TECHNOLOGICAL

COLLANA "MACRO TREND" | SETTORE ASSICURATIVO | 2018

DARK SIDE TECNOLOGIA

OSSERVATORIO

REPUTATIONAL & EMERGING RISK

Gruppo Unipol

TECHNOLOGICAL

DARK SIDE TECNOLOGIA

La numerosità e vitalità degli algoritmi dei sistemi digitali, unite a quel che offriamo loro quotidianamente su un piatto d'argento, producono già effetti rilevanti sul nostro presente, e potrebbero produrne ancora di più nel futuro.

Il primo computer basato sul sistema numerico binario totalmente programmabile fu costruito in Germania nel 1941 con componenti riciclati dalla telefonia. Circa venticinque anni dopo stanze di calcolatori consentivano all'uomo di lasciare la Terra ed atterrare sulla Luna. Ma per comprendere pienamente il trend tecnologico di questi ultimi ottant'anni bisogna focalizzare l'attenzione sul fatto che uno smartphone odierno è 180 milioni di volte più potente del computer usato per la missione Apollo. Eppure non siamo più andati sulla Luna; in compenso tutta questa enorme capacità di calcolo ci consente di inviare messaggi scritti, parlati e filmati, raramente di telefonare, più frequentemente di localizzarci, di ricevere informazioni su ciò che ci sta intorno, su ciò che potrebbe o dovrebbe esserci utile, di svagarci nei momenti di pausa, di leggere le notizie e di ricevere posta elettronica da amici, parenti e colleghi, di fare fotografie che vengono salvate in tempo reale su grossi server localizzati chissà dove, nel caso in cui il nostro "device" dovesse rompersi o noi dovessimo smarrirlo.

Gli utenti hanno passato collettivamente circa 200 milioni di ore tutti i giorni solo su Facebook, per buona parte creando contenuti che altri potessero consumare. E' il decuplo delle ore per persona che sono state necessarie per costruire l'intero canale di Panama.

(Brynjolfsson- McAfee)

Questa magnificenza tecnologica affascina la popolazione perché percepisce l'utilità immediata e reale, ma il 2017 è stato l'anno in cui le aziende tecnologiche sono state accusate dalla popolazione stessa (o quantomeno da una sua porzione) di essere sessiste, di aver inquinato gli esiti di elezioni importanti (in primis quella presidenziale degli USA), di aver indebolito il tessuto sociale, di aver distrutto una generazione e di aver manipolato la mente delle persone. Ma nonostante ciò sono cresciute tantissimo in borsa colossi come Apple, Microsoft, Google, Facebook e Amazon.

La forbice profitto/reputazione di queste aziende ha già iniziato ad aprirsi parecchio e nei prossimi anni sarà molto ampia la distanza fra la grossa quantità di profitti che faranno e la bassissima reputazione sempre più lontana dell'idea di filantropismo in stile Ted. Potrebbe non importare molto cosa penseranno gli utenti, perché i nuovi prodotti saranno sempre più convenienti, utili e quasi impossibili da evitare. Sembra ormai radicato

fortemente il fatto che, pur di trarre benefici dalla tecnologia, siamo disposti a cedere molto in cambio, anche se sta emergendo una consapevolezza nuova.

L'etica della tecnologia

La tecnologia sta assumendo un ruolo sempre più rilevante nella nostra quotidianità. Le ingerenze tecnologiche non sono più limitate all'economia e alla società, ma entrano prepotentemente nella nostra biologia e nel nostro sistema morale e valoriale. Si rende pertanto necessaria una riflessione etica nei confronti della tecnologia.

Le macchine lavorano in funzione di piattaforme software che dovranno affrontare il tema dell'etica. Attività scientifiche come la Medicina hanno già da tempo consolidato il rapporto con le conseguenze etiche di certe azioni, ma per i nuovi settori di tecnologia e informatica molto deve ancora essere affrontato. E in fretta. Le macchine programmate da noi esseri umani potrebbero svolgere azioni pericolose per la vita umana, si pensi alle auto che si guidano da sole, o discriminatorie, come ad esempio nella selezione dei curricula per future assunzioni.

L'Intelligenza Artificiale

La tecnologia non è solamente quella contenuta nei nostri cellulari iperconnessi, ma è anche quella che sta facendo progredire con velocità i settori dell'Intelligenza Artificiale e della robotica. Saremo contenti di farci curare da un robot? Riusciremo ad affezionarci a lui? Anche in questo caso, come è avvenuto per i Social Network, cosa saremo disposti a dargli in cambio?

Una risoluzione del Parlamento Europeo raccomanda, nel lungo termine, di creare uno specifico stato legale per i robot, così che almeno i robot più sofisticati e autonomi possano avere lo status di "persone elettroniche", con diritti e responsabilità. La concessione dei diritti va nella direzione di non effettuare modifiche software contro la loro volontà e addirittura di consentire loro di modificarlo in autonomia, di consentire loro di avere la privacy dei loro stati mentali e di replicarsi producendo loro copie, fino al diritto di non essere spenti contro la loro volontà, cosa che invece rappresenta proprio il gesto che dovrebbe sancire inequivocabilmente la loro assenza di responsabilità in quanto strumenti tecnologici creati dall'ingegno umano per sua utilità.

Poco prima della sua morte il cosmologo Stephen Hawking ha lanciato il suo anatema finale: l'Intelligenza Artificiale potrebbe essere il peggior evento della storia, se non riusciremo a gestirla al meglio. I computer possono emulare l'intelligenza umana e superarla, quindi non sappiamo bene se esiste realmente il pericolo che questo tipo di intelligenza possa essere dannosa per l'umanità. Su Science i ricercatori della società californiana Vicarious hanno pubblicato il risultato del loro lavoro, ovvero di un computer che riesce ad ingannare alcuni dei sistemi di sicurezza più diffusi su internet, i "captcha", fingendosi umano, perché costruito secondo i meccanismi del cervello umano. Si tratta all'incirca dei medesimi sistemi che possono essere installati sui nostri smartphone. Per alcuni di questi strumenti si fa già leva sul fatto che siano dotati di Intelligenza Artificiale, perché imparano le nostre abitudini e ci propongono scorciatoie.

Ma la capacità di apprendimento di questi software è realmente così potente e pericolosa? Pare di sì. Per due motivi: il primo perché nel 2017 è stato ottenuto un risultato importante relativamente all'apprendimento da parte dei software, il secondo perché questo risultato è stato ottenuto da Facebook, il social network che conta due miliardi di utenti e che ultimamente non ha dato prova di saper gestire la sua piattaforma secondo criteri di trasparenza. Ai laboratori Fair di Facebook due intelligenze artificiali hanno abbandonato l'inglese e hanno iniziato a dialogare in un linguaggio loro. Le macchine sono state precauzionalmente spente e i ricercatori hanno dato immediatamente segnali distensivi spiegando che si tratta di un risvolto tutt'altro che inedito per gli studiosi di Intelligenza Artificiale. Però il dubbio che qualcosa possa sfuggire di mano rimane.

Ed il Politecnico di Milano ha lanciato l'allarme, ad esempio, che è elevato il rischio di hackeraggio per i robot industriali. L'Industria 4.0 sempre più connessa si affaccerà a scenari preoccupanti: dal furto dei segreti industriali al sabotaggio, con l'introduzione di difetti nei prodotti e di danneggiamento di cose e persone. A fine 2017 durante il Forum Shipping di Genova un hacker ha "smontato" in diretta i sistemi di sicurezza di una petroliera, prendendone il controllo.

I pericoli per i più giovani

Secondo un sondaggio di Ipsos svolto nel 2017 per conto di Save the Children, nell'età compresa tra 11 e 17 anni il 97% dei ragazzi possiede un cellulare. Rispetto a quattro anni fa c'è stato un incremento del 26%. La connessione totale, ovvero 24 ore al giorno, riguarda il 47% di loro. L'età di accesso al mondo smartphone è passata dai 12 anni e mezzo del 2015 a 11 anni e mezzo nel 2017. Dal 2013 i tablet sono aumentati del 34%. In tasca insieme allo smartphone ci si porta appresso anche una serie di rischi, riguardo ai quali spesso manca consapevolezza. Perché lo stesso strumento è a disposizione di chi raccoglie dati a fini commerciali e addirittura politici. I devices digitali, e lo smartphone in particolare, sono diventati un'estensione di noi stessi, ed il rischio non deriva solamente da chi esternamente riesce ad avere accesso ai nostri dati, ma anche dalle nuove compulsioni che colpiscono, dallo zapping sulle app, alle "slot-machine" delle notifiche, al girone infernale delle chat senza tregua sulle quali scambiare qualsiasi cosa, ma soprattutto una moltitudine di selfie ormai individuati come la causa di una nuova patologia psichiatrica definita "selfite".

> **Il *nexting*, il "passare ad altro", è diventato parte della nostra ecologia emotiva.**
>
> **(Turkle)**

Se da un lato tutti questi strumenti consentono di stimolare la vivacità, è pur vero che come tutte le cose un abuso porta a delineare situazioni che contrastano con il benessere psico-fisico. Rappresentano il 98% i giovani che stanno svegli ben oltre la mezzanotte, riducendo il riposo o vanificandolo del tutto mantenendo acceso il cellulare tutta la notte e sottostando al fenomeno dell'illuminazione notturna, la cosiddetta "minaccia della luce bianca": ogni volta che arriva una notifica lo schermo del telefono si illumina intensamente di bianco, la retina viene colpita e in un istante si interrompe la produzione di melatonina; il ciclo giorno-notte viene compromesso e a lungo andare le ripercussioni sulle attività quotidiane si fanno sentire, tipicamente quelle

riferite alla scuola ed alla necessità di attenzione e reattività mentale. All'Università di Cagliari, che ha effettuato gli studi in questione, questi ragazzi sono chiamati "utilizzatori a tappeto". Apple ha da poco rivelato che da parte loro sarà rilasciato a breve un software contro la dipendenza da iPhone, ovvero una serie di strumenti per monitorare il tempo passato a usare lo smartphone e le singole app.

Grazie alla plasticità dei nostri tracciati neurali, più usiamo il web, più alleniamo il cervello ad essere distratto, a trattare l'informazione in modo rapido ed efficiente, ma senza un'intensa attenzione.

La facilità con cui si possono installare su smartphone e tablet app di tutti i tipi diventa molto pericolosa quando ad essere scaricate sono app che consentono il gioco d'azzardo. L'assenza di fisicità del controllo consente di fruire con facilità di questi servizi. La slot machine è in tasca e le app relative sono raddoppiate tra il 2013 ed il 2016. Aggirare i divieti è diventato molto facile e quattro adolescenti su dieci usano un canale telematico per il gioco d'azzardo. Sono 580 mila i minorenni che nel 2017 hanno giocato d'azzardo e la mancanza di cura, attenzione e informazione nei loro confronti si comprende quando l'11% degli studenti dediti al gioco dichiara di non sapere che in Italia il gioco è illegale sotto i 18 anni. La spesa pro-capite per il gioco d'azzardo telematico è di circa 10 euro al mese. Il giocatore tipo è maschio, di età compresa fra i 15 e i 24 anni, con basso livello di istruzione ed economico. Il gioco online è preferito per via di accessibilità, invisibilità, anonimato, assenza di controllo sociale e velocità.

L'Osservatorio Nazionale Adolescenza ha rilevato con il suo studio condotto su 8000 ragazzi quali sono le patologie legate all'iperconnessione: vamping, la connessione notturna di cui si è parlato sopra, FOMO (acronimo di Fear Of Missing Out) cioè la paura di essere accantonati da amici e conoscenti, likemania e followmania, alla ricerca continua di approvazione, nomofobia, cioè la paura che si scarichi il cellulare o che non abbia campo.

Il 95% dei ragazzi ha un profilo social, spesso gestito direttamente tramite app. Queste, per lo più sconosciute ai genitori, consentono di essere poco o nulla controllati, favorendo comportamenti come il sexting, il cyberbullismo e la diffusione in rete di materiale privato, che può portare al grooming ovvero all'adescamento di minori online.

La privacy in rete

Due anni fa la Comunità Europea ha adottato un regolamento per rafforzare e rendere omogena la protezione dei dati personali e dal 25 maggio 2018 il regolamento, noto come GDPR (General Data Protection Regulation) è diventato legge. Non rispettare la privacy degli utenti può costare molto caro, e le aziende dovranno cambiare l'approccio a queste problematiche. Le aziende dovranno chiedere esplicitamente il consenso all'utilizzo

dei dati, ma distinguendo secondo l'utilizzo che ne può essere fatto fra marketing, profilazione, geo-localizzazione e altro.

Anche l'età degli utenti ha da questo momento una rilevanza: con meno di 18 anni su Facebook non funzionerà l'opzione del riconoscimento facciale. E nella messaggistica WhatsApp sarà vietato sotto i 16 anni, almeno in Italia. E lo stesso dicasi per Periscope e Twitter. Ma l'azione di controllo non è facile, per non dire impossibile. Rimangono le nobili intenzioni, ma la realtà è che per eseguire i controlli le stesse aziende dovrebbero profilare gli utenti. Un paradosso.

Le sanzioni sono pesanti, soprattutto per le società che non conservano in misura adeguata i dati. Ma la cybersecurity è diventato un problema molto ampio, perché non ci sono solo gli smartphone e le app da gestire, ma anche tanti nuovi devices che sono collegati alla rete. Le auto di oggi stanno già nascendo con scatole nere native, e le case automobilistiche raccolgono tantissime informazioni sull'uso che si fa della vettura. La raccolta di dati e la loro trasmissione a server potenti e sofisticati rappresenta comunque la base per le vetture a guida autonoma, che senza queste importanti innovazioni tecnologiche non potrebbero mai funzionare. Ma la casa stessa sarà il centro principale di raccolta e smistamento di dati ed informazioni, molto private. I nuovi elettrodomestici contengono sistemi di diagnostica importanti utili per il loro utilizzo, come nel caso dei frigoriferi che possono tenere conto anche del tipo di alimenti contenuti e delle loro scadenze, ma anche per la loro manutenzione: se il device si guasta o presenta un mal funzionamento tramite la rete wifi di casa invia al centro di assistenza una diagnostica dettagliata, che un tecnico analizzerà rapidamente proponendo un appuntamento per la risoluzione del problema. Qualcosa di simile all'assistenza automatica in caso di incidente stradale.

Questi sistemi sono facili di hackerare e i costi di progettazione, volutamente contratti per non pesare sul prezzo finale, non possono tenere conto di sistemi di sicurezza interni. Il consiglio da parte di studiosi e specialisti è quello di diventare molto diffidenti. Quindi di controllare con attenzione i mittenti delle email, i link contenuti, le app installate. Diversi utenti coprono le webcam dei computer con nastro adesivo, perché un qualsiasi computer può essere preso sotto controllo da un hacker (tecnicamente si dice che il computer diventa un zombie) che può usare la webcam per vedere e il microfono per sentire.

La tecnologia ed il lavoro

Piattaforme come Uber e Foodora stanno rivoluzionando le relazioni tra lavoratori e imprese. L'economia digitale si basa su piattaforme che presuppongono una visione differente della cultura del lavoro, con lavoratori capaci di interpretare le opportunità in autonomia per raggiungere gli obiettivi aziendali ma anche i loro. A seconda di come vengono scritti gli algoritmi e i sistemi incentivanti i nuovi lavori della Gig Economy possono essere una fioritura di opportunità oppure un girone dantesco. Questo problema non può riguardare unicamente i lavoratori, ma anche i datori di lavoro perché c'è solo un parametro che distingue le organizzazioni di successo dalle altre: la qualità delle persone che ci lavorano.

Il mondo variegato della Gig Economy è composto da lavoratori che consegnano piatti caldi (30mila in Italia), piuttosto che farmaci (solo in quattro città italiane) o spesa personalizzata (con ben 250mila utenti registrati), ma sono anche disponibili per le pulizie domestiche (operativi in 5mila appartamenti), per guardare i bambini (in 83 città) oppure gli animali domestici (in 50 città).

Ma la sfida alla tutele riguarderà anche l'introduzione massiva della robotizzazione industriale. La proposta inglese dei laburisti è quella di una tassazione proporzionale alla quantità di automazione contenuta in azienda.

La distrazione da tecnologia

La tecnologia aumenta il livello di sicurezza, anche nella guida, con una riduzione degli incidenti grazie alla guida assistita e in prospettiva alla guida autonoma. Tuttavia il suo utilizzo non corretto può ridurla drasticamente. I dati degli ultimi anni mostrano che tra le cause degli incidenti stradali si sta imponendo la distrazione da tecnologia ed in particolare l'utilizzo dello smartphone mentre si guida. Sulla base dei dati ANIA l'incidenza di sinistri provocati dall'impiego del cellulare è aumentata negli ultimi anni , attestandosi al 20,1%. Secondo l'edizione 2017 del "Barometro europeo sulla guida responsabile" della Fondazione Vinci Autoroutes gli italiani sono poco disciplinati alla guida: il 32% dei conducenti legge o scrive sms o email mentre è al volante, rispetto alla media europea pari al 24%, e il 40% telefona senza utilizzare il vivavoce, rispetto al 32% in Europa. La distrazione da smartphone è un rischio non solo per i conducenti, ma anche per i pedoni, come evidenziato da tempo dall'Oms: i pedoni che utilizzano il cellulare mentre camminano (battezzati "petextrians") hanno minore consapevolezza delle situazioni e aumentano il rischio di incidenti per sé e per gli altri.

C'è uno scarso livello di percezione di questi rischi, verso i quali è importante un'attività di sensibilizzazione e prevenzione.

Impatti sul settore assicurativo

La necessità di sicurezza e tutela connessa alla tecnologia è uno dei filoni a maggiore tasso di crescita per le compagnie assicurative. La consapevolezza su questi temi è forte, ma l'evoluzione rapida delle minacce chiede sempre più attenzione. Il numero di devices interconnessi in rete è destinato a moltiplicarsi: sarà necessario affiancare la gestione del rischio con prevenzione, educazione e controllo da effettuarsi a monte della filiera. In questo contesto il settore assicurativo deve essere permeabile ai cambiamenti, tenendo testa alla velocità con cui il cambiamento stesso avviene.

I prodotti si dovranno adattare alla combinazione fra le esigenze del cliente ed il ruolo della tecnologia. Cambiano le prospettive su tematiche ben note alle compagnie. L'industria che si adegua ai tempi dovrà avere risposte assicurative in linea con i dettami 4.0, e la casa intelligente e connessa dovrà fare i conti con la sicurezza dei dati e la necessità di tutela della privacy.

Sarà sempre più importante prendere dimestichezza con il tema della resilienza, perché imprescindibile nei cyber attacchi e nel cyber crime che può avvenire in qualsiasi momento e in ogni luogo: nella piccola e nella grande azienda, in laboratori e università, ospedali e banche. Le prospettive sono certamente molto ampie.

FOCUS ON...

► HIKIKOMORI

Hikikomori è un termine giapponese che indica un fenomeno molto importante e drammatico, in forte crescita. Significa letteralmente "stare in disparte". Chi decide di ritirarsi dalla vita sociale per lunghi periodi, mesi e perfino diversi anni, rinchiudendosi nella propria camera da letto senza aver nessun tipo di contatto diretto con il mondo esterno, è un Hikikomori. Si tratta principalmente di giovani fra i 14 e i 25 anni di sesso maschile, ma si sta notando un'evoluzione sia nell'età che nel genere, con una rapporto maschi/femmine di 70 a 30. In Giappone, Paese nel quale è stato osservato per la prima volta, le associazioni che si occupano di questo fenomeno affermano che l'1% dell'intera popolazione nipponica ne è affetto, quindi circa un milione di persone. La diffusione ormai è planetaria ed in Italia i casi che possono essere considerati Hikikomori sono almeno centomila. La causa caratteriale è sicuramente alla base: si tratta di ragazzi introversi e sensibili quanto intelligenti. Vivono l'ambiente scolastico in maniera particolarmente negativa e molti potrebbero essere stati oggetto di bullismo. Sfuggono da una società che non capiscono e nei confronti della quale hanno una visione negativa. Quindi la mancanza di armi personali nei confronti delle difficoltà quotidiane portano all'isolamento. Questa situazione patologica di base trova sfogo con internet. Si rifugiano all'interno della rete e dei social network mediante profili fittizi, e questo è l'unico contatto con la società che hanno abbandonato. Gli Hikikomori quindi non sono di per sé malati di internet e tecnologia, ma in questi trovano terreno molto fertile per sviluppare pienamente la loro malattia. Spesso trovano nel monitor il loro mondo e quando giocano diventano compulsivi.

► Il futuro delle fake news

La notizie false esistono da sempre, ma i nuovi media digitali consentono più velocità e capillarità nella diffusione. Si producono fake news per scopi propagandistici, di profitto, influenza politica o anche interessi particolari. La profilazione degli utenti nei social network, nella navigazione in internet, nelle chat consente di predeterminare obiettivi specifici per le notizie false. Poi le notizie false spesso vengono condivise involontariamente, o volutamente se il messaggio contenuto è di rilevanza particolare. La nuova frontiera delle fake news però passa per le tecnologie più innovative. Basta una fotografia scattata con un telefono cellulare ed un volto umano prende vita e si muove perfettamente seguendo le movenze e le mimiche facciali del programmatore che utilizza il proprio viso come "master" per far fare e far dire tutto ciò che vuole al personaggio oggetto della truffa. Si tratta dei "fake videos". Ovviamente anche la voce è replicata perfettamente, elemento essenziale per ottenere la credibilità del video. CBS ha effettuato esperimenti altamente realistici con personaggi di altissimo rilievo politico mondiale. Ma nonostante l'impressionante efficacia dei trattamenti tecnologici, esistono categorie di esperti che con strumenti molto sofisticati riescono a distinguere i video reali dai "fake videos": una categoria di professionisti nata da poco ma che si sta evolvendo in fretta, anche nelle retribuzioni molto elevate.

► Digital detox

Dscout e Deloitte nei loro studi affermano che uno smartphone viene "controllato" dal proprietario fra le 2600 e 5400 volte al giorno, e che la maggioranza di noi accende il telefono entro i primi cinque minuti dal risveglio. Questo vale in generale per ogni device tecnologico e dipende dal fatto che il nostro cervello ha una predisposizione a fare attenzione agli stimoli in rapido cambiamento. È un retaggio dell'evoluzione legato alla sopravvivenza. La soluzione c'è però ed è appunto la digital detox. Si tratta di spegnere completamente smartphone, tablet, PC, dispositivi indossabili e di concedersi una pausa dal mondo digitale. Serve una buona motivazione, fissare un tempo di rehab non inferiore alle ventiquattro ore, programmare una porzione di vita analogica, ritornare online con calma e con tempi più lenti. Nella ricerca di un nuovo equilibrio e di un "benessere digitale" si può trasformare il FOMO prima citato nel JOMO: Joy of Missing Out, secondo l'espressione coniata dallo stesso CEO di Google.

Macro trend in a glance • DARK SIDE TECNOLOGIA

I DRIVER DEL CAMBIAMENTO

- Evoluzione tecnologica
- Evoluzione normativa e regolamentare
- Dilemmi etici crescenti nel rapporto fra uomo e macchina
- Tutela delle categorie più deboli, tipicamente giovani e anziani
- Dialogo fra figure con competenze tecniche e figure con competenze sociali

GLI IMPATTI SUL SETTORE ASSICURATIVO

Sul Sistema

- Desincronizzazione dei diversi sistemi (sistemi del diritto e dell'educazione vs sistema tecnologico)
- Patologie, dipendenze, distrazioni derivanti dalla tecnologia
- Strapotere dei player tecnologici

Sui Clienti

- Sistema assicurativo coinvolto nella fase di prevenzione e educazione ai rischi della tecnologia
- Miglioramento dell'esperienza del cliente nell'ottica della fiducia, della tutela e della salvaguardia del benessere e dei dati

OPPORTUNITA'

- Offerta di nuove forme assicurative
- Sviluppo di servizi in ambito educazione e prevenzione sui rischi della tecnologia in particolare su categorie più deboli (giovani, anziani...)
- Posizionamento competitivo differenziale rispetto ai player tecnologici

RISCHI

- Cyber risk
- Furto di dati e violazione privacy
- Impatti sociali

Hanno partecipato alla predisposizione del presente Quaderno:

Liliana Cavatorta
Capo Progetto - Responsabile Emerging and Reputational Risk
Gianluca Rosso – Emerging and Reputational Risk
Prof. Egeria Di Nallo
già Direttore del Dipartimento di Sociologia dell'Università di Bologna
Marco Lanzoni – SCS Consulting

Il Gruppo di lavoro si è avvalso del supporto del Tavolo Tecnico dell'Osservatorio R&ER e della sponsorship della funzione Risk Management nella persona di Gian Luca De Marchi.

unipol.it

Unipol Gruppo S.p.A.
Sede Legale
Via Stalingrado, 45
40128 Bologna