazioni che custodiscono sono magari critiche per il proprietario ma di ridotto valore se offerte a terzi. Questa classificazione evidenzia che mentre tutti i sistemi ICT possono il bersaglio di attacchi di massa solo alcuni saranno attaccati per il valore delle risorse che gestiscono o di quelle che pilotano.

Tra i sistemi coinvolti anche in attacchi mirati distinguiamo **quelli che gestiscono infrastrutture critiche come, ad esempio, la distribuzione di gas, luce ed acqua.** Il controllo illegale di questi sistemi provoca perdite non solo economiche ma anche di vite umane con forti ripercussioni e costi sociali.

Infine, l'ultima classe che consideriamo comprende un sottoinsieme delle infrastrutture critiche ed in particolare **i sistemi da cui dipende la sicurezza dello Stato**. Tipico esempio è quello di un sistema per il **voto elettronico** o per il controllo di **sistemi di arma o di difesa**. In questo caso, il controllo, soprattutto se persistente, da parte di terzi ha ripercussioni non solo sociali ma anche strategiche a livello nazionale ed internazionale.

Se applichiamo simultaneamente le due metriche, è ovvio che solo i sistemi che non meritano un attacco mirato possono non influenzare i processi dell'organizzazione. Di conseguenza, l'uso simultaneo delle due metriche genera la seguente classificazione dei sistemi target:

- **sistemi soggetti unicamente ad attacchi di massa** e che non hanno un impatto critico sui processi aziendali,
- sistemi soggetti unicamente ad attacchi di massa ma **con un impatto critico sui processi,**
- sistemi soggetti anche ad **attacchi mirati per il ritorno economico,**
- sistemi per il **controllo di infrastrutture critiche**,
- sistemi da cui dipende la **sicurezza dello Stato**.

Il tutto è riassunto nella piramide in fig. 1. La piramide, che indicheremo come economica, sottolinea che il numero di sistemi in una classe è sempre inferiore a quella della classe. Esaminiamo ora in dettaglio le classi e le strategie da adottare per difendere i sistemi associati.

Classe 1

Un tipico sistema target in questa classe è quello per la gestione amministrativa di un'azienda. È ovvio che le informazioni che esso gestisce sono fondamentali ma l'azienda può continuare le sue attività anche in assenza dell'amministrazione. Ciò riduce l'impatto di un attacco al sistema ICT e, di conseguenza, anche gli investimenti in sicurezza ICT previsti per il sistema target. Vista la costante riduzione degli attacchi di tipo ransomware, gli attacchi di massa tendono sempre più alla creazione di botnet. Questi attacchi hanno **un impatto spesso molto ridotto per l'organizzazione proprietaria poiché la botnet usa le risorse nei sistemi dell'organizzazione per tempi ridotti e, in generale, senza significativi danni economici**. Ad esempio, la botnet creata dalla prima versione di Mirai comprende dispositivi di tipo IoT e sfrutta un dispositivo infetto per cercare altri dispositivi da compromettere. I dispositivi infettati continuano a funzionare normalmente ma aumenta il loro utilizzo della banda di comunicazione. Inoltre, Mirai non attacca sistemi dove potrebbe essere scoperto. Ad esempio, non attacca sistemi del DoD o di industrie collegate.

Evitare di danneggiare significativamente il sistema target è una regola fondamentale per una botnet che voglia continuare a controllare le sue risorse. Questo è quello che avviene in natura dove i parassiti con più elevata diffusione e successo stabiliscono un equilibrio con gli organismi che li ospitano.

Come detto, **anche investimenti in sicurezza molto ridotti possono essere convenienti per sistemi target in questa classe.** Ad esempio, quasi tutti i ransomware possono essere sconfitti semplicemente aumentando la frequenza con cui si creano copie di backup. Di conseguenza, può non essere conveniente per l'organizzazione proprietaria del sistema disporre di competenze proprie su valutazione e gestione del cyber risk ICT. In questo contesto, la reazione più economicamente conveniente ad un attacco di tipo ransomware può essere quella di **pagare quanto chiesto**. Ovviamente, questa strategia può diventare non utilizzabile in base alla frequenza degli attacchi, ma questo è al di fuori del controllo dell'organizzazione.

Visti i ridotti investimenti possibili e la carenza di competenze, non conviene utilizzare strumenti personalizzati per la difesa di questi sistemi. **Le contromisure saranno quindi delegate a strumenti standard sia per la rilevazione di malware che per la gestione delle patch.** Meccanismi di filtraggio del traffico sono definiti configurando moduli già presenti nel sistema. Ad esempio, è possibile creare access control list per il routing di frontiera o per altri moduli del sistema. L'efficacia di queste soluzioni è comunque limitata dalla struttura piatta e non segmentata di molti di questi sistemi e che permette al malware di raggiungere tutti i nodi del sistema qualunque sia il nodo infettato inizialmente.

In generale, **visto il ridotto investimento in sicurezza ICT, la valutazione e la gestione del rischio di un sistema in questa classe è possibile solo automatizzando il processo corrispondente.** Solo una soluzione automatizzata può offrire un servizio di qualità elevata ed adeguato alla crescente complessità e sofisticazione dei malware. L'automazione permette da un lato di ridurre il costo delle attività e dall'altro di rimediare alla carenza di personale interno in grado di valutare il cber risk ed implementare le contromisure. **La ridotta complessità del sistema e delle contromisure semplifica il compito degli strumenti.**

Come detto nel seguito, questa classe di sistemi viene costantemente erosa a favore di quelli della classe successiva.

Classe 2

Un sistema target in classe 2 gestisce **risorse o informazioni che non hanno valore al di fuori dell'organizzazione proprietaria** ma la mancata o la ridotta disponibilità del sistema può avere un serio impatto sulla produzione o provocare ripercussioni legali che l'organizzazione deve comunque gestire. Tipico esempio è quello di un sistema per il controllo industriale o di un sistema target che gestisca informazioni personali protette dal GDPR. Anche se le informazioni che il sistema di controllo gestisce non hanno valore sul mercato, **una ridotta disponibilità del sistema provoca il blocco di una o più linee produttive con danni potenzialmente elevati**. Un attacco al sistema con **dati personali** provoca sicuramente i costi per la notifica alle persone i cui dati sono stati acceduti. Di conseguenza, **i sistemi in questa classe devono essere adeguatamente protetti**. **Visto il potenziale impatto economico degli attacchi, è necessario valutare e gestire il cyber risk individuando contromisure efficaci ed economiche.** L' impatto elevato permette anche di aumentare l'investimento in sicurezza. È quindi possibile adottare **strumenti di difesa personalizzati come firewall** e sistemi per la rilevazione di intrusioni. È compito della valutazione e gestione del rischio coordinare e dirigere gli strumenti in modo da bloccare tutti i percorsi di attacco.

La diffusione dell'industria 4.0 con la conseguente adozione di linee di produzione ad alta automazione sotto il controllo di algoritmi di **intelligenza artificiale** aumenta in maniera continua il rapporto tra il numero di sistemi in classe 1 e quelli in classe 2 a favore di questi ultimi. Uno svantaggio ineliminabile dell'automazione della produzione è la possibilità di attacchi cyber.

Anche in sistemi in questa classe, **l'automazione della valutazione e della gestione del rischio supera le carenze di dipendenti esperti ed ottimizza costo e numero delle contromisure utilizzate.** La criticità di un sistema in questa classe richiede un insieme completo di contromisure ovvero in grado di bloccare tutti i percorsi d'attacco. Approcci parziali alla valutazione del rischio come un penetration test o un vulnerability assessment non sono quindi adeguati perché non possono scoprire tutti i percorsi di attacco e non garantiscono di restituire delle contromisure che blocchino completamente tali percorsi.

Classe 3

Un sistema in classe 3 può essere il target di attacchi di massa e mirati ed un attacco con successo ha sicuramente un impatto sui processi aziendali [4, 5]. La scelta delle contromisure deve tener conto sia dei processi dell'organizzazione su cui il sistema va ad incidere sia dell'esistenza di attaccanti in grado di personalizzare l'attacco. Questi attaccanti possono essere anche di tipo APT nel caso di impatti rilevanti, ad esempio quando il sistema target è gestito da **organizzazioni bancarie o finanziarie**, o quando l'organizzazione appartiene ad una s**upply chain per componenti di sistemi in classi più elevate**, ad esempio una SME che fornisca componenti per infrastrutture critiche. Complessivamente, i due fattori aumentano sia il potenziale impatto di un attacco che la sua probabilità di successo. Questo aumenta sia il cyber risk che gli investimenti necessari per valutarlo e gestirlo.

La diffusione dell'industria 4.0 provoca una significativa crescita del numero di sistemi che gestiscono informazioni critiche per la produzione industriale e che hanno grande valore per la

concorrenza. Di conseguenza, aumenta la probabilità che un sistema tipico di industria 4.0 possa diventare il bersaglio di un attacco mirato.

Una organizzazione che utilizzi un sistema target in questa classe deve poter disporre di competenze informatiche in grado di applicare le contromisure selezionate. Il punto critico per la valutazione e la gestione del rischio è l'esistenza di attaccante che utilizza una strategia adattiva e non fissa come un malware. Di conseguenza, **l'attaccante può modificare la sua strategia ed il suo percorso anche in base alle contromisure adottate**. Di conseguenza, l'attaccante sceglierà alcuni percorsi contro il sistema originale, i percorsi iniziali, e percorsi diversi se alcune contromisure bloccano i percorsi iniziali. Poter conoscere in anticipo e bloccare tutti i percorsi, compresi quelli che l'attaccante sceglie quando reagisce alle contromisure sui percorsi iniziali, è quindi fondamentale per una difesa completa. **Ciò può essere garantito solo adottando, anche in questa classe, strumenti che automatizzino in modo completo la valutazione del rischio e la selezione di contromisure**. Infatti, solo un approccio automatico è in grado di scoprire sia tutti i percorsi d'attacco iniziali che quelli che un attaccante sceglierà reagendo alle contromisure adottate.

Classe 4

Un attacco ad un sistema target in classe 4 ha un impatto non solo economico perché può mettere in pericolo la vita delle persone. Un possibile esempio è un attacco ad una rete di distribuzione di luce e/o gas. Gli impatti di attacchi a questi sistemi possono comprendere, ad esempio il **mancato riscaldamento delle abitazioni, la sicurezza dei trasporti e la cura degli ammalati.** Riadattando una definizione di Bruce Schneier possiamo dire che se un attacco ai sistemi delle classi precedenti produce dei danni, qui **può provocare delle catastrofi**. Quindi, la difesa di questi sistemi non solo deve valutare e gestire il cyber risk ma anche applicare contromisure che possono non essere convenienti ma evitano impatti agli utenti finali delle infrastrutture. Sistemi in questa classe possono richiedere non solo robustezza rispetto a cyber attacchi ma anche una resilienza rispetto a guasti o fallimenti dei singoli componenti.

Gli attacchi possono essere mirati ma anche di massa. Ad esempio, attacchi ai sistemi per la produzione e distribuzione di prodotti petroliferi sono stati eseguiti tramite alcune varianti dei malware Disttrack e Shamoon.

La legislazione europea con la **direttiva NIS** richiede per questi sistemi l'applicazione di una valutazione del rischio sia rispetto a minacce intelligenti che a guasti e fallimenti. Visto l'impatto non solo economico, **i sistemi in questa classe possono essere il bersaglio di attacchi mirati provenienti da APT che possono essere supportati da Stati interessati a creare e manipolare movimenti di opinione o manifestazioni più o meno violente.** Quindi questi sistemi sono bersaglio non solo di attaccanti sofisticati ma anche di tipo ibrido che integrano, ad esempio, attacchi tecnologici con la manipolazione di mezzi di comunicazione. Questi attaccanti possono conoscere vulnerabilità non ancora pubbliche e quindi sistemi in questa classe devono poter resistere agli attacchi di questo tipo. Una valutazione del rischio adeguata deve quindi utilizzare **analisi di tipo *what-if*.** Questo approccio è l'unico che può di valutare come eventuali vulnerabilità non ancora pubbliche possono aumentare il cyber risk. Lo stesso approccio permette di scoprire se è possibile bloccare un percorso di un attaccante prima che possa sfruttare queste vulnerabilità. P**er evitare costose modifiche ad un sistema già funzionante è opportuno adottare anche metodologie di tipo *security-by-design*,.** La necessità di dover utilizzare simultaneamente *what-if e security by design* limita ulteriormente l'adozione di penetration test o di strumenti di breach simulation che devono lavorare sul sistema esistente e non su un suo modello.

Classe 5

Un attacco ad un sistema in classe 5 ha ripercussioni sulla sicurezza dello Stato. In questo caso l'organizzazione è di tipo statale o è un fornitore di una organizzazione statale. Sistemi tipici in questa classe possono essere, ad esempio, quelli per **votazioni nazionali** elettroniche, sistemi per la **gestione di informazioni coperte dal segreto di stato o sistemi d'arma**. Un attacco con successo a questi sistemi ha ripercussioni strategiche di lungo termine. Le minacce sono in generale supportate e finanziate da altri stati e, molto più raramente, da organizzazioni criminali. In generale, gli attaccanti sono estremamente sofisticati e dispongono di un arsenale di vulnerabilità non pubbliche. **Diventa ancor di più fondamentale per sistemi in questa classe l'adozione simultanea di metodologie *security by design* e *what-if***. L'uso di modelli formali e rigorosi è un supporto fondamentale per migliorare la cybersecurity di questi sistemi.

Aspetti tecnici, economici e sociali

È evidente come ai livelli bassi della piramide gli aspetti preponderanti siano quelli tecnici ed economici, salendo verso i livelli alti gli aspetti sociali e strategici diventano predominanti. Ai livelli alti cresce anche la **competenza degli attaccanti**, le risorse di cui dispongono e la loro persistenza, ovvero la volontà di ripetere attacchi fino al loro successo. Altra caratteristica è l'uso di tecniche stealth per minimizzare la probabilità di essere scoperti e massimizzare la permanenza nel sistema. Per impedire l'attribuzione dell'attacco, questi attaccanti usano catene sempre più lunghe di nodi intermedi, stepping stones, per mascherare la sorgente reale dell'attacco. **Questo non implica che ai livelli bassi gli attacchi siano banali** perché anche gli attacchi automatici hanno raggiunto un livello di sofisticazione elevato. Le principali carenze degli attacchi automatici sono legate alla **adattività** ovvero alla capacità di reagire al fallimento di un attacco non eseguendo il successivo in un ordine fisso, ma di sfruttare le informazioni raccolte per scegliere quello con maggiore probabilità di condurre all'obiettivo. Un ultimo aspetto da considerare è che **la diffusione di robotica e di tecnologie tipo industria 4.0** provoca la "promozione" del sistema informativo di molte organizzazioni dalla prima classe alla seconda.

In un attacco a sistemi di fascia alta, il tempo non è un problema critico in quanto l'attacco viene pianificato in modo da disporre di tutto il tempo necessario, in particolare per la raccolta di informazioni. Se un attaccante può scegliere il tempo da investire nella raccolta di informazioni sul target prima dell'attacco, quando l'attacco inizia è conveniente minimizzare il tempo per eseguire gli attacchi o per installare software sul sistema target.

Utilizzo di cloud

Nel caso di sistemi ai livelli bassi della piramide la migrazione ad un cloud pubblico può permettere ad una organizzazione di ridurre il cyber risk e disporre di personale con migliori competenze. Questo miglioramento va bilanciato con l'aumento del rischio dovuto alla condivisione di risorse tipica di un cloud pubblico. Inoltre, l'utilizzo di cloud può non essere possibile per vincoli in tempo reale o di connettività. Nel caso di sistemi dei livelli alti della piramide, l'utilizzo di sistemi cloud è limitato a cloud privati o a partizioni fisiche di cloud pubblici come già avvenuto negli USA.

Piramide e igiene pubblica

Questa sezione descrive brevemente **le possibili strategie di difesa del sistema target** da parte della organizzazione proprietaria. Nel seguito, considereremo solo sistemi di classe inferiore alle infrastrutture critiche poiché a partire da questa classe i sistemi devono rispettare **specifici vincoli di legge** che l'organizzazione proprietaria deve conoscere.

Sono due le domande che l'organizzazione proprietaria di un sistema nelle prime tre classi deve porsi:

- influenza del sistema target sui processi dell'organizzazione
- possibilità di un attacco mirato.

Una risposta positiva almeno alla prima domanda implica la necessità di valutare il cyber risk e di **adottare delle contromisure adeguate**. La seconda risposta determina la complessità delle contromisure da adottare.

Mentre l'organizzazione possiede le informazioni per rispondere alla prima domanda, la risposta alla seconda può essere più difficile perché dipende dal valore delle informazioni possedute e dall'interesse che queste possono suscitare. Si consideri, ad esempio, come la risposta cambia se una azienda diventa fornitore di una organizzazione bancaria o finanziaria o di una che operi nel settore della difesa nazionale. Ciò è indipendente dalla dimensione dell'azienda e dalle sue competenze informatiche. Vi può essere inoltre la spiacevole tendenza a dare una risposta negativa perlomeno alla seconda domanda per limitare i costi della sicurezza. Questo può però ripercuotersi su tutta la supply chain cui l'organizzazione appartiene.

In buona parte degli attacchi discussi in precedenza, le botnet hanno un ruolo fondamentale per nascondere la sorgente reale di un attacco e per fornire risorse agli attaccanti. Da questo punto di vista, solo l'esistenza delle botnet permette agli APT di agire e di nascondere le tracce delle loro azioni. È quindi ovvio che **la ridotta convenienza al livello basso della piramide di aumentare la robustezza dei loro sistemi provochi un aumento degli investimenti in sicurezza necessari ai livelli alti della piramide**. A questa asimmetria può rimediare da un lato l'automazione del processo di valutazione e gestione del rischio dall'altro un supporto agli investimenti.

L'automazione di valutazione e gestione del rischio provoca non solo una forte riduzione del costo di queste procedure ma supera la carenza di personale esperto in **cyber security**. Una valutazione automatizzata e di qualità è strutturalmente ripetibile e trasparente. Quindi, essa permette ad un'organizzazione di affrontare al meglio eventuali vulnerabilità del proprio sistema informatico e fornisce una valutazione realistica del cyber risk che il sistema genera, qualunque sia la posizione nella piramide. **Non solo la valutazione può essere opposta a terzi, ma evita all'organizzazione il falso senso di sicurezza generato da una valutazione non oggettiva svolta da personale non qualificato**. Una gestione del rischio automatizzata individua le contromisure più efficaci ed economiche mediante strumenti di ottimizzazione ben consolidati. Questo fornisce un solido supporto alle scelte degli investimenti in sicurezza.

Il principale problema da affrontare per una automazione completa della valutazione e gestione del rischio è la raccolta di informazioni sul sistema. La raccolta è di particolare complessità soprattutto nei due casi estremi di sistemi di aziende micro o piccole oppure molto grandi. **Aziende micro o piccole, infatti, non dispongono di personale in grado di raccogliere e fornire tutte le informazioni necessarie.** Aziende molto grandi hanno sicuramente personale competente ma i loro sistemi informativi sono talmente estesi e crescono ad una velocità tale da impedire la raccolta di informazioni complete. **Recenti risultati di ricerca permettono però di**

risolvere il problema e sono attualmente disponibili prototipi in grado di ricostruire con elevata accuratezza la topologia di un sistema e di produrre un inventario dei suoi moduli.

Anche la sofisticazione crescente di attacchi di massa dimostra che solo una valutazione automatica del rischio possa valutare e gestire il cyber rischio perché tutti i sistemi dovranno a breve poter resistere ad attacchi di massa e sofisticati. In altri termini, solo l'automazione della valutazione e gestione del rischio permette di fronteggiare l'automazione e la sofisticazione degli attacchi.

Il finanziamento pubblico applica alla gestione del cyber risk una strategia pienamente validata dalla sanità pubblica. Nel momento in cui si decide che è interesse pubblico limitare la diffusione di alcune malattie è compito dello stato intervenire e coprire costi di vaccinazioni di massa o di altre soluzioni. Una strategia simile può essere adottata e sovvenzionare sia l'esecuzione della valutazione del rischio che l'adozione di contromisure per migliorare la resistenza agli attacchi di sistemi il cui unico valore è di essere usato come stepping stone di attacchi mirati. Questa strategia assume che nessun sistema abbia un valore trascurabile e ne garantisce la robustezza ad attacchi quando viene connesso in rete.

Una strategia alternativa prevede l'obbligo della certificazione dei sistemi che si vogliano connettere ad una rete pubblica. Infine, l'obbligo si può accompagnare ad una assicurazione per coprire danni causati a terzi con facilitazioni e costi ridotti per chi valuta il cyber risk ed adotta le contromisure suggerite.

La strategia proposta e la classificazione su cui è basata evidenziano l'importanza strategica delle tecnologie per automatizzare in modo completo la valutazione e la gestione del rischio**. Solo l'automazione può fronteggiare in modo adeguato il rischio crescente posto dall'automazione degli attacchi e dalla crescente adozione dei sistemi cyber fisici alla base dell'industria 4.0 e dalla robotica.**

Definizioni

Attacco di massa

Un attacco non mirato o di massa non ha un obiettivo specifico ma vuole colpire il maggior numero di sistemi possibili. Attacchi di massa sono eseguiti da malware che comprendono un vettore di attacco ed un payload. Un **vettore d'attacco** è un frammento di codice che esegue sequenzialmente alcuni attacchi fino a quando uno ha successo. La sequenza è rigida e non specializzata in base al sistema attualmente attaccato. **Se uno degli attacchi ha successo, il malware può replicarsi sul nodo attaccato**, controllarlo ed usarlo come punto di partenza per attaccare altri nodi.

Il **payload** è un codice che sfrutta le risorse dei nodi attaccati con successo. Un tipico payload crea delle reti nascoste o botnet le cui risorse apparentemente restano sotto il controllo del legale proprietario. **Chi crea una botnet ne affitta le risorse per l'invio di spam, il mining di criptovalute, l'esecuzione di DDOS o di altri attacchi.**

Un **RAT,** remote access trojan, è un payload per il controllo di nodi ed il furto di informazioni sul nodo o prodotte dagli utenti. Discutiamo separatamente nel seguito un altro payload, il ransomware.

Un attacco di massa installa inizialmente il malware su alcuni nodi da dove lancia i suoi attacchi. Una strategia alternativa utilizza **una campagna di phishing** che invia e-mail con link per scaricare il malware. Il malware penetra così in sistemi ben protetti da cui si diffonde.

Tipico attacco di massa è quello realizzato dalle versioni di **Mirai** che attaccano non solo webcam ma anche router, sistemi di teleconferenza e dispositivi di memoria di rete. Alcune varianti **eseguono fino a 27 attacchi**, alcuni non noti in precedenza. Mirai usa le risorse controllate per eseguire DDOS:

Sono attacchi di massa anche quelli realizzati da **attaccanti non sofisticat**i, gli script kiddies, che usano strumenti automatici e che non sanno personalizzare per adattarli al sistema target. Questi attaccanti si muovono in maniera casuale e scegliendo come bersaglio quei sistemi cosi fragili da cedere ai loro attacchi.

Attacco ransomware

In questo attacco di massa, il payload cifra i dati di ogni sistema attaccato. Successivamente, l'attaccante ricatta il proprietario del sistema che solo pagando può ricevere la chiave per decifrare i propri dati. Quest'attacco è possibile grazie alle **criptovalute** che permettono pagamenti in forma anonima. Sperimentalmente, la frequenza di questi attacchi è proporzionale al valore delle criptovalute.

Si sono avuti attacchi di massa simili ad un ransomware ma che non miravano a controllare risorse o al pagamento di un riscatto ma alla distruzione di informazioni. Ad esempio, **NotPetya** pur essendo classificato come ransomware non lo era, perché non poteva decriptare quanto criptato in precedenza. Un attacco di massa di questo tipo è meglio descritto come cyber vandalismo.

Attacco mirato

L'attacco mirato ha uno specifico sistema come target ed è personalizzato per questo sistema. Obiettivo dell'attacco è la persistenza, ovvero una presenza prolungata nel sistema target per rubare informazioni o per manipolare alcuni moduli del sistema. **Un attacco mirato comprende più passi che raccolgono informazioni sul bersaglio, personalizzano degli attacchi**, creano una struttura di command e control per gestire il furto di informazioni o altro. L'attaccante impiega la maggior parte del tempo nella raccolta di informazioni e spesso sfrutta tecniche di phishing ma specializzando i messaggi con le informazioni raccolte sull'organizzazione ed il suo organigramma.

Un attacco mirato viene in generale eseguito da un umano, ovviamente con il supporto di strumenti informatici, ma può però essere anche delegato ad un malware esteso con informazioni per riconoscere il bersaglio, se e quando sarà raggiunto. In questa soluzione, utilizzata ad esempio da Stuxnet [6, 7], il malware ha una diffusione di massa ma agisce, e colpisce, solo i sistemi che sono il suo bersaglio. **Questa strategia richiede una raccolta delle informazioni che permetta di descrivere accuratamente il sistema target**. Un attaccante utilizza un attacco mirato mediante malware quando non può raggiungere direttamente il sistema target e non è interessato ad un controllo remoto su tale sistema.

Se confrontiamo un attacco mirato ed uno di massa, è evidente che quello di massa non comprende le operazioni più complesse e cioè la raccolta di informazioni sul sistema target e la trasmissione stealth dei dati raccolti.

Advanced Persistent Threat

Un Advanced Persistent Threat è un attaccante con elevate competenze che opera in modo stealth per minimizzare la probabilità di essere scoperto. Ciò aumenta il tempo dedicato alla raccolta informazioni sul sistema target perchè rallenta le possibili interazioni tra l'attaccante ed il sistema per scoprire le informazioni di interesse. Un APT privilegia attacchi che generano poco rumore sempre per minimizzare la probabilità che essi siano rilevati. C'è un ovvio, forte legame tra APT ed attacchi mirati perché sicuramente un APT userà tutte le strategie e gli strumenti tipici di questi attacchi.

Security by design e what if

La metodologia *security by design* applica la valutazione e la gestione del rischio in tutte le fasi di sviluppo di un sistema target, a partire dal suo progetto. Anticipare in fase di progetto l'individuazione delle sorgenti di rischio e l'adozione di contromisure non solo minimizza il rischio al momento del deployment del sistema ma permette di utilizzare contromisure più efficaci e meno costose. Infatti, modificare una vulnerabilità di un progetto è sempre meno costoso che intervenire su un sistema già operativo. Il GDPR richiede un approccio *security by design* ma la metodologia non è supportata dalle soluzioni più popolari per scoprire il cyber risk come, ad esempio, il penetration test. Solo strumenti in grado di lavorare su modelli, esatti o approssimati, del sistema sono in grado di supportare strategie di questo tipo. Considerazioni simili valgono per l'analisi *what-if* che analizza e prevede come il sistema reagisce ad eventi quali la scoperta di vulnerabilità o il furto di identità. Anche questa analisi richiede la costruzione di un modello del sistema.

BIBLIOGRAFIA

1. R. Derbyshire, B. Green, D. Prince, A. Mauthe and D. Hutchison, "An Analysis of Cyber Security Attack Taxonomies," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 153-161.
2. F.Baiardi, F.Tonelli, Metriche per la robustezza, La Comunicazione 2016, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione.
3. F. Baiardi, F. Coro, F. Tonelli, D., Sgandurra, Automating the assessment of ict risk. *Journ. of Information Sec. and Applications* 19(3), 182–193 (2014)
4. E. M. Hutchins, M. J. Cloppert, R. M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." *Leading Issues in Information Warfare & Security Research* 1.1 (2011): 80.
5. Mandiant. M-Trends: The Advanced Persistent Threat, January 2010. URL http://www.mandiant. com/products/services/m-trends.
6. A. Matrosov, E.Rodionov, D. Harley, J. Malcho, (2010). Stuxnet under the microscope. *ESET LLC (September 2010)*.
7. J. P., Farwell, R. Rohozinski, Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40, 2011.

I quaderni di

Agenda Digitale.eu

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ