

Internet of things: opacità dei nuovi spettri nell'era della trasparenza digitale

Autore: Biamonte Alessandro

In: Diritto civile e commerciale

“Gli spiriti non moriranno di fame, ma noi periremo”[1].

Così, Kafka, nelle Lettere a Milena, con imperante angoscia, analizza - a suo modo - il processo dispercettivo che sarebbe sotteso all'utilizzo del mezzo epistolare, interpretato come un medium comunicativo disumanizzante: “Come sarà nata l'idea che gli uomini possano mettersi in contatto tra loro mediante lettere? A una creatura umana distante si può pensare e si può afferrare una creatura umana vicina, tutto il resto sorpassa le forze umane”. Pertanto, anche ogni bacio, semplicemente scritto, finirebbe con l'essere fagocitato dagli spettri; quei fantasmi che continuerebbero ad alimentarsi per mezzo di fattori mediati, che eliminano l'elemento del contatto reale.

Del resto, la comunicazione umana si compone di elementi metaverbali di natura tattile che si realizza nella stratificazione di forme poliperceptive e pluridimensionali, che trasformano la semplice trasmissione delle informazioni in un profondo dialogo biunivoco destinato a fondare il suo senso profondo nella natura corporea (e interiore) dell'alterità.

Anche il medium digitale - in questi termini - alimenta il rischio di una moltiplicazione esponenziale di quegli spettri descritti da Kafka, e, dissimulando il mito della (apparente) trasparenza sinora vissuta come fine escatologico, può trasformarsi antitetivamente in enorme buco nero che attrae tutto in sé, anche la luce: ecco l'opacità si oppone alla trasparenza del digitale[2]. Dall'“altro” all'“uguale” il passo è breve e finisce per segnare, in termini involutivi, la parabola umana, in cui l'alienazione, superati gli schemi classici del conflitto sociale, si traduce in autosfruttamento. Dissolto il confine tra il Sé e l'Altro, seguendo lo schema freudiano[3], energie egoiche contribuiscono a una congestione narcisistica della libido che genera sentimenti di angoscia, senso di colpa e vuoto: la perdita del senso dell'alterità, cioè della percezione oggettuale della realtà (condizione che, in situazione di normalità, stabilizza l'io), genera quel sentimento di vuoto che è sintomo della depressione e del disturbo borderline di personalità. E' per questo motivo che, in un'ottica di analisi della società, di fronte alla presa d'atto dell'inesorabile processo di destabilizzazione delle coscienze, Byung Chul Han finisce per concludere che questo costituisce l'esito consapevole della “perfida logica del neoliberismo...: l'angoscia aumenta la produttività”[4]. “Trasparenza e ipercomunicazione ci privano di ogni interiorità in grado di proteggerci. Certo rinunciamo a essa spontaneamente, e ci rimettiamo alla rete digitale che ci pervade, ci controlla e ci svuota. La sovraesposizione digitale genera un'angoscia latente, causata non tanto dalla negatività dell'Altro, quanto dall'eccesso di positività. L'inferno trasparente dell'Uguale non è privo di angoscia. Angosciata è proprio

la sempre crescente ubriacatura dell'Uguale"[5].

Ecco, dunque, il senso di fenomeni sociali diffusi che, dall'originario binge eating, si traducono - nel mondo digitalizzato - secondo schemi sintesi dell'alienazione, in binge watching (intesa come smodata e incontrollata visione e fruizione del video), oppure, in IFS (Information Fatigue Syndrome) - o affaticamento informativo - indotto da una sovraesposizione di informazioni, in cui chi ne è affetto lamenta paralisi della capacità di analisi, disturbi dell'attenzione, incapacità di assunzione di responsabilità. In misura non meno patologica, la progressiva pervasività della comunicazione digitale (che si caratterizza per il carattere "simmetrico" della comunicazione, per il quale chi è parte della stessa non si limita a consumare informazioni, ma le produce) si traduce in shitshorm, termine con il quale viene indicato il fenomeno di discussione massiva in rete con linguaggio connotato in termini negativi e violenti, o, nella migliore delle ipotesi, prende la forma di smart mobs (aggregazioni spontanee, per lo più con fine critico e di protesta, che si caratterizzano per la liquidità dell'iniziativa). In breve, l'apparente assenza di distanza assume la sembianza di un reflusso (spesso anche violento, frutto della mancanza di dialogo - come nella shitshorm - o della incapacità riflessiva indotta dalla mera indignazione non strutturata - smart mobs - priva di metodo e organicità). Ancora una volta gli "spettri", opaci e antagonisti della trasparenza, fanno capolino, con la loro contraddittoria opacità (uno spettro dovrebbe essere anch'esso trasparente, ma nel nostro caso si frappone alla trasparenza e dunque diviene opaco) nella dark pool - transazione elettronica anonima di prodotti finanziari ad alta frequenza -, in cui l'alto rischio di volatilità e speculazione degli scambi (afferenti all'alternative trading system) trova la sua ragion d'essere nell'anonimato, senza rendere noti prezzi e volumi: in tal modo anche il flash crash - il repentino crollo dell'indice finisce con l'essere il risultato (di fatto accettato in nuce) della carenza di trasparenza.

Internet delle cose

Per tornare ai fantasmi kafkiani, anche l'**Internet delle cose** (Internet of Things, brevemente "IoT"), una nozione sinora poco conosciuta ai più (anche se ne siamo immersi) e destinata ad assumere un ruolo centrale nella vita quotidiana del prossimo decennio, produce nuovi spettri capaci di "assorbire" la comunicazione percettiva umana: le cose, un tempo mute, cominciano a parlare. La crescita è impressionante: dagli attuali 12 miliardi di dispositivi connessi, si schizzerà a 50 miliardi nel 2020. Non sono più i soli computer o gli smartphone a connettersi a internet, ma un novero crescente di "oggetti": climatizzatori, elettrodomestici, termostati, apparecchiature elettromedicali, attrezzi fitness, televisori, telecamere di videosorveglianza o per il traffico, serrature, scaffali dei supermercati, sensori ambientali, strade e addirittura anche animali; ognuno con il proprio numero identificativo (UID) e un indirizzo IP; connessi via filo, oppure mediante wi-fi o bluetooth, o ancora per mezzo di sensori e sistemi di identificazione a radiofrequenza (RFID - Radio Frequency IDentification) e di comunicazione di prossimità (NFC - Near Filed Communication).

Le "cose" perdono sempre più significato in sé, per sottomettersi alle informazioni (ecco il passaggio dalla

comunicazione - umana - all'informazione, intesa come sedimentazione - anche casuale - di dati, salvo rielaborazione con sistemi di intelligenza artificiale), che a loro volta nutrono fantasmi. Per dirla con Flusser: "Non la cosa, ma l'informazione costituisce ciò che è economicamente, socialmente e politicamente concreto. Il nostro ambiente, a vista d'occhio, diventa sempre più soft, nebuloso, spettrale"[6].

Per avere solo l'idea dell'impressionante rivoluzione alle porte, basti pensare che nel 2020 esisteranno 40 zettabyte di dati (1000 Terabyte - cioè 1.000.000 di Gigabyte - equivalgono a 1 petabyte; 1000 petabyte a 1 exabyte; 1000 exabyte a 1 zettabyte). Un solo zettabyte è in grado di contenere 250 miliardi di dvd (cioè più di 35 anni di visione no stop di video ad alta definizione[7]). Già oggi, un solo volo aereo civile di 6 ore produce 320 Terabyte di dati, che vengono immagazzinati, per un futuro utilizzo, dalla compagnia aerea.

Di base, esistono due tipi di oggetti connessi: fisici (physical first) e digitali (digital first). I primi - salvo non siano trasformati - non comunicano dati; i secondi, invece, generano e trasmettono informazioni per successivi utilizzi, in quanto geneticamente a ciò predisposti. L'Internet delle Cose è reso ulteriormente potente dalla capacità di connettere gli elementi physical - first tra loro e con i digital - first, sino a giungere all'Internet of Everything. Le "cose", immerse in un sistema evoluto, governato dall'intelligenza artificiale e attivato da un modello di apprendimento automatico, schiudono un mondo inesplorato, sospeso tra comunicazione di prossimità, filigranatura digitale e conservazione dei dati. L'IoT penetra in mondi impercettibili, spesso invisibili, oltre la dimensione sensoriale e addirittura anche al di là della coscienza stessa (muovendosi lungo uno schema preriflettente che anticipa il sistema limbico), dove i dataset (luogo di raccolta, memorizzazione e utilizzo di insiemi di dati) costituiscono il fulcro essenziale. Indosseremo abiti connessi a internet e guideremo auto tanto intelligenti da scegliere la strada migliore, ma saremo anche in grado di conoscere in tempo reale il nostro stato di salute.

Il fulcro è costituito dal crowdsourcing: una modalità di condivisione che consente il collegamento di conoscenze ed esperienze prima insuscettibili di analisi e sfruttamento[8]. Si pensi come, già oggi, il crowdsourcing possa garantire una svolta per la sanità pubblica oppure migliorare servizi pubblici con minore dispendio di risorse[9].

Un IoT inclusivo, fondato su standard e protocolli aperti che garantiscano interoperabilità tra tutti i dispositivi, in controtendenza con l'originario mito della tecnologia proprietaria è la risposta. I veri vantaggi dei dispositivi connessi non derivano dall'usare lo smartphone per accendere l'automobile o regolare a distanza la temperatura di casa, quanto dalla condivisione universali dei dati in un contesto evoluto e democratico.

Più potenzialità, ma anche maggiori rischi

Sicuramente l'interconnessione dei dispositivi sta modificando l'intelligenza umana e le dinamiche

dell'elaborazione umana delle informazioni, senza considerare l'incidenza in termini di **decrescita della capacità di concentrazione** e dell'atteggiamento da gratificazione istantanea, che prelude a una **riduzione della capacità critica**.

Altro profilo da non sottovalutare risiede negli effetti del **divario digitale** in un mondo globalizzato e dominato dall'IoT: i digitalmente ricchi prospereranno ai danni dei digitalmente poveri? Negli anni Novanta del XX secolo, l'incedere progressivo di Internet alimentò il dibattito sul digital divide come fonte di potenziale disuguaglianza sociale ed economica. Oggi, nel mondo segnato dalla diffusione massiva - e apparentemente democratica - del mezzo digitale, gli originari timori sembrerebbero dissolti, ma il pericolo in agguato è direttamente proporzionale alla posta in gioco. Se anche un frigorifero connesso (che scrive la lista della spesa) e un sistema di illuminazione basato su sensori potrebbero non rivelarsi essenziali nel quotidiano, ben presto i progressi tecnologici potrebbero alimentare fratture sociali irreversibili tra individui connessi e non. Nell'ambito della salute sensori microscopici indossabili o integrati potrebbero garantire una diagnosi in tempo reale, anticipando l'esordio di un arresto cardiaco o l'insorgere di un cancro; coloro che non saranno connessi oppure i paesi dove non fosse disponibile la tecnologia dovranno accontentarsi di procedure tradizionali e meno efficaci. Parimenti, nel campo dell'educazione l'IoT aprirebbe mondi sinora inesplorati e, piuttosto che preconizzare un processo di dequalificazione culturale (come qualcuno teme), non è peregrino affermare che dispositivi connessi, realtà aumentata e sistemi taggati introducono la scienza, la ricerca e l'istruzione in contesti inesplorati, ma anche potenzialmente divisivi (una vera iattura per la crescita e la competitività di una comunità), laddove non venga garantito un accesso pariordinato a ciascuno.

Una delle principali sfide è poi la predisposizione di sistemi che garantiscano alto **livello di affidabilità e sicurezza**. Non di rado il legislatore affronta i problemi una volta che la crisi si sia realizzata nel suo grado più acuto, oppure quando il peggio è ormai avvenuto. Nel contesto europeo la direttiva NIS sulla sicurezza delle reti (1148/2016) - di là da essere recepita a pochi mesi dal termine imposto (maggio 2018) - il Regolamento GDPR (in materia di privacy) direttamente applicabile dal 25 maggio 2018 e la «proposta» di Regolamento sulle comunicazioni elettroniche e la vita privata elettronica («proposta» ancora meramente tale, in attesa di approvazione del Parlamento Europeo e della Commissione) costituiscono la «punta dell'iceberg» di una dimensione spesso insondata e sottovalutata per l'incidenza sugli assetti strategici della comunità nazionale e internazionale.

Personalizzazione, de-identificazione, re-identificazione, persistenza e data retention costituiscono le nuove frontiere. In gran parte rischi attuali - come nel caso dei cyber attack - e potenzialmente detonanti al pari di gravi attacchi terroristici, o paradossali, tra il teorico e il reale (se si pensa alla privacy): qualche anno fa un gigante della distribuzione statunitense (Target) identificò una liceale in stato di gravidanza sulla base degli articoli apparentemente casuali che aveva acquistato; quindi spedì a casa promozioni per abbigliamento premaman, sconvolgendo gli ignari genitori[10]. Non dissimili i riflessi nel mondo finanziario e bancario delle analisi individualizzate delle scelte o nel contesto dell'healthcare, laddove l'utilizzo ragionato di dati sensibili (teoricamente soggetti al grado massimo di tutela nel contesto della disciplina sulla privacy) piuttosto che essere orientato al miglioramento della salute pubblica (in termini di

tutela individuale e collettiva dello stato di salute del cittadino) venisse distorta per usi commerciali (dati sul genoma trasferiti a singole imprese farmaceutiche oppure a spregiudicati assicuratori). Il problema non è tanto la proliferazione del malware, quanto la disponibilità degli operatori economici a tamponare le falle (così come degli Stati a comprendere la pericolosità strategica di un disinvolto disinteresse).

Modelli di comportamento e di consumo diventeranno (anzi già lo sono) di dominio pubblico in un mondo connesso dove evoluti schemi algoritmici di sistemi intelligenti anticiperanno a livello preriflessivo le scelte dell'individuo.

Il futuro (anzi il presente) passa da qui, ma non può prescindere da tutele efficaci, che, nel mondo dominato ormai dall'IoT non può limitarsi all'impiego di un IP dinamico (che ingenuamente sembrerebbe mettere al sicuro dalla diffusione indiscriminata dei dati personali). Non esiste un diritto realmente internazionale, al di là di trattati bilaterali, convenzioni e accordi temporanei. Le leggi acquistano efficacia solo se fondate su norme condivise (in una società transnazionale sempre più diffusa) che tutti si impegnano a rispettare e fare rispettare. Ecco l'ennesimo richiamo alla nozione di sovranità digitale in un contesto ageografico e astatuale.

Il paradosso consiste nel pericolo che l'enorme potenzialità dell'interconnessione si tramuti in un mondo muto. Camus ne Lo straniero delinea la condizione dell'essere-straniero come sentimento dell'esistenza: l'uomo è straniero nel rapporto con il mondo, fra gli uomini e addirittura con se stesso. Il protagonista è separato dagli altri da una "grata di linguaggio" - estraneità come assenza di parole -. Una babele senza fine, che solamente il ritorno alla dimensione umanamente percettiva dell'alterità può scongiurare dominando in termini costruttivi un mondo dominato dalle informazioni finì a se stesse.

Volume consigliato

[1] Franz Kafka, Lettere a Milena, Mondadori, Milano, 1979.

[2] Si noti come il silicio - elemento base dei processori - derivi dal latino silex, pietra. La pietra è l'antagonista della trasparenza, sottrae visibilità e con il suo pesante appartiene al mondo terraneo come osserva Heidegger: "Un sasso non ha in sé alcuna luce" (Martin Heidegger, Prolegomeni alla storia del concetto di tempo, Il Melangolo, Genova, 1991, p. 369, nonché cfr. Id., "L'origine dell'opera d'arte", in Sentieri interrotti, La Nuova Italia, Firenze, 1991, p. 19).

[3] Sigmund Freud, Introduzione alla psicanalisi, Boringhieri, Torino, 1981, p. 379; sul ruolo della libido: Sigmund Freud, Al di là del principio del piacere, Boringhieri, Torino, 1977. Così potrebbe concludersi che, mentre l'Eros dà vita all'organismo, il narcisismo lo destabilizza.

[4] Byung Chul Han, L'espulsione dell'altro, edizione Nottetempo, Milano, 2017, p. 46.

[5] Byung Chul Han, op. cit., p. 48.

[6] Vilem Flusser, La cultura dei media, Bruno Mondadori, 2004, Milano, p. 204.

[7] Cfr. www.siemens.com/press/pool/de/feature/2014/corporate/heuring-factsheet-en.pdf.

[8] Jeff Howe, Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business, <http://archive.wired.com/wired/archive/14.06/crowds.html>.

[9] In Finlandia sensori posti nei contenitori dell'immondizia inviano un impulso a un camion quando è richiesto lo svuotamento: ciò ha implicato un risparmio del 40% dei costi di trasporto. A Nizza, un sistema di parcheggio smart avvisa gli automobilisti sui posti disponibili in tempo reale. Il sistema ha già ridotto la congestione del traffico e la riduzione di ossido di carbonio.

[10] How Companies Learn Your Secrets, in «New York Times Magazine, 12 febbraio 2012, www.nytimes.com/2012/02/19/magazine/shopping.-habits.html?pagewanted=1&_r=2&hp&.

<https://www.diritto.it/internet-of-things-opacita-dei-nuovi-spettri-nellera-della-trasparenza-digitale/>