

LA PROTEZIONE DATI DA 25 ANNI LA BUSSOLA DEL FUTURO

CONTRIBUTI



Atti del Convegno in occasione delle
Celebrazioni per i 25 anni del
Garante per la protezione dei dati personali

Torino, 4 luglio 2022

a cura di
Agostino Ghiglia



LA PROTEZIONE DATI DA 25 ANNI LA BUSSOLA DEL FUTURO

CONVEGNO IN OCCASIONE DELLE CELEBRAZIONI
PER I 25 ANNI DEL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

TORINO, 4 LUGLIO 2022

a cura di
Agostino Ghiglia

INDICE

PAG.

PREFAZIONE <i>a cura di Agostino Ghiglia</i>	9
<hr/>	
SALUTI ISTITUZIONALI	13
<hr/>	
- Prof. Stefano Lo Russo	
- On. Alberto Cirio	
- Sen. Gilberto Pichetto Fratin	
<hr/>	
KEYNOTE SPEECH	
- Agostino Ghiglia	23
<hr/>	
Prima sessione	
LE COSTITUZIONI DEL METAVERSO: OCCORRONO META-LEGGI?	35
<hr/>	
- COSTRUIRE INSIEME IL METAVERSO Stefano Fratta	37
- COME REGOLAMENTARE I METAVERSIS Francesco Pizzetti	42
- DAL METAVERSO ALLA METACITY: IL FUTURO DELLE PROSSIME GENERAZIONI Derrick de Kerckhove	53
- RELIGIOSITÀ E SPIRITALITÀ NEL METAVERSO. UN CONTRIBUTO PER CUSTODIRE L'UMANO AL CENTRO Luca Peyron	56

Seconda sessione	
AI, SMART CITY, IoT, AUTO CONNESSE: FUTURO, INNOVAZIONE, LAVORO	63
<hr/>	
- MOBILITÀ E DIGITALIZZAZIONE. SCENARI, TRAFFICO, VEICOLI, PERSONE Mauro Velardocchia	65
- L'INTELLIGENZA ARTIFICIALE IN ITALIA: STRATEGIE PRESENTI E PROSPETTIVE FUTURE Barbara Caputo	74
- NUOVE PROTESI COGNITIVE? I DATI AI TEMPI DELL'INTERNET DELLE COSE Anna Maria Mandalari	76
- INNOVAZIONE, AI & IoT: RIFLESSIONI DEI PROFESSIONISTI Paola Zambon	82
- PRIVACY E GESTIONE DEI DATI, VALORE E RISCHI DI UNA SINERGIA Marco Gay	88
Terza sessione	
IL GARANTE DEL FUTURO	91
<hr/>	
- INTERVENTO DI Pasquale Stanzione	93
- SANITÀ DIGITALE E PROTEZIONE DEI DATI PERSONALI: UN BINOMIO POSSIBILE Ginevra Cerrina Feroni	98
- METAVERSO, PRIVACY E FUTURO Guido Scorza	103

Quarta sessione L'ERA DELLA CYBERWAR

109

- INTERVENTO DI Adolf Urso	111
- CYBER-RESILIENCE: L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE Annunziata Ciardi	116
- LA DIFESA E IL CYBERSPACE Carmine Masiello	120
- LE SFIDE GLOBALI DEL CYBERCRIME, COME DIFENDERSI E IL RUOLO DELLA GUARDIA DI FINANZA Marco Menegazzo	125

Quinta sessione L'INFORMAZIONE NELL'ERA DIGITALE: VERO, FALSO O VIRTUALE?

143

- MODERA: Baldo Meo
- Martina Pennisi
- David Puente
- Raffaele Barberio
- Massimiliano Panarari
- Federico Ferrazza



**Convegno in occasione delle Celebrazioni per i 25 anni del
Garante per la protezione dei dati personali**

4 luglio 2022 – 8,30-18,00

Torino, Palazzo Reale Salone delle Guardie Svizzere

La protezione dati: da 25 anni la bussola del futuro



CON IL PATROCINIO DI

**INIZIATIVA FINANZIATA DAL MISE CON
IL FONDO A VANTAGGIO DEI CONSUMATORI**



CITTÀ DI TORINO

**E' POSSIBILE VEDERE LA REGISTRAZIONE
DELL'EVENTO E LE INTERVISTE AI PROTAGONISITI
SUL SITO WWW.GPDP.IT**



PREFAZIONE

Dott. Agostino Ghiglia

Componente del Garante per la protezione dei dati personali

Son passati 26 anni o 1 secolo?

L'anno scorso, iniziando dalla sala della Protomoteca di Roma, passando per il Palazzo Reale di Torino e il Museo di Pietrarsa a Napoli, concludendo con un bellissimo incontro con gli studenti al Teatro Argentina, abbiamo celebrato i primi 25 anni del Garante per la Protezione dei Dati Personalini.

Sono stati anni intensi che hanno non solo accompagnato la storia degli italiani ma ne hanno modificato usanze, costumi, abitudini consolidate, spesso sotto traccia, a volte con importanti iniziative da parte dell'Autorità.

Da 25 anni, quindi, si parla di Privacy o, meglio, di protezione dei dati personali, talvolta a sproposito talora (ancora) con uno sbuffo annoiato ma, grazie all'attività dei Garanti che si sono succeduti nell'ultimo quarto di secolo, sempre più spesso con la consapevolezza che la protezione dei nostri dati personali e della nostra riservatezza equivale alla protezione della nostra libertà.

Il “right to be let alone” ossia il diritto alla tutela della nostra sfera più intima, alla solitudine dell’*io* e il “right to be forgotten” ovvero il diritto all’oblio e alla cancellazione dei nostri dati (e della nostra storia) quando non più necessari per le finalità cui era sottesa la loro raccolta (e la loro pubblicità), sono entrati a far parte del nostro immaginario: percepiamo la necessità che tali diritti esistano.

Mi permetto, prima di procedere con il ragionamento, una digressione: sono personalmente e profondamente convinto del potere profondamente simbolico delle parole, della comunicazione emotiva.

Se, infatti, cancellassimo il termine privacy sostituendolo, sempre, con “personal data protection” e, in Italia, con “protezione dei dati personali”, credo che saremmo molto più “popolari”, immediatamente percepiti come indispensabili (soprattutto nella nascente era digitale) e il RGDP

diventerebbe più che un regolamento, una preziosa “linea guida” per lo stile di vita del XXI secolo.

Parlando di “protezione” e di “personale”, infatti, la nostra amigdala viene immediatamente colpita da richiami ancestrali tesi alla preservazione della nostra intimità (e della serenità del nostro gemello digitale), trasformando così lo sbuffo verso “l’ennesima regola” in un sospiro verso “la” regola.

Ragion per cui è con orgoglio che, nella scia dei personaggi illustri che hanno disseminato e fatto crescere la consapevolezza della protezione del dato personale, ogni giorno cerchiamo di coltivarla e affinarla con la nostra attività.

Fatta questa premessa, la domanda che mi pongo è: sono passati 25 anni o un secolo?

La risposta è resa ancora più difficile da un’accelerazione tecnologica cui l’essere umano non è ancora preparato e, nella maggioranza dei casi, neppure consapevole; uno scatto che pone di fronte ad una vera e propria prova di resistenza: la protezione dei diritti che tutelano la dignità delle persone.

Migliorare la consapevolezza della protezione dei dati nell’era digitale, invero, è un compito estremamente arduo perché significa difendere e preservare i diritti fondamentali nei confronti dei colossi privati della tecnologia, tesi più al business che alla tutela delle persone ma anche, talvolta, nei confronti degli attori pubblici i quali, spesso in buona fede e nel tentativo di dare risposte veloci ai cittadini, rischiano di perdere di vista l’indispensabile bilanciamento tra diritto ed efficienza, tra difesa dei cittadini e invasività nelle loro vite, tra doverosa presenza e pervasiva immanenza nella loro sfera privata.

A tal proposito, mi preme particolarmente sottolineare la funzione di preservare il diritto alla protezione di dati personali nell’era digitale, evo improntato al “pensiero fuggevole” e alla velocità imposta dalla proposizione di sempre nuovi e sempre più rapidi e superficialmente evanescenti stili di vita.

E’ indispensabile, quindi, salvaguardare la protezione dei dati

personal, il diritto alla nostra intimità giacché è ciò che non muta e non deve mutare lasciandosi inerzialmente trascinare dal vento di un progresso tecnologico, quello dell'era digitale, che non rappresenta una semplice evoluzione ma una vera e propria rivoluzione sociale, culturale, economica, addirittura antropologica.

Ma oltre a questo compito “alto”, di custodi dei dati personali, ci sono le mille e mille questioni di una quotidianità sempre più complessa che vede il RGPD come snodo e presidio ineludibile dei diritti del terzo millennio: dalla realtà virtuale, alla sorveglianza remota estesa quando non di massa, dalle nuove frontiere della medicina predittiva basata sui dati, alle smart cities, ai *gatekeeper* (“nuovi tiranni” identificati nei grandi *provider* internazionali, coloro che gestiscono l’accesso alla nostra vita digitale) di rifkiniana memoria con le nuove spunte blu di Twitter e Meta, dai chatbot relazionali alle app che imitano la voce, dal revenge porn al cyberbullismo, dai data breach alla telecamera mal direzionata del vicino di casa....un sommario di voci e competenze in parte antiche e in gran parte nuove in un’era in cui il dato personale che circola tramite il nostro gemello digitale, diventa sempre più centrale nella nostra vita quotidiana.

Per tutti questi motivi, e per molti altri che non riesco ad immaginare mentre andremo in stampa, è essenziale un Garante più forte e potenziato nel suo organico, nelle sue intelligenze e trasformato nelle sue competenze, per poter continuare ad essere un'avanguardia e allo stesso tempo un vigile guardiano nella protezione dei diritti.

Il compito più arduo, infine, che sentiamo come dovere fra i doveri, è quello di contribuire ad educare e proteggere le nuove generazioni, creando in loro - protagonisti di una nuova era - la coscienza che la tecnologia è bifronte e che debbono crescere imparando a dominarla e non a diventarne succubi inconsapevoli e fruitori passivi e, a tal proposito, anche in questa occasione, mi preme riproporre l’idea dell’educazione civica digitale quale materia di studio nelle scuole: solo la consapevolezza della nuova era e dei suoi linguaggi potrà formare la coscienza individuale e collettiva delle nuove generazioni.

Per tutti i sopraccitati motivi, dopo aver pensato per un attimo di far redigere le mie considerazioni da un *chatbot* e aver pensato di farle leggere con la voce del mio allenatore di calcio preferito, ho pensato che fosse meglio, in una visione antropocentrica del diritto, fare da solo senza dimenticare che, concludo con questa riflessione, qualcosa e, non qualcuno, avrebbe potuto sostituirmi.



SALUTI ISTITUZIONALI



- **Prof. Stefano Lo Russo**
Sindaco della Città di Torino
- **On. Alberto Cirio**
Presidente della Regione Piemonte
- **Sen. Gilberto Pichetto Fratin**
Vice Ministro dello Sviluppo Economico

Saluti del Sindaco della Città di Torino
Prof. Stefano Lo Russo

Grazie a tutte e tutti voi, sono molto contento di essere qui in questo luogo così importante per la storia della nostra città, ringrazio l'Autorità per aver scelto la nostra città come sede di questo convegno nazionale per celebrare i 25 anni di attività dell'Authority.

Mi consentirete anche una qualche riflessione di carattere politico sull'attualità: oggi si celebrano 25 anni di un'Istituzione che il nostro paese si è dato quale organo a tutela del cittadino come bene ha espresso il componente On. Agostino Ghiglia. La privacy è una delle condizioni di una democrazia liberale, dove i diritti a tutela della sfera personale hanno avuto un crescente interesse tra i cittadini e anche nelle norme. In una democrazia in cui la sovranità appartiene al popolo attraverso un meccanismo democratico di selezione della classe dirigente dove al cittadino è garantito il rispetto delle prerogative proprie dei diritti fondamentali liberali. Mai come in questo momento, il tema delle garanzie delle libertà è quanto mai attuale, soprattutto in questa fase così complessa della vita europea, con una guerra d'invasione in Europa, una guerra che nessuno immaginava e nessuno poteva prevedere. In questo caso assistiamo alla violazione del più evidente dei principi alla base del diritto internazionale: inviolabilità dei confini e la volontà popolare rispetto alla propria sovranità.

Il ruolo dell'UE è assolutamente crescente e strategico, quando parliamo di difesa anche attraverso le nuove tecnologie, assume quindi un ruolo centrale nella competizione globale della Digital age del XXI secolo e si comprendono le resistenze in atto da parte delle Big Tech all'evoluzione della normativa europea in tema di circolazione dei dati e del ruolo della privacy nell'epoca digitale.

E' evidente come il tema di oggi, l'attività della Authority diventi quanto mai essenziale. Lo era già 25 anni fa, quando non c'erano nelle nostre tasche telefonini quando non c'era neanche Internet, quando tutto quello ci riguarda aveva un'accessibilità decisamente minore, ora con la rivoluzione digitale sono entrate prepotentemente anche nella nostra vita quotidiana.

Infine il mio augurio per lo svolgimento del convegno. Ovviamente il mio sostegno a questa vostra attività va anche nell'ottica e, qui concludo, riprendendo quanto diceva il Componente del Collegio dell'Autorità Garante Agostino Ghiglia: è bene che chi ha la responsabilità di gestire dati sensibili mantenga un alto livello di autonomia e terzietà. È un principio che tutela tutti. Oggi la proprietà del dato, soprattutto nel mondo digitale, diventa condizione essenziale, diventa condizione e fattore economico. Determinante anche il fattore di influenza politica. E i casi sono numerosi in tutto il mondo.

Determinante quindi il lavoro, il ruolo che ha l'Authority, che non è solamente quello di un rispetto formale dei dispositivi comunitari italiani di garanzia e di tutela, ma diventa un ruolo sostanziale nella tenuta dell'equilibrio democratico, nella valorizzazione di quello che ribadisco essere il concetto stesso di democrazia liberale e lo è, a maggior ragione, adesso nel momento in cui tutte le nostre vite sono sostanzialmente costantemente interconnesse. Quindi buon lavoro Presidente, buon lavoro a tutto il Collegio.

Saluti del Presidente della Regione Piemonte On. Alberto Cirio

Grazie Agostino e buongiorno a tutti.

Benvenguti in Piemonte, benvenguti a Torino. Innanzitutto benvenguto Presidente, benvenguto a tutto il Collegio, un saluto cordiale a tutte le Autorità: le autorità militari, le autorità civili, le autorità religiose che sono quest'oggi con noi.

Abbiamo aperto, Signor Presidente, il salotto buono, come si fa nelle case di campagna, dove sa che c'era quel salotto dove si passava solo ma dove non ci si sedeva se non quando arrivavano gli ospiti importanti.

Ecco per noi voi siete ospiti importanti, non soltanto perché la vostra presenza qui avviene attraverso una energia preziosa del nostro Piemonte che è Agostino Ghiglia che è una persona di valore, che oggi siede all'interno del suo Collegio, Signor Presidente, ma anche soprattutto perché noi crediamo molto nel vostro lavoro. E soprattutto nella necessità, come voi scrivete negli atti del vostro convegno di oggi, di accompagnare le Istituzioni verso quello che è il futuro.

Ecco questa parola “accompagnare” è fondamentale, perché per accompagnare qualcuno devi starvi insieme e noi, se una cosa abbiamo imparato, è che solo insieme potremo uscire da questa crisi in cui siamo quotidianamente costretti a vivere, che sia la crisi della post pandemia o pandemia di ritorno, che sia la crisi dell'aumento dei costi delle materie prime, della crisi energetica, la crisi della guerra, la crisi della siccità.

Usciamo da questa situazione così complicata solo se lavoriamo insieme, se ci aiutiamo, e noi abbiamo bisogno che le Istituzioni ci aiutino, abbiamo bisogno che lo Stato ci aiuti...quello Stato che è nato qui, che è nato in questa piazza dove c'è stato il primo Senato d'Italia. Un valore per noi, non soltanto romantico e di passione per l'orgoglio della nostra storia, ma anche un valore di prospettiva. Quindi credo che non ci fosse luogo migliore per celebrare i vostri 25 anni che lavorare qui.

Noi abbiamo peraltro, sul tema della tutela dei dati personali, un'attenzione particolare perché la Regione, secondo la nostra Costituzione,

ha la competenza sulla salute, sulla sanità e quindi abbiamo tutto il tema della gestione dei dati sanitari delle persone.

Un aspetto che io ho vissuto prima da legislatore qualche anno fa al Parlamento europeo, quando ho approvato anch'io l'ultima regolamentazione sulla tutela dei dati personali, quella vigente. E mi sono trovato quindi a doverla spiegare, perché era evidente che questo portasse una serie di adempimenti e oneri in più per tutti coloro i quali nella loro vita professionale avevano un contatto con dati personali, dati che andavano gestiti in una determinata maniera. Ma l'ho fatto con convinzione, perché era importante trasmettere all'opinione pubblica che stavamo andando nella direzione di tutelare la libertà delle persone.

Una cosa che io credo sarebbe opportuno fare oggi, e sarebbe opportuno che il nostro governo lavorasse in questa direzione, è spiegare di più ai cittadini cosa fa l'Authority, spiegare di più ai cittadini che quello che può sembrare un lacciolo, quello che può sembrare un adempimento burocratico in più, invece, è una tutela della libertà delle persone. A volte la regolamentazione fa arrabbiare Presidente: in questi due anni di pandemia mi trovavo, pensate, nella situazione di avere - per la Costituzione italiana - la responsabilità della salute dei miei cittadini, ma di non poter sapere se fossero vaccinati o no. Pensate che paradosso, ma poi affrontando il tema abbiamo trovato con tutte le Regioni d'Italia, con la Conferenza delle Regioni, con cui peraltro l'Authority è in stretto contatto, quell'equilibrio di lavoro comune che ci ha permesso da un lato di tutelare quella che era la giusta protezione dei dati personali, ma dall'altro di poter noi intervenire con quelli che sono i soggetti competenti a conoscere anche i dati personali. Ma è un tema questo, una riflessione, che dobbiamo portare di più tra la gente comune, dobbiamo spiegarlo di più.

Prima il sindaco Lo Russo ricordava le ricerche su Internet. La regolamentazione che noi approvammo al Parlamento europeo era proprio la limitazione di quelli che chiamano i cookies, cioè il fatto che accedendo a un motore di ricerca viene memorizzato quello che tu hai ricercato. Di fatto la regolamentazione ha imposto che si debba dire "sono d'accordo", ma se non lo fai si blocca la schermata e non è possibile proseguire nella ricerca. Va

spiegato però alla gente che un minuto dopo, se io cerco una cucina, quel motore di ricerca sa che Alberto Cirio cerca una cucina, ne prende i dati e li vende a chi commercializza le cucine. Questo passaggio è un qualcosa che introduce un'attività di marketing da parte di soggetti che, sapendo le mie esigenze, impostano poi le loro attività di vendita, però nello stesso tempo viola la libertà della persona. È quello che i supermercati hanno fatto tra i primi con le tessere di fedeltà. Pochi ricordano questo aspetto, ma una volta strisciata la tessera viene memorizzata la tua spesa. E lì dentro c'è la nostra vita. Dalla mia spesa è possibile sapere se ho delle persone anziane in casa, se ho i bambini, se ho degli animali. È possibile scoprire quelle che sono le mie esigenze.

Oggi il sistema sta cambiando. Internet prevede altri strumenti e quindi è giusto che ci siano altre garanzie per i cittadini. Ma questo, e chiudo caro Agostino, l'hai detto bene, citando il Presidente europeo, la gente deve capirlo. E dobbiamo noi per primi far capire loro che questa è davvero, una battaglia di libertà. Perché non c'è libertà se non c'è tutela di quelle che sono le inclinazioni personali di ciascuno, che appartengono alla sfera individuale e che nessuno può avere il diritto di non rispettare. Anzi, non devono neanche conoscerle.

Ci sono degli aspetti dell'individuo che devono rimanere nella riservatezza dell'individuo stesso. Il rispetto è il passo successivo, perché per rispettare devi già conoscere, ma noi dobbiamo fare un passo prima: la mia identità personale è giusto che sia patrimonio mio e di chi voglio io.

Quindi, grazie di aver scelto Torino e grazie della libertà che ci trasmettete oggi.

Saluti del Vice Ministro dello Sviluppo economico Sen. Gilberto Pichetto Fratin

Buon compleanno al Garante!

Un grazie al Presidente Stanzione e naturalmente a tutto il Collegio, ad Agostino che non riesco a non immaginare nel ruolo di “componente” del Collegio e che per me continua a essere semplicemente “Agostino”.

Sono contento di essere qui a esprimere la stima a nome del Ministero dello Sviluppo Economico e del Governo nazionale in questo passaggio significativo anche dal punto di vista territoriale, perché è importante far conoscere a livello locale il ruolo del Garante e la sua rilevante funzione.

Peraltro, con il Ministero dello Sviluppo Economico, come delegato anche alle carte valori, abbiamo riconosciuto l'importanza di questi venticinque anni con l'emissione di un francobollo che è simbolo dello Stato. Il Ministero dello Sviluppo Economico, infatti, ha il ruolo di riconoscere il simbolo dello Stato a chi è meritevole di essere citato e di poter passare alla storia, al di là di quella che è la funzione postale.

Il compito dell'Autorità del Garante è stato già tratteggiato, quindi non dico altro. Devo aggiungere, però, che, leggendo il programma ho notato un'evoluzione del ruolo: se forse trent'anni fa si poteva parlare di giornali rispetto alla privacy, oggi ho trovato termini come “metaverso” e “smartcity”: queste sono le nuove frontiere.

L'utilizzo dei moderni strumenti dell'intelligenza artificiale rischia, però, di essere qualcosa di incomprensibile e poi di non gestibile da parte del consumatore. Questo lo dico anche da Presidente del Consiglio Nazionale Consumatori Utenti, che deve tutelare e stimolare anche l'Autorità Garante nel tutelare la privacy in un momento particolare del nostro Paese e del mondo.

Ne ha parlato prima il Presidente Cirio: è un momento che ci vede in un cambiamento epocale perché abbiamo avuto la pandemia e non sappiamo quale sarà il punto di caduta di un nuovo quadro geopolitico. Dobbiamo fronteggiare l'inflazione che, chi ha meno di cinquant'anni, conosce se l'ha studiata sui libri di scuola e, quindi, c'è un moltiplicarsi di iniziative a fianco dello sviluppo tecnologico che rischiano di travolgere in particolare i più fragili.

Quindi la vostra funzione è anche proprio quella di tutelare i più fragili, coloro che rischiano di rimanere indietro. Ed è una sfida che tutti noi dobbiamo affrontare davvero, tenendo presente che fa parte della nostra visione.

Dunque, ancora buon compleanno al Garante della Privacy, al Consiglio e a tutti gli operatori.



KEYNOTE SPEECH



- **Dott. Agostino Ghiglia**

Componente del Garante per la protezione dei dati personali

KEYNOTE SPEECH

Dott. Agostino Ghiglia

Componente del Garante per la protezione dei dati personali

Ringrazio i rappresentanti delle Istituzioni: il Sindaco di Torino, Stefano Lo Russo, il Presidente della Regione Piemonte, Alberto Cirio e il Vice Ministro del MISE, Gilberto Pichetto Fratin.

Ringrazio i Parlamentari e le autorità accademiche e militari presenti nonché tutti gli “amici” della privacy che, da 25 anni, cooperano - assieme a noi - alla protezione dei nostri dati.

Ringrazio la dott.ssa Pagella, direttrice dei Musei Reali di Torino e Palazzo Reale per l’ospitalità nella incantevole cornice di Palazzo Reale

Ringrazio il Garante, dai Dirigenti a tutti i dipendenti, per l’enorme lavoro svolto a tutela della nostra Libertà e in questa occasione in particolare il Servizio Relazioni esterne e Media capitanato dal dott. Baldo Meo per il prezioso contributo alla realizzazione di questo appuntamento.

Ringrazio il mio staff (Cristiana Luciani, Licia Cristiano, Raffaella Bufo) per l’instancabile e intelligente supporto e, in questa occasione, in particolare la dott.ssa Alessandra Genisio per l’instancabile opera di raccordo.

Ringrazio, per ultimi, ma solo per enfatizzare col cuore il ringraziamento, i miei eccezionali Colleghi: il Presidente Pasquale Stanzione, la Vice Presidente Ginevra Cerrina Feroni, il Collega Professor Guido Scorzà; le nostre diversità trovano ogni giorno la sintesi per fare, parafrasando Andrea Jelinek Presidente del Comitato europeo per la protezione dei dati: *“il mestiere più bello del mondo: proteggere i dati delle persone e con essi la loro libertà”*.

E così “*ci sarà un pensatore che costruirà un cervello che sappia pensare esattamente*”. Sembra che Goethe¹, nel suo celebre Faust, avesse già

1) Goethe, Johann Wolfgang von. “Faust”, In Opere, vol. 2, a cura di Emilio Castellani, pp. 311-312. Torino, Einaudi, 1962.

previsto con una sorta di anticipazione profetica, quanto sta accadendo alla nostra società cibernetica, sempre più abbandonata, in un percorso quotidiano ormai prevalentemente inconsapevole, alla tecnica. Vite che, mescolandosi in un vincolo intrinseco di realtà e virtualità, scorrono tra le vie affollate delle nostre città e fiumi digitali di *bit*.

All'uomo, tuttavia, non è - e non deve essere - sufficiente far parte della realtà: l'uomo ha bisogno di sapere che "abita" il mondo e come lo abita. L'essere umano necessita di un ambiente dotato di un senso, un contesto nel quale tutto mantiene una certa relazione e la cui evidenza può appunto essere imparata, capita, spiegata. L'aspirazione umana non è mai stata quella di vivere in un ambiente chiuso dal determinismo biologico né, tantomeno, meccanico bensì in un mondo costituito da una realtà poliedrica: dalla realtà familiare, lavorativa, culturale, a quella affettiva, sociale, sino ad arrivare alla comunità nazionale a cui apparteniamo e, simbolicamente e materialmente, all'Umanità nel suo complesso e nella sua complessità.

Lo sviluppo ipersonico della tecnologia ci mette di fronte a scambi sino a pochissimi anni fa impensabili nei processi di interazione tra uomo e macchina. L'uomo si "macchinizza" e la macchina si umanizza... La priorità, la sfida dei prossimi anni quindi, è umanizzare la tecnica e non macchinizzare l'uomo rendendolo amorfo, un automa routinario che cede alle macchine troppa parte della sua vita.

La tecnologia, d'altro canto, risponde da sempre alla naturale vocazione dell'uomo all'azione e alla scoperta finalizzata ai suoi interessi vitali e produttivi. Potremmo allora affermare, da qui a qualche anno, che l'artificialità è qualcosa di meglio della naturalità e che la sua funzione - la funzione delle macchine - è quella di proteggerci dalla natura o di modificarla nel profondo, disumanizzandoci? Nell'attuale e futura società digitale la risposta, che potrebbe sembrare retorica, è ben lungi dall'essere banale e scontata.

Se le macchine debbono essere strumenti a servizio dell'uomo è fondamentale che l'uomo nell'utilizzarle non perda mai il controllo della sua individualità e della capacità di autodeterminarsi, che non confonda mai il mezzo con il fine e che, soprattutto, non deleghi il fine al mezzo.

Riusciremo a restare consapevoli della necessità di considerare una subordinata la parte “tecnologica” del nostro essere o la confonderemo e fonderemo man mano con la nostra umanità?

L'uomo, nel compiere delle scelte, riconosce una caratteristica profonda delle proprie azioni: il bene e il male. L'uomo, con il proprio libero arbitrio, matura un senso di responsabilità che appunto definiamo etica.

E’ l’etica, caratteristica umana che ci rende unici, si basa sui valori ma questi ultimi debbono basarsi a loro volta sulla conoscenza che è, prima di tutto, capacità di comprendere e capire e non su un’accettazione neo fideistica del futuro. Con l'avvento dell'era digitale tale capacità di comprensione dovrà essere sorretta inevitabilmente da nuove forme di educazione digitale; senza di essa il rischio è che venga meno il “*posse non peccare*” che Sant’ Agostino poneva fra le basi del libero arbitrio.

Anche la macchina effettua delle scelte su dei valori ma si tratta di valori numerici, relativi a dati. Se vogliamo, tuttavia, che la macchina, senza mai sostituirsi all’essere umano, sia di effettivo supporto all'uomo e al bene comune, allora gli algoritmi devono includere valori etici e non solo numerici e ciò significa che l’etica ha bisogno di contaminare l’informatica.

Sarà necessario regolamentare principi e norme etiche in un linguaggio comprensibile e fruibile dalle macchine perseguiendo lo studio e la codificazione di quella che Paolo Benanti, già nel 2018, definì “*algoretica*”². Solo così quella dell'intelligenza artificiale sarà una rivoluzione che porterà ad un autentico sviluppo non solo economico ma anche sociale e culturale. In una parola uno sviluppo “*umanamente sostenibile*”.

Cionondimeno quando si parla di valori etici, di limiti etici e morali - in questo caso relativi alle applicazioni e alle implicazioni dell’Intelligenza Artificiale - occorre premettere che nonostante esistano oggi valori largamente condivisi e sovente riconosciuti in quasi tutte le zone del pianeta , non si può non considerare che le radici culturali, quindi i valori morali, siano differenti

2) Benanti, Salvatore, “*La sfida etica dell'intelligenza digitale*” in *Le nuove frontiere della tecnica e della scienza. Il futuro tra tecnologia, etica e diritto*, a cura di Mauro Nicolini, p. 71-84. Aracne Editrice, 2018

da paese a paese e differentemente osservati e metabolizzati , soprattutto laddove non vi siano norme giuridiche che li recepiscono o costituzioni che li identifichino come valori da proteggere.

Noi occidentali abbiamo ancora una tendenza ottocentesca a presumere che la nostra “*Weltanschauung*”, la nostra visione del mondo, sia “la visione” oggettiva ed oggettivabile, quindi esportabile. Non è più, neppure numericamente, vero. Non sembra perciò azzardato ritenere che un’ulteriore difficoltà stia proprio nel pensare algoritmi universali alla base della futura Intelligenza Artificiale; algoritmi “valoriali” accettati da una nuova “ONU digitale”.

A tal proposito, la scelta dell’Unione Europea di dotarsi di un Regolamento generale sull’Intelligenza Artificiale (*Artificial Intelligence Act* del 21 aprile 2021) appare fondamentale ma la sua approvazione definitiva è sempre più urgente. L’auspicio o, meglio, la necessità indifferibile, è che la discussione in corso produca armonizzazione e certezza del diritto su cui si deve fondare l’affidabilità dell’utilizzo della tecnologia, senza ovviamente costituire un freno al progresso e alla ricerca. Ci troviamo, però, di fronte un’altra esigenza egualmente importante: la velocità decisionale; non sembri un paradosso dire che il futuro ci incalza, ci sprona a fare bene ma a farlo presto.

Come il GDPR ha avviato la “rivoluzione” globale della Protezione dei dati (ricordiamo che ha richiesto più di quattro anni di negoziazione e sei anni prima dell’entrata in vigore), anche il Regolamento sull’IA dovrà auspicabilmente diventare uno standard globale traendo influenza e ispirazione dal GDPR e fungendo da catalizzatore per un processo di regolamentazione internazionale. È in gioco non solo la pura certificazione di nuovi strumenti tecnologici a protezione dei dati personali (e non) a cui le Autorità di Garanzia debbono, a mio avviso, candidarsi quali controllori e supervisori, ma il tracciamento delle coordinate su cui fondare un nuovo modello di società. Una società nella quale componenti umane e non umane saranno chiamate a convivere in modo duraturo, secondo un innovativo principio di sussidiarietà tecnologica in cui, come detto prima, l’entità di livello superiore rimanga l’uomo.

La sfida etico-tecnologica che abbiamo di fronte richiede, dunque, un impegno trasversale che, spronato da un rinnovato e celere attivismo normativo, coinvolga non solo la comunità accademica ma tutti coloro - Istituzioni e società civile - che hanno a cuore la crescita e lo sviluppo umano in una società che, nello sfruttare l'enorme potenziale delle nuove tecnologie, garantisca il rispetto dei diritti e delle libertà fondamentali degli individui.

Dobbiamo essere consapevoli che la rivoluzione digitale in atto non è semplicemente un'evoluzione tecnologica ma una nuova scoperta del fuoco che porterà, però, ad una tempistica evolutiva difficilmente immaginabile.

In tale ambito, la nostra Autorità dovrà assumere un ruolo centrale nella definizione di regole che, coniugando innovazione tecnologica e diritto, consentano di congiungere i benefici offerti dal progresso scientifico con la garanzia del rispetto della dignità e dei diritti fondamentali della persona.

Il complesso delle norme che garantiscono la libertà della persona fisica (*habeas corpus*) necessita di essere rinnovellato come “*habeas mentem*” a fronte delle nuove, quotidiane, indefinibili ed inimmaginabili minacce e ai possibili condizionamenti che i sistemi di intelligenza artificiale possono avere per la mente della persona in termini di libertà decisionale.

L'algoritmo va circoscritto nel suo uso. Vale qui ricordare l'art. 22 par. 1 del GDPR che recita: “*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*” (salvo deroghe per stipula di un contratto o consenso dell'interessato).

Tale norma, sancendo tra l'altro il diritto alla revisione umana della decisione automatizzata e il divieto di discriminazione, già esercita un freno a eventuali invasioni e predominanze dell'algoritmo sulle scelte che deve compiere l'uomo. Conseguentemente le Autorità di protezione dati possiedono, già oggi, i requisiti di competenza, di intelligenza umana, di storia e consuetudine per garantire il miglior approccio al tema, minimizzando i rischi e le criticità che, indubbiamente, possono generarsi

con l'utilizzo dei sistemi di intelligenza artificiale. Per questo motivo, le Autorità di Protezione dei Dati vanno tempestivamente e convintamente potenziate, dotandole di robuste risorse umane nel settore tecnologico da affiancare ai più tradizionali comparti giuridici.

Se finora l'utilizzo delle tecnologie informatiche ha visto l'uomo interagire con l'ambiente intermediato da sistemi ICT - e sui quali l'uomo possedeva comunque il controllo - l'ecosistema che viene a costituirsi con l'utilizzo combinato di tecnologie quali l'*Internet of Things*, i *Big Data*, il 5G, agenti intelligenti ed i sistemi di Intelligenza Artificiale, impone un radicale cambio di paradigma: l'uomo diviene fruitore del servizio reso dal sistema, delegando parzialmente o totalmente al medesimo il controllo dell'interazione con l'ambiente.

L'utilizzo delle tecnologie, in un ecosistema digitale che vede l'Intelligenza Artificiale come elemento centrale del nuovo paradigma tecnologico, potrebbe divenire un formidabile strumento di progresso a favore dell'umanità anche quando avrà la capacità di comprendere le nostre sensazioni, i nostri stati d'animo, le nostre emozioni e pulsioni più profonde? Se la risposta è sì, a fronte di un'informatica emotiva sarà necessario prevedere tutele per garantire l'autonomia dell'individuo nel processo cognitivo prima che volitivo.

In caso contrario le sterminate applicazioni dell'Intelligenza Artificiale, anche nei suoi impieghi più banali come la domotica o gli *smart assistant*, rischiano di diventare abitudine inconsapevole, gestualità routinaria, profilazione passiva ed inconsapevole di atteggiamenti, gusti, emozioni.

Quando gran parte delle nostre scelte possono essere catturate da sensori, impastate e sintetizzate tramite il *machine learning* il quadro delle garanzie per l'individuo, evolvendosi, deve rimanere la solida base prima accennata: una combinazione tra principi etici del trattamento e i principi fondamentali di protezione dei dati personali - tra cui legittimità del trattamento, trasparenza, "esplicabilità" delle operazioni di trattamento, minimizzazione dei dati, sicurezza del trattamento - che costituiscono un riferimento imprescindibile a tutela della libertà e della coscienza individuale e collettiva.

Come dice lo storico Yuval Noah Harari, nel rimettere l'uomo al centro della nuova narrazione del XXI secolo: “*in un mondo alluvionato da informazioni irrilevanti, la lucidità è potere*”.

La lucidità nel rimanere profondamente umani e critici, non solo pigri individui digitali, cresciuti con una cultura digitale che se sostituirà quella tradizionale, rischierà di “produrre” una società profilata e neo massificata.

Senza dubbio ci stiamo addentrando nel web 3.0 dove la realtà virtuale e la realtà aumentata consentiranno di “vivere” un mondo in cui le esperienze virtuali 3D si fonderanno con quelle fisiche.

Come non fare un accenno, allora, al Metaverso e agli Ultraversi? Nel 2004, nasceva Facebook e con esso la “*social age*”. Oggi, tale strumento (che vanta ancora 3 miliardi di adepti) non rispecchia più i gusti dei *millennials* né, tantomeno delle generazioni X e Y, e allora, oltre un anno fa, Mark Zuckerberg ha lanciato Meta, non una semplice rivisitazione del marchio ma un’idea diversa: una realtà virtuale, aumentata, in cui i nostri avatar attraverso il visore *Oculus* vivranno, ameranno, acquisteranno...

In questa nuova “realità” - ancorché lontana a causa degli enormi problemi gestionali e di interoperabilità tra “mondi” che comporta - non sarà più necessario usare Photoshop: ci saranno esseri digitali, donna o uomo, che si muoveranno e “vivranno” al posto nostro.

Per inquadrare meglio il tema ricordiamo due numeri: i social network contano circa 4,6 miliardi di utenti pari al 58,4% della popolazione; trascorriamo sui social network circa due ore e mezza al giorno che diventano oltre quattro nella fascia tra gli 11 e i 18 anni.

C’è da chiedersi se il Metaverso sia già fra (in) noi. Meta. inoltre, è solo uno dei 141 ultraversi finora censiti (al momento della pubblicazione di questo libro); tra questi ci sono DECENTRALAND, in cui si crea il proprio avatar e si ha la possibilità di acquistare e rivendere lotti di terra tramite una valuta Mana; EARTH 2, metaverso in cui l’intero pianeta è stato suddiviso in una griglia di appezzamenti da 10x10 metri da vendere ai migliori offerenti e sui quali si potrà costruire la propria attività commerciale; FORTNITE, ... e via con la fantasia! Gli ultraversi supereranno il livello

di giochi virtuali, immersivi e aumentati per, pochi, benestanti? “Il Futuro è un’ipotesi” come canta Ruggeri.

Nonostante il Metaverso sia, ad oggi, solo un termine di moda di cui tanti parlano e di cui pochi conoscono il significato o, meglio, le reali potenzialità e il vero stato di attuazione, giova ricordare i numeri che ruotano attorno ai metaversi (nel 2021, infatti, ci sono stati 500 milioni di dollari di vendite nel Metaverso, cifra stimata ad 1 miliardo per l’anno corrente con una crescita prevista nei prossimi anni del 32% fino al 2028).

Purtuttavia tali cifre, che ci appaiono enormi, rappresentano una particola rispetto ai miliardi di investimenti operati delle piattaforme che li creano e li gestiscono, con risultati negativi che hanno sin qui portato al licenziamento di decine di migliaia di lavoratori impegnati nel “metasettore”.

Giova, tuttavia sottolineare come il volume dei dati o dei metadati che si stanno generando, e che si conserveranno negli ultraversi, risulta infinitamente superiore a quelli acquisibili nel web, così come lo abbiamo conosciuto fino ad oggi. L’utente non avrà più bisogno di fornire in modo proattivo i dati personali accedendo al proprio smartphone e utilizzando una delle tante app. Piuttosto i suoi dati saranno raccolti in background mentre svolgerà la propria vita virtuale.

Molto diversa anche la tipologia e la qualità dei dati ottenuti: si pensi alla possibilità di acquisire lo “sguardo” dell’utente, la dilatazione dei pori in ottica predittiva, o determinate emozioni e movimenti che i cd. visori virtuali - *headset* - potranno raccogliere.

Per non parlare dei dati biometrici raccolti che comporteranno l’inevitabile necessità di ripensare profondamente la verifica del consenso da parte degli utenti e, soprattutto, dei minori.

A questo punto è lecito ipotizzare un metaverso per soli maggiorenno, o, quantomeno, per over 16?

Preoccupazione legittima se si considera che i metaversi potrebbero creare molte nuove tipologie di illeciti e reati anche - ma non solo - attraverso l’uso di tecniche di sovrapposizione dell’immagine umana basate sull’Intelligenza Artificiale (cd. *deepfake*) che risulteranno ancora più gestibili con gli *avatar*.

Sarà fondamentale una revisione della normativa sui reati informatici che risale al 1993.

Strettamente collegato a quanto sopra è il mercato degli NFT - *token* unici, non fungibili e, quindi, non sostituibili né replicabili che possiedono un valore digitale - con la possibilità di effettuare transazioni in cryptovalute che necessiterà, inevitabilmente, di garantire un adeguato processo di gestione delle procedure antiriciclaggio e anti evasione conferendo, per contro, una maggiore certezza agli scambi di valore che, peraltro, dato lo strumento, sono immutabili e quindi definitivi.

In conclusione, i metaversi e lo sviluppo digitale in generale pongono problemi etici e giuridici rivoluzionari, ulteriori rispetto a quelli sopra evocati dalle innumerevoli estrinsecazioni dell'IA.

D'altronde siamo entrati ufficialmente in un'epoca nuova, radicale: la *Digital Age*. Viviamo già una realtà doppia e parallela. Si può davvero pensare di tornare indietro o pretendere di bloccare tutto ciò? Se in questo caso la risposta è no, occorrerà un profondo cambiamento a cominciare da forme scolastiche di educazione digitale per far sì che le nuove generazioni siano padrone e consapevoli del proprio futuro, non oggetti di consumo (dei loro dati personali e sensibili) o avatar prigionieri in un'esistenza virtuale. Non mi sembra eccessivo, o fantascientifico, sostenere che l'avvento ovvero il sopravvento dell'era digitale - dallo SPID alla CIE, dai metaversi al "semplice" e-commerce - rappresenti una rivoluzione epocale senza precedenti (se non nel Paleolitico inferiore, con il fuoco...) che modificherà il nostro modo di vivere ad una velocità evolutiva che non ha paragoni nei secoli recenti.

È importante, insomma, creare e diffondere consapevolezza, sensibilità, cultura di fronte a cambiamenti che i nonni Orwell o Asimov (eh sì, ormai molto antichi pure loro) neppure avrebbero sognato affinché non si avveri la profezia di Nietzsche contenuta nel libro "*Umano, troppo umano*": tutta la vita umana è profondamente immersa nella non verità"

Sarà, questa, la sfida per i prossimi 25 anni?

PRIMA SESSIONE



LE COSTITUZIONI DEL METAVERSO: OCCORRONO META-LEGGI?



- COSTRUIRE INSIEME IL METAVERSO
Dott. Stefano Fratta
- COME REGOLAMENTARE I METAVERSIS
Prof. Francesco Pizzetti
- DAL METAVERSO ALLA METACITY: IL FUTURO DELLE
PROSSIME GENERAZIONI
Prof. Derrick de Kerckhove
- RELIGIOSITÀ E SPIRITUALITÀ NEL METAVERSO.
UN CONTRIBUTO PER CUSTODIRE L'UMANO AL CENTRO
Don Luca Peyron

PRIMA SESSIONE*

LE COSTITUZIONI DEL METAVERSO: OCCORRONO META-LEGGI?

COSTRUIRE INSIEME IL METAVERSO

Dott. Stefano Fratta

Emea Privacy Policy Director at Meta

Da quando Mark Zuckerberg ha annunciato il nuovo nome dell'azienda (oggi, Meta) e la sua volontà di contribuire alla realizzazione del Metaverso, alcuni temi considerati di nicchia sono diventati oggetto di un intenso confronto pubblico e politico.

Oggi abbiamo un'occasione unica per discutere opportunità e sfide della rivoluzione digitale del Web 3.0. Per la prima volta infatti, il quadro regolatorio non dovrà intervenire su una tecnologia già completamente realizzata, ma potrà evolvere contestualmente al suo sviluppo.

Se dovessimo darne una definizione generale, potremmo dire che il Metaverso è un insieme di spazi digitali interconnessi e accessibile attraverso una molteplicità di dispositivi e tecnologie diverse: occhiali per la realtà aumentata, visori per la realtà virtuale, personal computer, smart display e cellulari. Il Metaverso ha la potenzialità di rendere le nostre esperienze *online* più realistiche, consentendoci così di andare oltre le due dimensioni dell'Internet odierno.

Il metaverso e le realtà immersive vengono accolte con entusiasmo in alcuni ambienti e approcciati con scetticismo in altri. È facile però comprenderne il motivo, specialmente quando la società già si interroga sul modo in cui la tecnologia opera nel mondo - bidimensionale - di oggi.

Quando Facebook è nato 18 anni fa, la navigazione online era limitata per lo più alla fruizione e alla redazione di testi scritti. Con l'arrivo degli smartphone, dotati di fotocamere sempre più sofisticate, le foto hanno assunto

* La sessione è stata moderata dalla dott.ssa **Martina Pennisi**, Corriere della Sera

un ruolo centrale nelle interazioni digitali, la comunicazione è diventata sempre più visiva e Internet ha fatto sempre più affidamento sulle immagini. Inoltre, man mano che le connessioni sono diventate più veloci, i video si sono affermati come mezzo privilegiato per condividere e comunicare la propria quotidianità. Il Metaverso, quindi, non è che il prossimo naturale passo del percorso tecnologico fatto fino ad oggi: un'esperienza che non sarà più bidimensionale, ma immersiva e, di conseguenza, molto più coinvolgente e realistica.

Tre sono i fattori chiave che renderanno le interazioni nel metaverso più simili a quelle della nostra vita quotidiana: cioè effimerità, presenza fisica e immersività.

L'effimerità sarà una caratteristica fondamentale delle nostre interazioni nel metaverso. Nel mondo fisico, quasi tutte le conversazioni che abbiamo sono "effimere"; vale a dire che non esistono registrazioni permanenti di ciò che diciamo nella nostra quotidianità.

Al contrario, le ricerche su internet, le email, gli SMS e i post scritti sui social media sono caratterizzati da una permanenza più duratura. Nel metaverso vi sarà un passaggio verso una comunicazione orale e diretta, proprio come nelle conversazioni faccia a faccia.

E se niente finora ha raggiunto un livello di percezione audiovisiva tale da ricreare la sensazione di condivisione degli spazi, come accade durante una conversazione con gli amici al bar o una riunione con i colleghi in ufficio, l'immersività del metaverso ci permetterà di comunicare con le altre persone come se ci trovassimo effettivamente insieme a loro. L'obiettivo delle tecnologie immersive, tuttavia, non sarà quello di sostituire lo stare insieme di persona. Al contrario, il metaverso potrà affermarsi come uno spazio complementare che renderà possibile creare comunità e vivere relazioni anche quando limitazioni di diverso genere impediscono di incontrarsi di persona.

Possiamo quindi immaginare il metaverso come un edificio in cui ogni piano sostiene quello superiore. Le fondamenta dell'edificio comprendono l'hardware (telefoni, visori per la realtà virtuale, occhiali per la realtà aumentata, ecc.), i protocolli e gli standard tecnici che garantiscono l'interazione tra le varie tecnologie - in gergo, la loro "interoperabilità". Il piano terra del metaverso sarà costituito da reti e piattaforme che realizzano i mondi 3D del

metaverso nella loro interezza. Il primo piano è invece quello popolato di esperienze a cui ciascun utente può accedere.

Per fare un esempio, gli utenti di *Quest*, il nostro visore VR, possono accedere ad esperienze virtuali che migliorano l'esperienza del lavoro online, come *Horizon Workrooms*.

In questo contesto, la realtà aumentata permette di combinare realtà e mondo virtuale, consentendo di visualizzare immagini virtuali sovrapponendole alla visuale dell'ambiente circostante tramite l'utilizzo di occhiali dotati di lenti trasparenti. Attraverso la realtà virtuale, invece, saremo in grado di immergervi in un ambiente tridimensionale totalmente digitale, grazie all'utilizzo di appositi visori. Nel loro complesso, le tecnologie alla base del metaverso ci permetteranno in modo semplice e coinvolgente di comunicare, rimanere connessi e in contatto grazie allo sviluppo di ologrammi e avatar.

Il fil rouge, in questa discussione, è l'interoperabilità, ovvero l'interconnessione di standard, sistemi e app che consentono alle persone di viaggiare facilmente da una parte all'altra del metaverso. Non si tratta di un assoluto: non tutti gli elementi delle esperienze del metaverso devono essere, o saranno, compatibili con gli altri. Tuttavia, senza l'integrazione di un grado significativo di interoperabilità in ogni piano, il metaverso risulterà frammentato e suddiviso in compartimenti stagni impenetrabili tra loro.

Per accelerare questo percorso è stato fondato il *Metaverse Standards Forum*. Il Forum esplorerà i punti in cui la mancanza di interoperabilità frena la diffusione del metaverso e in uno spazio collaborativo che coinvolge tra i membri fondatori, oltre a Meta, anche, Adobe, Alibaba, Autodesk, Epic Games, Google, Huawei, IKEA, Microsoft, NVIDIA, Qualcomm Technologies, Sony Interactive Entertainment.

Lo sviluppo del metaverso è quindi un processo collettivo, un percorso di sviluppo di un sistema di governance che coinvolge il settore privato, i legislatori, la società civile, il mondo accademico e le persone che useranno queste tecnologie.

AR e VR hanno la capacità di cambiare il modo in cui le persone interagiscono tra loro, e per questo è cruciale che lo sviluppo di queste tecnologie sia responsabile e trasparente. Il ritmo dei cambiamenti tecnologici

è molto veloce e può far nascere interrogativi o suscitare preoccupazioni ed è quindi fondamentale discutere di rischi e opportunità con tutti gli attori coinvolti nello sviluppo e regolazione del metaverso, come le istituzioni e le autorità di controllo. Il nostro impegno è finalizzato a migliorare la comprensione di queste tecnologie rivoluzionarie, perché riteniamo che sia il modo migliore per favorire l'innovazione e consentire a tutti di trarne vantaggio.

Da un lato, Meta ha lanciato, insieme a Essilor Luxottica, una campagna di sensibilizzazione su diversi mezzi di comunicazione allo scopo di migliorare l'accettabilità sociale e la consapevolezza intorno all'utilizzo degli occhiali smart, concentrando sulla spiegazione di come usare questi strumenti in modo responsabile da parte del grande pubblico.

Dall'altro, ci impegniamo affinché la riflessione sulla normazione delle realtà immersive cominci già oggi. Non c'è nulla di deterministico nel modo in cui una tecnologia interagisce con la società. La tecnologia, di per sé, non è né buona né cattiva. Pertanto, il suo impatto dipende dall'utilizzo che ne viene fatto ed è per questo necessario che si discuta insieme di come garantire uno sviluppo adeguato dell'ecosistema facendo tesoro di quanto imparato dallo sviluppo di quello esistente che riguarda Internet e i social media. Tuttavia, le regole non potranno essere identiche, in quanto per molti aspetti le esperienze all'interno del Metaverso saranno più simili a quelle della realtà fisica che non ad Internet come lo conosciamo oggi. Inoltre, le regole dovranno essere flessibili e in grado di potersi adattare a una tecnologia che è ancora in evoluzione.

Pensiamo alla tutela della privacy. Come possiamo ridurre al minimo la quantità di dati utilizzati, costruire tecnologie per consentire un loro utilizzo responsabile che garantisca la tutela della privacy e possa offrire alle persone più trasparenza e controllo sui propri dati?

Oppure, possiamo riflettere sui dati relativi alle caratteristiche umane. L'elaborazione dei dati generati dal corpo umano è fondamentale per la natura del metaverso. Una delle questioni principali è riuscire a stabilire una definizione chiara di questi dati, che potremmo chiamare Human Characteristic Data. Sebbene non sia una questione nuova di per sé, è un lavoro cruciale per il futuro del metaverso.

I dati relativi alle caratteristiche umane comprendono "dati fisici, fisiologici e comportamentali relativi ai dati sul tracking di mani, corpo, viso, testa o occhi, tipicamente posizioni, gesti/movimenti, sguardo".

L'elaborazione di questi dati sulle caratteristiche umane rappresenta la premessa indispensabile per l'esperienza funzionale delle connessioni sociali del metaverso, che non ha lo scopo di identificare univocamente un individuo ma piuttosto di consentire la comunicazione umana e le interazioni sociali attraverso altri mezzi.

Pensiamo anche al tema dell'identità digitale. Gli utenti avranno l'opportunità di creare diverse identità distinte e separate sulle piattaforme e vivere quindi nuove esperienze identitarie attraverso avatar fisici. Crediamo che questo offra alle persone una grande opportunità per esprimere la propria autenticità attraverso varie iterazioni o rappresentazioni della propria identità digitale nel metaverso. A questo proposito, ci deve essere collaborazione tra aziende, esperti e responsabili politici per definire standard condivisi in merito a temi fondamentali quali l'identità, la privacy e la sicurezza.

Siamo proprio agli inizi del nostro percorso verso il metaverso. Molte delle esperienze saranno accessibili solo tra 5-10 anni, così molti dei casi d'uso che immaginiamo oggi.

Questa finestra temporale ci dà l'opportunità di porci le domande più complesse sul modo in cui dovrebbero essere costruiti questi prodotti, ed offre alla nostra azienda, e a tutte le aziende che si occupano di innovazione, il tempo per investire nella ricerca, lavorare a stretto contatto con le autorità di controllo e i responsabili politici e per comprendere al meglio sfide ed opportunità di queste tecnologie già nelle fasi preliminari del suo sviluppo.

COME REGOLAMENTARE I METAVERSI

Prof. Francesco Pizzetti

Professore ordinario di Diritto costituzionale presso l'Università degli studi di Torino, già Presidente del Garante per la protezione dei dati personali

Innanzitutto un grazie sentito per l'invito a questo incontro su un tema così interessante. Non vi è dubbio, infatti, che la prospettiva del Metaverso è destinata ad aprire una nuova fase della digitalizzazione e dunque del modo di vivere degli esseri umani. Peraltro, come sempre accade rispetto a cambiamenti di queste dimensioni è difficilissimo comprendere quali potranno essere tali effetti fino a che le nuove tecnologie non saranno pienamente funzionanti e diffuse.

Del resto proprio durante la pandemia abbiamo avuto una dimostrazione concreta di come i mutamenti tecnologici possano assumere, a seconda del contesto in cui operano, effetti persino impensati. Basta ricordare l'effetto enorme che la didattica a distanza, resa possibile dalle tecnologie digitali, ha avuto sulla vita dei giovani durante la pandemia per comprendere che gli effetti delle innovazioni possono essere di dimensioni tali da comportare mutamenti permanenti nelle abitudini e nella vita dei gruppi umani e nei rapporti tra chi ne fa parte.

Certo è che oggi, a distanza ormai di qualche mese dalla punta massima della pandemia e mentre i rischi medici mutano e diminuiscono, resta estremamente difficile organizzare convegni in presenza, essendosi ormai diffusa in modo che pare irreversibile, l'uso della tecnologia per organizzare incontri a distanza che però, grazie appunto al web, sono anche sostanzialmente in presenza consentendo ai partecipanti non solo di vedersi gli uni con gli altri ma anche di interloquire tra loro e discutere con effetti e modalità molto vicine a quelle tradizionali dei convegni in presenza.

Ancora più forti sono stati gli effetti sull'organizzazione dell'attività didattica, fino a coniare la non bellissima sigla di DAD per intendere sistemi didattici che si sviluppano interamente sul web, esami compresi. Il che, fra l'altro, ha determinato una sfida che anche attualmente è in corso tra le Università tradizionali e le Università telematiche, conseguente appunto al fatto che ormai anche le Università tradizionali organizzano sempre di più attività

didattiche che ricorrono a tecnologie telematiche. È ben difficile, dunque, dire ora quali potranno essere gli effetti del Metaverso non tanto rispetto all'uso della rete quanto rispetto ai tipi di relazioni umane che usando questa nuova tecnologia, e grazie ad essa, potranno svilupparsi.

Si comprende benissimo, dunque, che in un contesto di questo tipo e in presenza di un cambiamento così importante, annunciato ormai da tempo e al quale si stanno dedicando risorse impressionanti nel mondo, sia forte la tentazione di cominciare ad esplorare il futuro anche per cercare di contenerne fin da ora gli effetti più rischiosi per le nostre società e il loro modo di vivere.

È stato questo, del resto, il significato di maggior respiro del già citato intervento del rappresentante di Facebook. Si tratta di un intervento a mio giudizio molto importante e che, per questo, merita sia esaminato con la dovuta attenzione.

Il centro di quanto ci è stato detto è, a me pare, l'affermazione che noi stiamo sicuramente vivendo un'epoca di grandi cambiamenti, rispetto alla quale il senso di realismo e di correttezza deve indurci a dire che non sappiamo dove andremo e non sappiamo che evoluzione avrà la società.

E' un processo in atto che ricorda il viaggio di Cristoforo Colombo che credeva di trovare la via delle Indie e trovò le Americhe.

Anche noi non sappiamo cosa troveremo e dove approderemo nell'ambito di questa evoluzione digitale della società, che è certamente cominciata ormai parecchi anni fa. Del resto sarà bene tenere presente che Internet è stata inizialmente pensata per scopi militari e per essere allo stesso tempo facile strumento di comunicazione planetario, dotato di caratteristiche specifiche come quelle di essere facilmente espandibile nello spazio, facilmente modificabile nel tempo, facilmente riparabile e rispondente alla necessità di assicurare comunicazioni militari semplici e sicure in ambito Nato.

Non dimentichiamo inoltre mai che Internet è il fondamento stesso della società digitale; essa non è stata un prodotto dell'economia anche se certamente la sua evoluzione ha favorito lo sviluppo della tecnologia e delle relazioni economiche globali basato su quello che è stato a suo tempo definito come il *Washington consensus*: una dottrina che si è sviluppata grazie al pensiero di J.Williamson alla fine degli anni ottanta e che ruota intorno a 10 direttive

formulate da Williamson ma soprattutto è fondata sulla convinzione che la tecnologia e l'economia, lasciate libere di operare senza un eccesso di vincoli e condizionamenti giuridici, sono più capaci di produrre innovazione.

Si tratta di una visione molto importante che ha dominato anche il pensiero e l'attività della BEI, del Fondo Monetario Internazionale e delle grandi istituzioni finanziarie globali. Di essa noi parliamo molto, forse troppo, poco dimenticando che essa ha accentuato moltissimo la differenza fra Europa e Stati Uniti, andando ben oltre quella diversità che noi usualmente vediamo soprattutto legata alla protezione dei dati personali. La realtà, invece, è che nella società digitale la differenza tra USA e UE è ben più ampia.

Soprattutto dalla fase successiva all' entrata in vigore del GDPR, l'Europa (UE) concepisce la regolazione delle tecnologie anche come uno strumento di recupero dei ritardi accumulati dall'Unione Europea nella competizione tecnologica globale.

Nasce anche di qui la visione di una maggiore regolazione come capacità di dettare regole che consentano la costruzione di una società digitale più garantista, più ordinata, più tutelata, nella quale i cittadini possano operare e sentirsi più protetti anche ben oltre la privacy come la intendiamo tradizionalmente in UE. La visione europea è proprio l'opposto di quella americana e lo scontro è molto più profondo di quello che viene raccontato o percepito.

Purtroppo, anche nella comunicazione scientifica e tecnica, viviamo tutti in un'epoca che non è eccessivo definire della “comunicazione spettacolo”.

Si comunica sempre meno per informare e per mettere a confronto i risultati delle ricerche e delle analisi scientifiche. Sempre più invece le trasmissioni di informazione sono dominate dal desiderio di acquisire visibilità, notorietà e soprattutto, almeno per le emittenti, *audience*.

Questa evoluzione è ancora più forte nella comunicazione ordinaria: sempre di più viene meno la informazione come strumento di intermediazione fra opinione pubblica e i fenomeni che accadono.

Al contrario, si afferma sempre di più, anche per ovvi motivi di carattere economico, la comunicazione spettacolo. Infatti costa molto meno un'ora di trasmissione televisiva fatta da un giornalista diventato *ancorman* che

invita 3,4,5 esperti che poi ne ricavano notorietà con tutto quello che ne consegue, di quanto può costare un'ora di spettacolo basata anche solo con un corpo di ballerine e un'orchestra.

In questa epoca sta diventando sempre più difficile spiegare cosa succede all'opinione pubblica e sta diventando sempre più difficile per il pubblico comprendere e capire quello che sente o legge sui mezzi di informazione.

Tuttavia è certo, e facilmente constatabile, che l'Unione Europea si è messa dal 2020 in poi su una strada che la vede come una netta antagonista non solo del modello cinese, basato essenzialmente sulla tecnologia del controllo, ma anche del modello americano, basato sulla competizione tra fornitori di servizi e controlli antitrust. La UE, infatti, preferisce regolare la tecnologia della rete e dare garanzie ai cittadini attraverso la disciplina normativa della società digitale che non limitarsi ai controlli antitrust per regolare un mercato digitale visto come una sfida più che come un eldorado sociale.

Questo aspetto della strategia UE è alla base di tutto il pacchetto di proposte regolatorie note come il *Digital services Act package* proposto dalla Commissione fin dal 2020 (DSA) e il 2022 (DMA) e sul quale, tra il 22 marzo e il 23 aprile del 2022, è stato trovato un *agreement* col Consiglio tanto da far prevedere che le misure proposte possano entrare in vigore entro il 2024.

Si tratta di due regolazioni molto impegnative che confermano la continua produzione da parte della UE di proposte regolatorie, compresa quella sull'intelligenza artificiale presentata il 21 aprile 2021. Proposte che hanno tutte l'obiettivo di rafforzare innanzitutto il mercato unico, assicurando una regolazione uniforme in tutto il territorio UE e quindi, attraverso il c.d. “*Effetto Bruxelles*”, anche di condizionare il mercato digitale globale o almeno larga parte di esso.

Diversa l'evoluzione digitale negli Stati Uniti. In USA la digitalizzazione dell'economia e della società si è continuamente accentuata fin dalla direttiva Clinton che, anche per influenza di Al Gore, aprì all'uso commerciale della rete in un'epoca nella quale anche il nuovo protocollo web mutava profondamente le potenzialità del digitale.

Tutto questo collocò gli USA in una prospettiva orientata a lasciare il

mercato più libero possibile, nella convinzione che esso fosse in grado di assicurare, grazie al suo stesso funzionamento, la massima innovazione possibile. Alla base della impostazione di Clinton, diventata poi stabile nella visione USA, sono gli utenti consumatori a guidare il mercato e a spingerlo a sviluppare sempre nuove tecnologie in grado di soddisfare le loro esigenze.

È innegabile che la visione americana dell'epoca Clinton applicata alla rete ne ha segnato profondamente le caratteristiche e ha accentuato il suo continuo, costante e accelerato sviluppo come dimostra la rapida evoluzione che ha avuto la società digitale degli Stati Uniti a partire da quell'epoca.

È proprio quella, del resto, l'epoca dello sviluppo della Silicon Valley e dei "social" che, anche grazie allo sviluppo del web.2, hanno da allora iniziato a colonizzare, con i servizi offerti e l'uso commerciale dei dati raccolti, la rete e quindi il mondo. In sostanza, da quando a cavallo tra la fine degli anni novanta e l'inizio degli anni 2000 dall'uso prevalentemente militare della rete si è passati all'uso commerciale e allo sviluppo del web.2, negli USA ha prevalso un orientamento basato sulla convinzione che bastasse aver fiducia nel mercato vigilato dal controllo antitrust per garantire la competizione nelle tecnologie digitali e quindi anche il loro rapido sviluppo nella tutela degli interessi dei consumatori.

Questo ha, ovviamente, accentuato ulteriormente il divario tra USA e UE ed è stato - e tuttora è - una delle ragioni per le quali la UE ha visto sempre con diffidenza il trasferimento di dati in USA.

Peraltro vi sono segnali recenti che anche negli Stati Uniti la visione della rete e della regolazione digitale stia in parte cambiando. Negli USA infatti la regolazione delle relazioni commerciali lasciata prevalentemente agli Stati rischia, in assenza di una regolazione federale unica, di frammentare il mercato interno non meno di quanto accadeva (e ancora in parte può accadere) in UE. Di qui la ragione per la quale ora anche gli Stati Uniti stanno riflettendo sul rischio di vedere il loro mercato interno digitale frammentato dalle diverse regolazioni degli Stati che questi hanno adottato anche a protezione dei dati personali o dalle diverse esigenze dell'uso delle tecnologie digitali nelle diverse aree economiche. Non a caso in questi ultimi tempi ha avuto inizio la discussione di un progetto di legge di protezione dati federale (si tratta dello

American Data Privacy and Protection ACT, già usualmente indicato come ADPPA).

Un progetto presentato sulla base di una giustificazione che riguarda anche la società digitale nel suo complesso in una visione assai vicina a quella dell'Unione Europea. Anche negli USA si segnala infatti la necessità di evitare una eccessiva frammentazione del mercato federale interno: rischio che, come il caso UE dimostra, aumenta con l'aumentare dell'uso delle tecnologie digitali.

In sostanza sembra che negli USA l'idea che il mercato è per la sua stessa natura produttore di una innovazione rispettosa dei diritti e degli interessi dei consumatori sia destinata ad andare sempre di più mano nella mano con la diversa e opposta idea che un'innovazione non regolata adeguatamente può frantumare il mercato interno. Tutto questo consente di pensare che nei prossimi anni la differenza di impostazione tra UE e USA possa attenuarsi, accentuando, grazie a un avvicinamento tra le due impostazioni, i futuri mutamenti del quadro complessivo. Cosa questa che ovviamente inciderebbe anche sulla regolazione dei trasferimenti di dati tra USA e UE.

Dentro questo quadro, già di per sé assai complesso e in costante mutamento, dobbiamo anche tenere presente che ormai la società digitale ha cominciato a galoppare e la tecnologia è in continuo sviluppo.

Non possiamo prevedere oggi quali evoluzioni avrà questa società: un po' perché, come ho detto, il quadro culturale sul digitale che domina nella società occidentale è guidato dalla visione americana e non ancora da quella europea; un po' per il fatto che nessuno sa né quali domande verranno fatte alla tecnologia né quali suggestioni la tecnologia metterà a nostra disposizione.

Possiamo solo essere sicuri e consapevoli che il futuro sarà molto diverso dalla situazione attuale, tanto che, come dice Floridi, i ragazzi che nasceranno nei prossimi anni chiederanno stupiti a noi di sapere come si viveva (e come si poteva vivere) in una società tutta *of line*.

Tuttavia, proprio per la nostra cultura di fondo che, soprattutto negli ultimi tre secoli, ha scommesso moltissimo, anche con ottimi risultati, sulla scienza e sulla tecnica noi siamo tendenzialmente aperti a pensare che ciò che le innovazioni che la scienza sta ricercando e proponendo saranno certamente cose utili per noi. Solo da qualche tempo, soprattutto in connessione con la

Intelligenza Artificiale, abbiamo cominciato a preoccuparci seriamente della evoluzione digitale, ma da almeno 2 o 3 secoli il mondo laico ha scommesso sulla scienza, anche a costo di scontri duri col pensiero religioso e per noi con quello cattolico. L'illuminismo è stato questo ed è per questo che spesso la cultura occidentale si è scontrata con chi voleva frenare l'evoluzione scientifica in nome della centralità dell'uomo.

Non a caso noi oggi, per mitigare la nostra preoccupazione verso una evoluzione troppo rapida della tecnologia, abbiamo rimesso al centro la preoccupazione, più che rispettabile, per la dignità dell'uomo e quindi abbiamo cominciato a valorizzare sempre di più un approccio etico anche rispetto alla tecnologia digitale. Speriamo che questa riscoperta dell'etica sia soprattutto una riscoperta della necessità degli esseri umani di riflettere sullo sviluppo della tecnologia e non solo di prendere a scatola chiusa come buona e positiva qualunque innovazione tecnologica la scienza ci proponga.

Detto questo, però, dobbiamo riconoscere che attualmente non sappiamo neanche che punti di orientamento utilizzare proprio perché da tre secoli non poniamo a noi stessi questo interrogativo. La nostra attenzione è stata posta solo nel bisogno di sicurezza dei mezzi tecnici utilizzati. Si pensi, ad esempio a come si è declinata la attenzione sulle cinture di sicurezza o sugli air bag o sui guardrail. Ogni innovazione è stata esaminata essenzialmente non per evitare ma per proteggere dalle conseguenze negative che un cattivo uso di essa poteva avere in un quadro visto comunque come positivo. Se invece il richiamo all'etica è oggi, in questa fase della nostra società, una spinta a ritornare a riflettere sui rischi, oltre che sui vantaggi, delle scoperte scientifiche allora è certamente una cosa buona e positiva ma che richiede uno sforzo, anche culturale, molto rilevante.

Detto questo non vorrei tuttavia diminuire l'importanza dell'intervento del rappresentante di Face book- Meta che ci dice: ma perché non facciamo il contrario di quello che è avvenuto finora? Negli anni che ci stanno alle spalle la tecnologia è andata avanti per conto suo e dopo sono intervenute le Autorità garanti a dirci che cosa era sbagliato, che cosa andava a corretto, che cosa non si poteva fare. Se ho capito bene, l'intervento di oggi ci propone di dar vita al Metaverso “insieme” .

Facebook e Meta ci metterebbero le competenze tecnologiche, indicando lealmente gli obiettivi che le imprese vogliono raggiungere: obiettivi che allo stato attuale non sono chiarissimi anche perché non sono chiarissimi gli strumenti che dovrebbero consentire di vivere nel mondo digitale con modalità molto vicine a quelle del mondo *of line*. Tuttavia, proprio per questo la offerta è ancora più attraente. Ci si dice in sostanza: considerata la complessità della tecnologia da usare costruiamola insieme noi tecnologi, voi “eticisti” e voi Autorità e regolatori custodi delle regole relative alla salvaguardia delle libertà fondamentali degli esseri umani.

Come ho già detto si tratta di una suggestione assai interessante ma, almeno a me pare, non compatibile il GDPR, e credo che questo Meta lo sappia benissimo. Il GDPR si fonda su una altra scommessa e su un altro pilastro: quella che noi chiamiamo, forse non sempre in modo abbastanza consapevole, “*accountability*”. Il GDPR in sostanza afferma che, tanto più nel quadro della *privacy by design* e della *privacy by default*, il problema di tutelare i diritti fondamentali ricade integralmente su chi progetta, chi costruisce, chi verifica e chi usa una nuova tecnologia. A questo però si aggiunge il tema della valutazione del rischio che ricade integralmente sul titolare del trattamento.

In sostanza spetta a chi sta progettando l’innovazione tecnologica valutare tutto questo e in questo quadro la tecnologia stessa e i rischi che essa può comportare, comprese le responsabilità dei costruttori di devices e di chi li mette a disposizione dei titolari dei trattamenti.

Spetta però a chi usa queste tecnologie valutare il rischio che il loro uso può comportare per gli interessati e i loro dati e adottare le misure necessarie per ridurre o eliminare tali rischi oltre che assicurare agli interessati una informazione adeguata anche rispetto a tali rischi.

Sulla base di questa riflessione è importante invitare quanti si misurano con il mondo di Meta a ricordare sempre l’art. 5 del GDPR e quanto esso dice circa il concetto di dato e sulla responsabilità di chi, trattando i dati, è tenuto a rispettare questa norma.

Dunque, certamente se in un domani le Autorità dei singoli Stati o lo EDPB volessero accettare l’offerta di studiare insieme i problemi che Meta pone è dall’articolo 5 che si dovrebbe partire.

Chiunque volesse avventurarsi su questa strada deve sapere però fin dall'inizio che è necessario studiare e porre in essere tecnologie rispettose dei vincoli, delle condizioni, delle caratteristiche che devono caratterizzare questi trattamenti in base al GDPR. Vincoli che non a caso sono stati riassunti in questo articolo 5 del GDPR che è lungo ma non lunghissimo e quindi sostanzialmente anche molto padroneggiabile.

Non dipende da me ma dal Presidente Stanzione e da tutti i suoi colleghi sia nel Collegio italiano sia nello EDPB, costituito da rappresentanti di tutte le autorità europee, valutare e decidere se approfondire e accettare di dialogare con Meta sulla base di questa suggestione e di questa normativa.

Io faccio solo due osservazioni e poi chiudo: attenzione che la strada proposta è veramente suggestiva ma presenta aspetti e rischi che devono far riflettere tutti.

Dobbiamo assolutamente evitare di far uscire dall'ambito democratico la regolazione della tecnologia, soprattutto quando questo riguarda la tutela della persona. A questo punto infatti si potrebbe dire che se si accetta questa proposta si crea una situazione nella quale gli studiosi di innovazione tecnologica, le imprese e le Autorità garanti diventano in qualche modo codecisorì che però, proprio per questo, tendono a sostituire il decisore politico e a diventare molto autoreferenziali. Si tratta dunque di una decisione e di una scelta che non può essere fatta alla leggera. A mio giudizio accoglierla, per quanto suggestivo possa apparire, rischia di far venire meno gran parte delle garanzie offerte dal GDPR agli interessati.

Qualora, infatti, alla prova del funzionamento di Meta, le decisioni adottate di intesa tra Garante e Meta fossero ritenute da uno o più degli interessati contrastare col GDPR a chi costui o costoro potrebbero rivolgersi per tutelare il loro diritto? E, in ogni caso, quale grado di libertà di fatto e giuridica il Garante potrebbe rivendicare per deliberare eventualmente anche in contrasto con le scelte compiute dalla maggioranza delle Autorità nello EDPB?

E ancora: come potrebbe poi il Garante partecipare ai lavori dello EDPB sul tema trovandosi oggettivamente in una posizione molto diversa da quella delle Autorità garanti di altri Stati che non avessero accettato la offerta di Meta?

Infine: proprio per le caratteristiche di Meta, una tecnologia del tutto nuova della quale possiamo solo intuire benefici e rischi, come è possibile che le Autorità, partecipando alla fase della elaborazione e attuazione del progetto, rischino di compromettere il loro essenziale ruolo di controllori e verificatori sul funzionamento in concreto della innovazione di cui stiamo parlando?

Il tema posto dalla offerta di Meta, che anche oggi ci è stata ripetuta dal suo rappresentante, ci impone di ricordare sempre che siamo una generazione (e molto di più lo sarà quella che verrà dopo di noi) chiamata una grande sfida.

Per questo di fronte ai problemi che certamente Meta porrà ai Garanti è doveroso rinnovare piuttosto il sostegno, l'affetto, l'amicizia alla Autorità Garante e a chi ne ha oggi la responsabilità.

Il Garante è, e deve rimanere, l'unica vera ed effettiva tutela dei nostri diritti fondamentali di fronte all'esplosione delle nuove tecnologie.

Questa, infatti, tanto sul piano nazionale quanto su quello europeo è l'unica Autorità che ormai da 25 anni ha accumulato davvero una ampia esperienza relativa all'evoluzione digitale della società sia sul piano etico sia sul piano tecnologico sia sul piano giuridico.

Accanto all'Autorità però ci sono i decisori nazionali ed unionali che rappresentano i popoli europei. Essi non possono e non devono rinunciare a svolgere i loro compiti ed esercitare i loro poteri. I temi che si profilano col passaggio al Metaverso sono enormi e ancora solo appena intravedibili ma mi pare chiaro che spetta ai decisori europei e alle Autorità europee dire se è lecito che una persona su Metaverso possa presentarsi come donna essendo uomo o viceversa; come adulto essendo minore o viceversa; o se, partecipando a una riunione di bambini, possa adottare un avatar con sembianze da bambino che può diventare, ovviamente, anche uno strumento per indurre in errore gli interlocutori.

Sono solo pochi cenni problematici, utili tuttavia a metterci in grado di comprendere quanto forte potrà essere l'evoluzione della società digitale e, più in generale, della nostra realtà di vita nel mondo Meta. Ci troveremo di fronte a nuovi enormi problemi che non è giusto pensare di risolvere favorendo o sollecitando un previo accordo tra Autorità e imprese.

Al contrario: è proprio di fronte a queste evoluzioni e ai problemi che esse comportano e comporteranno che dobbiamo sempre più rafforzare le Autorità, tutelando ed esaltando anche il ruolo culturale ed etico che esse svolgono. Un ruolo che, certamente, ha una valenza politica di primissima grandezza come dimostra il fatto che tanto il DSA che il DMA implichino un forte rafforzamento del ruolo della Commissione sia nell'ambito dell'evoluzione della normativa che del controllo del suo rispetto.

Insomma siamo davvero entrati in un “nuovo mondo” e Meta sarà probabilmente destinata ad esserne il segnale più evidente.

Una cosa tuttavia merita di essere sottolineata con forza: proprio i cambiamenti in atto e quelli che sono all’orizzonte dimostrano sempre di più la necessità di nuove forme di garanzia delle libertà e dei diritti fondamentali dei cittadini europei e di ogni parte del mondo.

In questo senso possiamo esser orgogliosi che la UE abbia anticipato col GDPR una normativa che ogni giorno si mostra più adatta e adeguata alla società digitale e, soprattutto, che la UE, anche contando sull’effetto Bruxelles, stia cercando di dare un contributo fondamentale alla costruzione di un pianeta sempre più digitale ma anche sempre più rispettoso dell’essenza umana e dei diritti dell’uomo.

Doveroso dunque concludere questo intervento non solo con un ringraziamento ma anche con un forte augurio alla Autorità Garante e a chi la guida, dicendo tutta la nostra fiducia nella loro capacità di collaborare ad accompagnare con mano ferma il popolo italiano e quello europeo nella nuova era che si sta aprendo davanti a noi.

**DAL METAVERSO ALLA METACITY:
IL FUTURO DELLE PROSSIME GENERAZIONI**
Prof. Derrick de Kerckhove

*Direttore scientifico osservatorio TuttiMedia e MediaDuemila,
docente POLIMI, già Direttore del MacLuhan Program di Toronto*

I 25 anni di privacy che hanno accompagnato la veloce evoluzione del nostro essere uomini, ci hanno condotto fino qui oggi a parlare della nuova tappa della trasformazione digitale che è molto più profonda di quanto la più parte della gente sembra essere consapevole.

Voglio ricordare che tutto il cambiamento parte dal concetto legato alla duplicazione. Prima dell'era digitale doppiare qualcosa era complicato e costoso.

Duplicazione, dopo duplicazione siamo arrivati alla creazione del metaverso che praticamente sancisce il nostro vivere in tre spazi. Conosciamo bene lo spazio fisico e quello mentale, poi ecco lo spazio virtuale.

Il punto è che questi tre spazi cominciano ad essere sempre meno distinti l'uno dall'altro. Indossare un visore ed entrare nel metaverso è semplice, un gioco che ci porta in una realtà parallela dove l'essere e il non essere si confondono ed inizia la meraviglia del mondo digitale, con tutti i suoi lati positivi e negativi che i relatori prima di me hanno ben illustrato.

Ma il metaverso è, senza dubbio, la nuova tappa della trasformazione digitale nella sua complessa ridefinizione dello spazio, perché ci sta conducendo verso l'esternalizzazione della nostra immaginazione.

Ecco che diventa chiaro che i punti saldi dell'essere umano, e cioè spazio, tempo e sé si stanno inesorabilmente e profondamente modificando.

Negli anni'90 ho anticipato l'esternalizzazione della nostra memoria, ho parlato e riparlato delle nostre protesi tecnologiche: computer e poi telefono. Oggi la mia visione del cambiamento si completa con l'immaginario che diventa reale: non c'è più lo schermo che divide.

La trasformazione ci porta dentro. La realtà virtuale è l'opposto di un libro, poiché non nutre l'immaginazione interna, ma propone il nostro pensiero interno al mondo esterno. Nella mia visione la realtà aumentata del metaverso ridotta a simulazione, mette in pericolo la nostra stessa cultura

umana e ci mette di fronte anche un dilemma politico perché un bene pubblico, in virtù della realtà aumentata, finisce per diventare privato.

Mi chiedo cosa succederà quando come dice Matthew Ball (amministratore delegato di Epyllion, Venture Partner di Makers Fund, Senior Advisor di KKR, Senior Advisor di McKinsey & Company, il suo primo libro *The Metaverse and How it Will Revolutionize Everything*, pubblicato nel luglio 2022 subito bestseller nazionale e internazionale): "La generazione di bambini di oggi si esprime, spesso impara e socializza costantemente attraverso mondi virtuali che può toccare, modificare e collaborare. Questo non si fermerà. Anzi, le capacità di questi mondi virtuali si amplieranno, la loro facilità d'uso migliorerà e la loro importanza crescerà. Inoltre, la generazione "nativa iPad" (o forse "nativa mondo virtuale") continuerà a maturare. La maggior parte di loro è ancora un consumatore, pochi sono creatori e quasi nessuno è un leader aziendale. Lo saranno. E i loro quadri di riferimento porteranno a un cambiamento trasformativo."

Ebbene in questo cambiamento trasformativo come riporteremo le regole sociali, legali e soprattutto i concetti legati ai nostri modi di vivere e operare come quello della privacy, appunto.

Le regole del vivere sono legate alla condivisione del linguaggio, oggi sotto attacco, perché la crisi epistemologica che viviamo ne ha rimesso in discussione le basi. Infatti, la nostra cultura alfabetica dava all'uomo la sicurezza del rapporto tra linguaggio e realtà. La realtà cambia si trasforma e si riforma nel metaverso.

L'uomo occidentale fa parte del gruppo antropologico definito naturalismo che è fondato sulla partecipazione e la condivisione di uno spazio comune (la natura appunto), e sulla privatizzazione interiore del pensiero. Come gestire la privacy in questo nuovo contesto, il metaverso, è la sfida che vedo davanti soprattutto per l'Authority istituita 25 anni fa a garanzia del nostro essere privato.

Non voglio demonizzare assolutamente, non possiamo tornare indietro ma dobbiamo impegnarci per capire come funziona in modo da essere in grado di rispondere alla sfida che questo nuovo spazio presenta. Il professor Pizzetti ha già fatto emergere alcune questioni, fra queste la commercializzazione di questo nuovo spazio che è privato, ma in un certo

senso pubblico perché a disposizione di tutti. E qui sottolineo che non esiste solo il metaverso di Meta.

Dopo aver analizzato il punto in cui ci ha portato la trasformazione digitale, la mia soluzione è sostenere le meta-città dove poter importare alcune regole di privacy, ad esempio.

In questo cambio si gioca il nostro futuro perché la smart city nella sua metaversione si fonda sulla raccolta di dati relativa ad ogni aspetto, dal traffico ai pedoni, dalla criminalità all'istruzione, e l'elenco continua. Da questa pratica dipende il timore della perdita della privacy che è una questione culturale. Gli Stati Uniti tollerano la flessibilità a vantaggio del "capitalismo della sorveglianza", mentre l'Unione Europea si difende con il GDPR e la Cina sceglie in modo rapido e drastico: niente privacy, punto.

Cosa facciamo? La risposta all'Authority che per un quarto di secolo ha governato questo aspetto e che è stata rappresentata da un mio grande amico, Stefano Rodotà, con il quale ho discusso più volte dibattuto su "*privacy is over?*"

RELIGIOSITÀ E SPIRITALITÀ NEL METAVERSO
UN CONTRIBUTO PER CUSTODIRE L'UMANO AL CENTRO
Don Luca Peyron
Apostolato digitale Arcidiocesi di Torino, Università Cattolica

L'espressione 'umano al centro' è da sempre piuttosto ambigua e rischia di essere velleitaria nella misura in cui essa non diventi più specifica o non offra maggiori criteri per poter essere specificata.

La teologia e l'esperienza vitale delle religioni possono offrire uno sguardo ulteriore, non necessariamente alternativo, anzi piuttosto complementare che, nel dialogo con i saperi, offre un contributo sostanziale all'impresa. L'impresa di custodire l'umano nella metamorfosi digitale e segnatamente nella presumibile ulteriore metamorfosi che il metaverso o i metaversi offriranno o determineranno⁽¹⁾.

La Chiesa Cattolica, pur con i suoi diversi e fin troppo noti difetti, certamente può a buon diritto fregiarsi di quell'espressione con cui iconicamente la definì papa Giovanni XXIII: "Esperta di umanità". E la Bibbia, principio e fondamento dell'esperienza religiosa e della teologia, in effetti è un grandioso racconto dell'umano, in dialogo con se stesso ed il mondo, in dialogo con Dio ed il mondo interiore.

Di qui nasce l'interesse, o per meglio dire il servizio, che la teologia e la fede possono rendere all'umanità, ai credenti, ai credenti in un diverso sistema religioso ed ai non credenti. L'umano che ci accomuna, anche se non sempre ci unisce.

A ben guardare infatti, le questioni che nascono dalla trasformazione digitale e quelle connesse al metaverso sono sostanzialmente questioni di

1) Sulla definizione di metaverso o di metaversi non mi soffermo essendo il tema di altri interventi contenuti in questa raccolta di atti. Vale la pena ricordare che il termine "Metaverse" è stato coniato da Neal Stephenson nel libro appartenente alla cultura cyberpunk "Snow Crash" nel 1992. Esso è descritto dall'autore come una sorta di realtà virtuale condivisa tramite internet, dove si è rappresentati in tre dimensioni attraverso il proprio avatar.

carattere antropologico. Da esse derivano questioni eminentemente tecnoscientifiche ma anche fisiologiche, psicologiche, economiche, giuridiche e sociali. Ma l'essere umano, l'idea che ne abbiamo, il senso che determina l'esserlo, sono la grande chiave, il metro di lettura e giudizio e, nella nostra prospettiva, il fine ultimo di ogni azione umana, compresa quella tecnica, oserei dire in questo tempo soprattutto quella tecnica.

Soffermiamoci un momento su di uno sguardo di insieme da cui poi generare il ragionamento che vorrei proporre analizzando due limiti strutturali dell'essere umano, di ciascuno di noi.

A ben guardare l'artefatto tecnologico nasce, da sempre, per rispondere ad un primo limite che è insistito nella stessa natura umana. A differenza degli altri esseri viventi su questo pianeta, l'essere umano non è in grado di sopravvivere nella natura in cui nasce così come è, *sic et simpliciter*. Un bambino appena nato non ha bisogno, come altri cuccioli, solamente delle cure dei genitori, ha bisogno che lo si copra con delle pelli di altri animali, che lo si difenda dai predatori con bastoni e lance, che lo si nutra per diversi anni prima che sia in grado, autonomamente, di difendersi e procurarsi cibo.

L'essere umano, in natura, soccombe con le sue sole dotazioni naturali. Non ha un particolare udito, né olfatto. Non è veloce, non vola, con si arrampica con particolari abilità. Ma è intelligente, dotato di una capacità intellettuale combinatoria e creativa, che lo mette lo in grado di risolvere problemi, creare oggetti, imparare abilità, adottare comportamenti totalmente inediti e non ereditati dai genitori ecc. Con tale intelligenza sopperisce all'apparente divario che lo separa dalle altre creature che vivono in natura. E le sopravanza. Lo fa, per tornare al punto di partenza, con la tecnica. Costruisce la palafitta, tiene da parte strumenti efficaci, ne forgia di altri, via via sino a sbarcare un giorno sulla luna o a mettere in orbita sistemi di rilevamento satellitare in grado di mappare il suo mondo. Non prevede ancora i terremoti e fa fronte ad una pandemia in tempi che si allungano. Ma la tecnica fa la differenza, inganna la natura molto bene.

Non è un caso se la parola macchina deriva dal greco antico mecanomai che, significa letteralmente, proprio ingannare. Ed ingannare con parvenze quasi divine. Vale la pena qui ricordare il Deus ex-machina del teatro

greco, poi divenuta locuzione del senso comune. Una mechanè (mēkhanē) era una sorta di gru usata nel teatro greco, in particolare nel V e IV secolo a.C. Composto da bracci di legno e da un sistema di pulegge, questo marchingegno teatrale era usato per sollevare in aria gli attori, simulandone il volo.

Era sicuramente in grado di sollevare almeno due persone e trasportarle nel mezzo dell'orchestra, oppure sopra la *skené*. Proprio per questo motivo, la mechanè era spesso usata per simulare l'intervento di un dio sulla scena, a risolvere questioni così intricate da non essere altrimenti risolvibili. Da questa tradizione nasce l'espressione latina *Deus ex machina*.

La tecnica dunque è espressione tipica dell'umano, è parte integrante della sua natura. Noi siamo, per dirla in altri termini, naturalmente tecnologici. Questo, dal punto di vista teologico, è un bene, può essere considerato un bene accessorio e parecchio indispensabile, donato dal Creatore alla creatura ed espressione piena del suo essere immagine e somiglianza di Dio. Due esempi possono sostenere queste affermazioni. La prima è l'uso della tecnica da parte di Dio per salvare i giusti dal diluvio: l'arpa dell'Alleanza è un costrutto tecnologico i cui piani sono dati da Dio stesso a Noè affinché costruisse quel manufatto (Genesi 6, 13-16). La tecnica è dunque parte della salvezza e della cura che Dio ha della sua creatura prediletta. Tale orizzonte è ribadito nella vicenda terrena di Cristo, archetipo del compimento che Dio ha in serbo per l'essere umano. Cristo fu facitore di tecnica, non solo un semplice falegname, ma qualcosa di più. Il termine greco che leggiamo nei Vangeli di Marco e Matteo può essere infatti interpretato in vari modi. La parola usata nei testi evangelici è téktōn, usata per artigiani e lavoratori del legno (e quindi si può tradurre come "falegname"), ma è interessante che si possa riferire anche a scalpellini, costruttori e perfino coloro che eccellevano nel loro mestiere ed erano in grado di insegnarlo agli altri. La traduzione latina che troviamo nella Vulgata, faber, mantiene i vari significati del greco téktōn. Il falegname non solo falegname di Nazareth è un uomo, vero Dio, che per buona parte della sua esistenza si prende cura dei suoi simili costruendo artefatti che permettano loro di vivere meglio. Il tavolo, la sedia, la scala che Gesù costruisce non sono semplicemente finalizzati a vivere, ad avere un reddito con cui vivere.

Ogni gesto compiuto da Cristo ha un significato teologico più ampio

del semplice gesto in sé. Dunque il gesto ripetuto di creare tecnica per l'essere umano ha una portata teologica ben superiore, a dire il vero non ancora del tutto esplorata dagli studi teologici stessi. Possiamo dunque concludere che la tecnica, espressione dell'umano, è a servizio del suo stare nella natura ed in essa vivere nel rispetto di se stesso e della natura stessa in cui vive in equilibrio. L'essere umano ha però un secondo limite che non è semplicemente di ordine naturale biologico, fisico creaturale. Lo potremmo definire interiore, profondo, spirituale e psicologico. Egli aspira ad un compimento, ad un di più rispetto al semplice vivere, sente una insufficienza cronica nel suo essere profondo. Quell'aspirazione così radicale lo porta a creare arte, poesia, musica e filosofia. Quel di più lo porta a guardare il cielo non semplicemente in funzione dei suoi bisogni materiali, ma come ispirazione dei suoi bisogni spirituali, trascendenti. L'essere umano è alla ricerca di qualche cosa di più e di altro rispetto a se stesso.

Una prima risposta a tale desiderio profondo lo trova nell'altro da sé, negli altri esseri umani. La Bibbia racconta questo desiderio con l'incontro tra il maschile e femminile, in quella diversità creata proprio perché il singolo non basta a se stesso e perché da quell'incontro nascesse l'intuizione che il compimento definitivo, totalizzante, fosse in quel totalmente altro che è Dio stesso. Questo ulteriore passaggio, questo salto necessario, è significativamente evocato in un altro brano della Scrittura là dove, nel dare a Mosè le dieci parole, quelle che comunemente noi chiamiamo comandamenti, lega ad uno di questi, ed a questo solo, una promessa. È il quarto comandamento, la quarta parola, che nel libro del Deuteronomio è riferita così: "Onora tuo padre e tua madre, come il Signore Dio tuo ti ha comandato, perché la tua vita sia lunga e tu sia felice nel paese che il Signore tuo Dio ti dà". (Deuteronomio 5,16) Delle dieci parole dunque questa è l'unica a cui è associata una promessa. Tutte le altre parole, gli altri comandamenti, apparentemente anche più importanti o significativi di questi non promettono nulla, qui sì. Per quale ragione?

La portata di questa parola non è quella che ci restituisce una prima lettura o una lettura segnata dall'abitudine o dalla prassi culturale. La questione in gioco non è semplicemente quella di trattare bene i genitori, rispettarli quando siamo giovani ed accudirli quando loro sono vecchi. Vi è qui molto di più. Lo rivela il verbo ebraico sottostante a quanto traduciamo con 'onorare'.

Il termine usato è *kabod*, *kabed* (o *kaved*) che significa dai il giusto posto, il giusto peso, la giusta considerazione. Giusta non in termini morali ma per così dire, fisici, numerici. Dai ai tuoi genitori quanto è corretto, non di meno, ma neppure di più.

Cosa si intende qui?

Il fatto che tutti siamo figli e che essere figli comporta molte questioni, molto spesso non risolte per tutta l'esistenza. L'essere figli comporta il vivere in una tradizione, ma anche in alcune aspettative, vere o presunte. Comporta stare in alcune tensioni e delusioni, essere eredi di tradizioni importanti e significative oppure sconsolanti e distruttive. Ma meno decisive, costringenti, stringenti di come comunemente l'umano le vive. Il passato e le radici sono fonte di profonde lacerazioni e ferite, di un desiderio di compimento, imitazione, affrancatura a seconda dei casi, scenari a cui nessuno sfugge. Quale rimedio suggerisce la Scrittura? Dai il giusto peso. Non di meno, ma neppure di più. Tu sei tu, non sei semplicemente la somma, il risultato, l'esito di chi ti ha preceduto. In positivo ed in negativo. Non sei la somma degli errori dei tuoi genitori e neppure dei loro successi ed onori. Cristo ribadirà questo concetto invitando ad affrancarsi dall'idea che il male giunge come castigo delle colpe dei padri. Dai padri e dalle madri, dal passato, ereditiamo certamente una cornice di senso, culturale, tecnica, di saperi che ciascuno poi, liberamente, deve scegliere come gestire. La tecnica in tutto questo come si inserisce? Qui sta il punto e qui vengo alle conclusioni di questo breve intervento.

La tecnica e la tecnologia sono uno straordinario strumento che ci permette di andare oltre alcuni limiti di natura, di stare nel tempo e nella storia custodendo il creato e noi stessi, possibilmente nella reciprocità ecologica che garantisca il nostro pianeta.

Di qui la necessità che la tecnica venga progettata, distribuita, ed utilizzata con un fine ultimo antropico, per custodire la vita umana nel suo complesso e l'equilibrio che essa deve avere con la vita sul pianeta. Mettere l'umano al centro nella metamorfosi digitale può avere questo significato. Ma tale operazione deve essere temperata prendendo in considerazione la seconda ferita dell'umano, il suo secondo limite. Sarebbe una fatale illusione pensare che il limite dato da chi siamo come persone, come storia personale, come

fardello negativo o eredità positiva possa essere, come per la natura biologica, soccorso e temperato dalla tecnica. Delegare responsabilità abilitanti agli algoritmi, creare mondi paralleli in cui non dover affrontare se stessi e la propria storia, immaginare inserzioni cyborg che permettano al corpo di affrancarsi dal suo essere in tensione tra un incompiuto ed un incompiuto, sarebbero errori fatali. Perché priverebbero l'essere umano di un suo eminente specifico: l'essere in ricerca di se stesso, esercitare la propria libertà nella storia e contemporaneamente nonostante la storia, essere figli e nello stesso tempo poter essere genitori del futuro, biologico e culturale. La ferita del nostro non essere sufficienti a noi stessi, in altri termini, va guarita nella relazione con gli altri e con l'altro, non con la macchina che rinchiude in un solitario virtuale privo di frizioni, ma anche privo di personalità e dunque deprivato del nostro essere sostanziale di persone in cerca di relazioni che compiano la nostra nativa solitudine esistenziale.

La tecnica, in definitiva, deve permetterci di stare nel tempo e nello spazio per concentrare le nostre energie e le nostre capacità nello scoprire noi stessi e l'altro, delegando alla macchina quanto più possibile ciò che ci disumanizza e trattenendo per noi, anzi chiedendo alla macchina, di renderci più capaci ad esercitare responsabilità e libertà, giustizia e ricerca del bello, del vero, del bene. Con chi vive accanto a noi. Coloro che abbiamo scelto, coloro che ci hanno scelto e coloro che, semplicemente, la storia ci pone accanto.

SECONDA SESSIONE



AI, SMART CITY, IoT, AUTO CONNESSE: FUTURO, INNOVAZIONE, LAVORO



- MOBILITÀ E DIGITALIZZAZIONE. SCENARI, TRAFFICO, VEICOLI, PERSONE
Prof. Mauro Velardocchia
- L'INTELLIGENZA ARTIFICIALE IN ITALIA: STRATEGIE PRESENTI E PROSPETTIVE FUTURE
Prof.ssa Barbara Caputo
- NUOVE PROTESI COGNITIVE? I DATI AI TEMPI DELL'INTERNET DELLE COSE
Prof.ssa Anna Maria Mandalari
- INNOVAZIONE, AI E IoT: RIFLESSIONI DEI PROFESSIONISTI
Dottore Commercialista Paola Zambon
- PRIVACY E GESTIONE DEI DATI, VALORE E RISCHI DI UNA SINERGIA
Dott. Marco Gay

SECONDA SESSIONE*

AI, SMART CITY, IOT, AUTO CONNESSE: FUTURO, INNOVAZIONE, LAVORO

MOBILITÀ E DIGITALIZZAZIONE.

SCENARI, TRAFFICO, VEICOLI E PERSONE

Prof. Mauro Velardocchia

*Meccanica del veicolo e sistemi di sicurezza attiva, Dipartimento
di Ingegneria meccanica aerospaziale, Politecnico di Torino*

Sommario

La mobilità è il risultato di una molteplicità di esigenze e contributi di natura tecnologica, giuridica, sociale, che da tempo superano l'obiettivo definito dal perimetro classico della viabilità e della sicurezza.

Il tema, che si inquadra nella disciplina costituzionale della libertà di circolazione, oggi si estende ad ambiti quali le politiche dei trasporti, la salute, la logistica, i mezzi stessi più adeguati ad assicurare gli spostamenti.

Si tratta di temi sottoposti a continue evoluzioni settoriali, chiamati ad interagire a favore del miglioramento dei molti obiettivi che la parola mobilità racchiude, affrontando complesse questioni economiche e sociali.

Rispetto alla mobilità, la digitalizzazione delle informazioni può essere considerata il comune linguaggio tecnico che consente a contesti molto differenti di interagire efficacemente elaborando dati in un formato matematico comune. Diviene così possibile integrare capacità e competenze varie, ciascuna influente sulla mobilità, valorizzando le peculiarità di ognuno degli ambiti che vi concorrono.

Una delle conseguenze pratiche più evidenti di tale integrazione di competenze si manifesta nell'incremento del livello di automazione della mobilità stessa, per rispondere ad esigenze molto articolate in termini di

* La sessione è stata moderata dalla dott.ssa **Simona Burattini**, Giornalista RAI TG2

sicurezza, flussi di traffico, emissioni, mezzi di trasporto, pianificazione territoriale, logistica, ecc.

Lo sviluppo dei veicoli presenta riconoscibili tappe evolutive in relazione alle tecnologie. Sino agli anni '70 la dinamica di un veicolo si presenta interamente dipendente dal guidatore. Successivamente, i primi sistemi di controllo elettronico del motore e degli impianti frenanti (ABS) danno origine ad una pluralità di sistemi di assistenza alla guida (ADAS). Il veicolo, ormai sensorizzato, sino alla fine del '900 è però ancora privo di comunicazione con il mondo esterno e la focalizzazione è sulla sicurezza funzionale (safety). Nel primo decennio degli anni 2000 il veicolo inizia a comunicare con l'esterno (smartphone, mappe per navigazione).

Si introducono georeferenziazione e sensori (radar, lidar, telecamere) per fornire ai sistemi di controllo del veicolo informazioni su traffico, persone e segnaletica intorno al veicolo e sviluppare di conseguenza gli ADAS attuali. Si rilevano accessi malintenzionati alla rete informatica di bordo, con conseguenze sul controllo dinamico del veicolo. La focalizzazione tecnologica si estende così alla security.

Di recente compaiono sistemi in grado di rilevare anche l'interno del veicolo, per osservare sia il comportamento del guidatore (incipiente addormentamento, stato di ebbrezza, ecc.) sia dei passeggeri.

La focalizzazione tecnologica inizia a recepire necessariamente le direttive sulla privacy.

Analogo sviluppo tecnologico accompagna negli anni la digitalizzazione degli scenari ambientali di traffico (si pensi alle mappe), la georeferenziazione dei veicoli con crescente precisione, la trasmissione di grandi quantità di dati attraverso le reti di radionavigazione, la progettazione delle infrastrutture viarie.

A questi sviluppi tecnologici si accompagna l'evoluzione delle normative, che ne disciplinano l'impiego a favore dell'interesse collettivo.

Si giunge così alla situazione attuale, con uno scenario tecnologico in cui vi è grande abbondanza di dati, acquisibili in forma digitale dalle fonti più varie: amministrazioni pubbliche, reti di comunicazione, veicoli, persone, infrastrutture, ecc.

La digitalizzazione è pertanto applicata a più ambiti e livelli: veicolo, infrastruttura, ambiente, giuridico, economico, ecc.

Semplificando, si possono individuare essenzialmente quattro ambiti di digitalizzazione, di cui il primo è il contesto della mobilità, in termini di gestione dei segnali e dei dati delle infrastrutture: mappe tridimensionali, definizione scenari ambientali, acquisizione flussi mobilità, regolamentazioni, ecc.

Il secondo è la riproduzione realistica del traffico generato da qualsiasi veicolo, persona o animale, che acceda all'infrastruttura stradale.

Il terzo è costituito dall'ambito della descrizione delle caratteristiche e della dinamica dei veicoli, più o meno equipaggiati con sistemi automatici, e dei guidatori.

Il quarto riguarda le reti di comunicazione e di radionavigazione. Si prospetta una crescente rilevanza della capacità di gestire grandi quantità di dati (IA) e di integrare un quadro normativo in prevedibile evoluzione.

Le normative evolvono recependo il potenziale che l'integrazione delle tecnologie riassunte sopra porta con sé.

Ad esempio, il Regolamento UE 2019/2144 prevede la dotazione obbligatoria di vari ADAS (oltre a ABS e ESC, già obbligatori) e della scatola nera sui nuovi veicoli passeggeri a partire dal 6 luglio 2022 per rilascio dell'omologazione UE, dal 7 luglio 2024 per i veicoli di nuova immatricolazione, dal 2029 per i mezzi pesanti.

Tra i sistemi ADAS obbligatori dal 2022 si ricordano la frenata automatica di emergenza (AEB), il mantenimento di corsia (Emergency Lane Keeping - ELK), il monitoraggio della sonnolenza e riconoscimento della distrazione del conducente (DMS), l'ausilio al mantenimento della velocità più idonea (Intelligent Speed Assistance - ISA), l'interfaccia di installazione di dispositivi di tipo alcolock, la segnalazione di arresto di emergenza e rilevamento in retromarcia, il registratore di dati di evento (c.d. scatola nera), ecc.

Si tratta di un'evoluzione tecnologica che ha importanti implicazioni sul tema della responsabilità in caso di violazioni, incidenti o malfunzionamenti.

Per quanto riguarda le crescenti implicazioni sulla privacy, si pone l'obbligo del suo rispetto, assicurando una chiara gestione dei dati in termini

di analisi, trattamento, conservazione, flusso dai dispositivi di bordo e di comunicazione verso i centri di gestione dei dati stessi.

E' prevedibile che l'evoluzione della mobilità sarà progressiva e molto graduale.

Quanto indicato in precedenza comporta la necessità di uno sviluppo parallelo di diverse tecnologie, competenze, regolamentazioni e modalità di verifica che rendano sicuro, vantaggioso e sostenibile l'intero processo.

Esiste il problema di definire chi sosterrà il costo di questo cambiamento.

Obiettivi ambientali, di sicurezza ed economici, sono comunque destinati a continuare a mantenere questa tendenza.

Ciò comporterà, insieme a quelle strettamente tecnologiche, crescenti sfide legate alla privacy.

C'è infine da chiedersi se ci si stia preparando a considerare la persona nella prospettiva di una mobilità diretta verso una crescente automazione. Se la risposta è affermativa, con quali metodologie.

La presentazione introduce per questo all'impiego di simulatori dinamici come sistemi di sviluppo dei veicoli, talvolta utilizzati per la formazione di guidatori professionali, in grado di verificare come il guidatore interagirà con un qualunque scenario di traffico, rete di comunicazione, allestimento veicolo, condizione meteo, ecc., in condizioni di sicurezza e ripetibilità di qualunque situazione di guida.

E' una metodologia basata sulla digitalizzazione di quanto concorre alla mobilità, che consente di analizzare preventivamente gli effetti introdotti dall'evoluzione di uno qualsiasi degli elementi presentati.

L'analisi del flusso dei dati che permette a tali sistemi di simulazione dinamica di riprodurre in sicurezza quanto potrà effettivamente avvenire in uno scenario di mobilità, si pensa che possa consentire di verificare preventivamente in un ambiente di laboratorio anche le modalità di trattamento dei dati stessi al fine di confermare il rispetto delle norme sulla privacy.

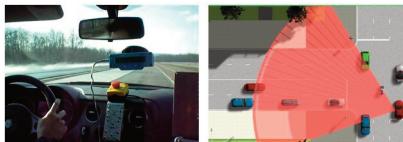
Mobilità e digitalizzazione

scenari, traffico, veicoli, persone

Prof. Mauro Velardocchia

Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)

Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino



“La Protezione dati: da 25 anni la bussola del futuro”

Torino, Palazzo Reale
4 luglio 2022



Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)
Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino

1/16

Contesto

Le direzioni di sviluppo della mobilità sono molteplici:

- impostazione globale della pianificazione di città, territori, logistica
- gestione di flussi di traffico crescenti, preservando il consumo di territorio
- risparmio energetico e riduzione delle emissioni ambientali ed acustiche
- incremento della sicurezza stradale, anche in relazione all'invecchiamento della popolazione

Questo richiede una accresciuta capacità di analisi e induce a perseguire una crescente automazione del sistema della mobilità.

A un livello comparabile alla rivoluzione della mobilità degli anni '30 dovuta alla diffusione del motore endotermico, si pone il tema della riscrittura delle regole che assicurino diritti/doveri del singolo, la tutela della strada, ed il primato dell'interesse collettivo (v. Direttiva gestione integrata sicurezza stradale del 2019 – ITS e Smart Road, Regolamento EU 858/2018 e 2144/2019 – Requisiti omologazione e ADAS)

Gli interessi economici in gioco sono enormi, come lo sono le opportunità di lavoro e le ricadute sociali.



Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)
Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino

2/16

Safety – Security - Privacy

Un passo dopo l'altro

- Sino anni '70 - dinamica veicolo interamente dipendente dal guidatore;
- Fine '70 - primi sistemi di controllo elettronico impianti frenanti (ABS). Si sviluppa una pluralità di sistemi di assistenza alla guida (ADAS). Il veicolo, ormai sensorizzato, è però ancora privo di comunicazione con il mondo esterno. La focalizzazione tecnologica è sulla sicurezza funzionale (**safety**):
- Primo decennio 2000 - il veicolo inizia a comunicare con l'esterno (smartphone, mappe per navigazione). Si introducono georeferenziazione e sensori (radar, lidar, telecamere) per osservare il traffico, persone e segnaletica intorno al veicolo e sviluppare gli ADAS attuali. Si rilevano accessi malintenzionati alla rete informatica di bordo, con conseguenze sul controllo dinamico del veicolo. La focalizzazione tecnologica si estende alla **security**;
- Di recente compaiono sistemi in grado di rilevare anche l'interno del veicolo, per osservare sia il comportamento del guidatore (incipiente addormentamento, alterazione, ecc.) sia dei passeggeri. La focalizzazione tecnologica inizia a recepire le direttive sulla **privacy**

Col tempo le tecnologie hanno incrementato la **sicurezza** di un veicolo ma siamo ad un incrocio tra safety – security – privacy, e responsabilità, che deve tenere conto della **mobilità nel suo insieme**



Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)
Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino

3/16

Mobilità e digitalizzazione

Esiste una **abbondanza di dati**, acquisibili in forma digitale dalle fonti più varie: **amministrazioni pubbliche, reti di comunicazione, veicoli, persone, infrastrutture, ecc.**

I temi trattati richiedono **competenza multidisciplinare** (ingegneristica, giuridica, ecc.) nel tema **Mobilità e digitalizzazione**

Si può intendere con **digitalizzazione** la capacità di elaborare dati, disponibili da ambiti anche molto differenti (infrastruttura, veicolo, comportamentali, condizioni ambientali, Leggi, ecc.), in un formato matematico comune, idoneo per analizzare scelte alternative.

Ad esempio, per integrare una immagine di un segnale stradale nel sistema di controllo della dinamica di un veicolo devo necessariamente digitalizzarla.

La digitalizzazione è pertanto applicata a **più ambiti e livelli**: veicolo, infrastruttura, comportamentale, ambientale, giuridico, economico, ecc.



Mobilità e digitalizzazione. Ambiti

Semplificando, possiamo individuare almeno **tre ambiti di capacità di digitalizzazione**:

1. **Il contesto della mobilità**, in termini di gestione dei segnali e dei dati delle infrastrutture e dei veicoli: mappe 3D HD, definizione scenari ambientali, acquisizione storico flussi mobilità, regolamentazioni, ecc.;
2. **Riproduzione realistica del traffico** generato da qualsiasi veicolo, persona o animale, che sia abilitato a fruire o ad interferire con **l'infrastruttura stradale**;
3. **Veicoli**, più o meno equipaggiati con sistemi automatici, e **guidatori**.



Insieme a questi ambiti agiscono quelli, di per sé digitali, propri delle **reti di comunicazione e di radionavigazione**



Mappe 3D HD, gestione segnali infrastrutture e veicoli



Esempio di mappe dinamiche (HERE Technologies)



HERE HD Live Map – integrazione di segnali provenienti da sensori bordo veicolo



Modellazione realistica del traffico

I sistemi per la simulazione digitale del traffico consentono di:

- Simulare realisticamente complesse interazioni tra veicoli, pedoni, infrastruttura e gestione dinamica della segnaletica;
- Modellizzare domanda, offerta e comportamenti, inclusa la valutazione dei consumi, dei tempi di spostamento, degli intasamenti, ecc.
- Simulare nuove forme di mobilità: Veicoli Connessi e Automatizzati (CAV) e Mobility as a Service (Mobilità come Servizio – MaaS – Il MaaS (Mobility as a Service), un modello di gestione per l'erogazione di servizi di trasporto, che prevede un abbonamento mensile a forfait per un insieme di trasporti pubblici e privati: treni, bus, taxi, car, bike sharing, ecc.



Simulazione flussi di traffico per l'ottimizzazione della gestione dei semafori per ridurre le emissioni

La mappa è corrispondente alla realtà, il traffico vi è simulato all'interno



Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)
Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino

7/16

Modellazione realistica del traffico

Smart city e smart road. La simulazione digitale studia come migliorare i flussi di traffico, la sicurezza delle strade e la mobilità. Si applica ad ambienti urbani o extraurbani per mantenere o migliorare la capacità di trasporto grazie all'uso più efficiente di infrastrutture esistenti.

Di rilievo è la possibilità di applicare tempestivamente le Regolamentazioni nel loro divenire.



Simulazione Multimodale del Traffico
Studiare la mobilità considerando una pluralità di mezzi di trasporto ed i pedoni.

Simulazioni in VR del traffico possono essere utilizzate anche nell'ambito di consultazioni pubbliche, per presentare in modo coinvolgente e immersivo una diversa gestione del traffico urbano, nuove infrastrutture, l'adozione di veicoli con nuove potenzialità.



Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)
Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino

8/16

Il veicolo - Sicurezza stradale e sistemi ADAS

E' ormai normato che l'azione del guidatore possa essere assistita o preceduta dal controllo automatico del veicolo (ADAS).

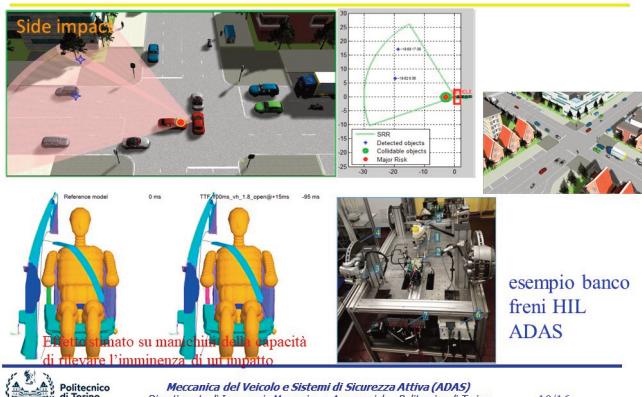
Questo implica una vasta sensorizzazione del veicolo per valutarne la dinamica e lo scenario dinamico (applicazioni IA) intorno ad esso. E' indispensabile la verifica della permanente sicurezza dell'intervento dei sistemi automatici, anche al variare delle condizioni operative e manutentive



Meccanica del Veicolo e Sistemi di Sicurezza Attiva (ADAS)
Dipartimento di Ingegneria Meccanica e Aerospaziale - Politecnico di Torino

9/16

Scenari di veicoli nel traffico, banchi studi ADAS, dieci anni fa...



Integrazione mappe, scenari, traffico, regole, veicoli, ecc. OGGI

Gli ambienti di sviluppo software sono in continuo sviluppo. E' necessaria una competenza specialistica sul veicolo e sui sistemi meccatronici.

Si prospetta una crescente rilevanza della capacità di gestire grandi quantità di dati (IA) e di integrare un quadro normativo in prevedibile evoluzione.



ADAS, sensorizzazione abitacolo, scatola nera

Il Regolamento UE 2019/2144 prevede la dotazione obbligatoria di vari **ADAS** (oltre a ABS e ESC, già obbligatori) e della **scatola nera** sui nuovi veicoli entro:

- 6 luglio 2022 per rilascio dell'omologazione UE
- 7 luglio 2024 per i veicoli di nuova immatricolazione; 2029 per i mezzi pesanti

Sistemi ADAS obbligatori dal 2022:

- Frenata automatica di emergenza (AEB);
- Mantenimento di corsia (Emergency Lane Keeping - ELK);
- Monitoraggio della sonnolenza e riconoscimento della distrazione del conducente (DMS);
- Ausilio al mantenimento della velocità più idonea (Intelligent Speed Assistance - ISA)
- Interfaccia di installazioni di dispositivi di tipo alcolock;
- Segnalazione di arresto di emergenza e rilevamento in retromarcia;
- Registratore di dati di evento: velocità del veicolo, ecc.

Il Driver Monitoring System (DMS) funziona in base a **sistemi di imaging** che elaborano informazioni provenienti da sensori che acquisiscono l'interno dell'abitacolo.
L'ISA si basa su rilevo e interpretazione (IA) della **segnaletica stradale**.

Per quanto riguarda la **privacy**, la gestione dei dati non deve permettere di identificare né il singolo veicolo, né il proprietario, conservando inoltre le informazioni per un tempo limitato.



La persona alla guida nello scenario evolutivo della mobilità

CHE FINE FA, IN TUTTO QUESTO, LA PERSONA ALLA GUIDA?

E' prevedibile che l'automazione della mobilità sarà progressiva e molto graduale. Quanto indicato in precedenza comporta la necessità di uno **sviluppo parallelo** di diverse tecnologie, competenze, regolamentazioni e modalità di verifica che rendono sicuro, vantaggioso e sostenibile l'intero processo. Esiste il problema di definire chi sosterrà il costo di questo cambiamento (costruttori, gestori infrastrutture stradali e di comunicazione, cittadini, ...?)

Obiettivi **ambientali**, **di sicurezza** ed **economici**, sono comunque destinati a continuare a sostenere questa tendenza.

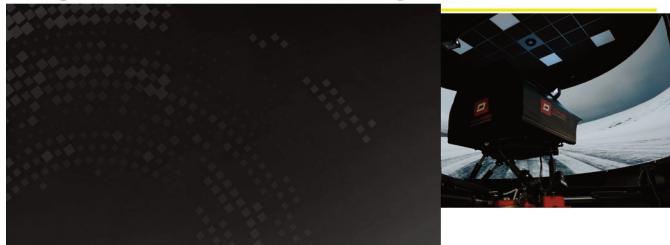
Ciò porterà, insieme a quelle strettamente tecnologiche, sfide legate alla **privacy**.

C'è ancora da chiedersi se ci stiamo preparando a considerare la persona nella prospettiva di una mobilità diretta verso una crescente automazione.

Se la risposta è affermativa, con quali metodologie?



La persona nello scenario della mobilità digitalizzata



Un simulatore di ultima generazione (Driver-in-the-loop) consente di verificare come il guidatore interagirà con un qualunque scenario di traffico, rete di comunicazione, allestimento veicolo, condizione meteo, ecc. in condizioni di **sicurezza** e **riperibilità** di qualunque situazione di guida

Questa metodologia, basata sulla digitalizzazione di quanto concorre alla mobilità, consente di analizzare preventivamente gli effetti introdotti dall'evoluzione di uno qualsiasi degli elementi presenti



Conclusioni

Lo sviluppo della mobilità, sostenuto dalla capacità di digitalizzazione, (scenari HD, traffico, mezzi di trasporto, comunicazioni) si varrà nel tempo di ulteriori tecnologie e regolamentazioni. Esso pone **opportunità ed interrogativi** (chi presidia le tecnologie? Come si definiscono le regole? Come si assicura la privacy?) di complessità destinata a crescere.

Il ruolo delle Università pare **molto rilevante** e da **aggiornare**, anche in questo ambito. E' infatti prevedibile che si rivelerà essenziale la **qualità della formazione**.

A investimenti comparabili, al solito, la **differenza** continueranno a farla persone con competenze diverse e la loro capacità di lavorare per integrarle.



Questa presentazione è dedicata ai Professori che mi sono stati maestri ed ai miei allievi



L'INTELLIGENZA ARTIFICIALE IN ITALIA:
STRATEGIE PRESENTI E PROSPETTIVE FUTURE
Barbara Caputo

Professoressa di Intelligenza Artificiale, Politecnico di Torino

L'Intelligenza Artificiale e' senza dubbio la scienza le cui ricadute tecnologiche avranno l' impatto trasformativo piu' dirompente sull'economia, la società, la sicurezza, la difesa e gli equilibri geopolitici a livello mondiale nel ventunesimo secolo. Una tecnologia dagli effetti cosi' dirompenti va presidiata a vari livelli: scientifico, tecnico, legislativo e strategico.

Per questo motivo tutti i paesi industrializzati (e non solo) hanno dedicato negli ultimi 5 anni grande attenzione al tema, dotandosi di strategie Nazionali per pianificare investimenti a supporto di politiche di sviluppo. Parimenti, diversi attori internazionali hanno promosso la creazione di associazioni e tavoli permanenti sull'Intelligenza Artificiale, per cercare di costruire un linguaggio comune con cui dialogare su questo tema, e individuare principi condivisi per governare il suo sviluppo.

L'Italia non ha fatto eccezione, e nel 2021 il paese si e' dotato di un Programma Strategico per l'Intelligenza Artificiale 2022-2024. Il documento, frutto della collaborazione del Ministero dell'Universita' e della Ricerca, del Ministero dello Sviluppo Economico e del Ministro per l'innovazione tecnologica e la transizione digitale, individua ventiquattro politiche strategiche per il potenziamento del sistema dell'Intelligenza Artificiale in Italia.

La visione complessiva e', in linea con la Strategia Europea sul tema, quella di una IA che metta l'uomo al centro, individuando nella formazione, la ricerca di base e l'innovazione i tre pilastri fondamentali intorno ai quali strutturare le 24 linee di intervento. Alcune delle azioni identificate dalla strategia, come la nascita del dottorato nazionale in intelligenza artificiale e la nascita di un ecosistema diffuso di ricerca sponsorizzato dai fondi PNRR sono in corso, altre sono in procinto di partire, come il centro di AI per automotive e aerospazio che dovrebbe fare da catalizzatore per l'innovazione in questi due settori strategici per l'economia nazionale.

E' però importante essere consapevoli che l'attuale Programma Strategico e' stato concepito in piena emergenza pandemica, immaginando un futuro post-covid di grande ripresa economica su scala globale.

Quel futuro immaginato non si e' realizzato.

Ci troviamo ormai in un mondo diverso, con equilibri geopolitici radicalmente diversi e una nuova prospettiva di futuro. E' fondamentale iniziare a lavorare ora al nuovo Programma Strategico per l'Intelligenza Artificiale 2025-2027, un programma che tenga conto di questo mutato contesto mondiale e che venga sviluppato coinvolgendo il mondo accademico così come quello produttivo, i vertici della sicurezza e della difesa, e la Pubblica Amministrazione nella sua totalita'.

E' altresi' cruciale avviare una riflessione sull'opportunita' di riconoscere all'Intelligenza Artificiale l'importanza strategica che e' stata riconosciuta alla Cybersecurity e all'Aerospazio, riconoscimento che porti ad assegnare sull'Intelligenza Artificiale i poteri di indirizzo, coordinamento, programmazione e vigilanza alla Presidenza del Consiglio dei Ministri.

I recenti fatti di cronaca, con il lancio su scala mondiale di ChatGPT da parte di OpenAI, l'enfasi sfrenata e interessata rispetto alle sue capacita' di generare automaticamente testi e rispondere a richieste ad amplissimo spettro da parte degli utenti in maniera piu' o meno competente; l'emergere di criticita' in termini di veridicità e affidabilità del contenuto di tali testi e la reazione del Garante per la Protezione dei Dati Personalii a difesa dei diritti dei cittadini e dei minori, fanno capire come la partita dell'Intelligenza Artificiale sia complessa e solo all'inizio.

L'auspicio è che l'Italia possa reagire con prontezza a questa sfida e diventare punto di riferimento e pungolo critico a livello mondiale ed europeo, dove ormai da troppo tempo si attende l'emanazione di una proposta di regolamento nella forma dell'AI Act.

NUOVE PROTESI COGNITIVE?
I DATI AI TEMPI DELL' INTERNET OF THINGS
Prof.ssa Anna Maria Mandalari
*Professoressa presso l'Institute for Security
Science and Technology dell'Imperial College di Londra*

Sappiamo che qualsiasi oggetto al giorno d'oggi può essere connesso a Internet dagli altoparlanti intelligenti alle camere di sicurezza, anche il frigorifero può essere connesso a Internet. Chiamiamo questi dispositivi Internet of Things (IoT).

L'Internet delle cose è uno strumento molto potente e ci permette di vivere una vita comoda.

Ma perché costano così poco e qual è il vero valore che ci restituiscono?

È proprio qui che è iniziato il mio viaggio di ricerca, volevo capire cosa stiamo invisibilmente offrendo in cambio a questi dispositivi.

In questo contesto, dobbiamo considerare tre passi fondamentali:

1)Privacy contro espedienti minori.

2) In che modo i dispositivi IoT espongono la privacy in una casa intelligente

3) Qual è l'impatto che i dispositivi avranno in futuro.

All'inizio di questo viaggio, abbiamo studiato come i dispositivi IoT trattano i dati degli utenti e esplorato in modo approfondito se violano la privacy dell'utente. La motivazione principale della ricerca in questione è che questi dispositivi sono considerati "black hole", possono (per definizione) accedere a Internet e quindi possono esporre informazioni private.

Inoltre, vi è una mancanza di comprensione su quali informazioni espongono, su quando le espongono e a chi. Non sono chiare le differenze regionali nelle normative (ad es. il GDPR è presente in Europa ma non è disponibile all'estero).

La nostra prima ricerca include i seguenti punti:

1) Quali sono le destinazioni contattate dai dispositivi IoT?

- 2) Quali informazioni vengono inviate?
- 3) Si comportano in modo inaspettato?

Per rispondere a queste domande, abbiamo acquistato più di 200 dispositivi diversi, dagli elettrodomestici alle camere intelligenti, agli hub intelligenti e altri dispositivi di automazione domestica e li abbiamo posizionati presso l'Imperial College di Londra e in un appartamento-studio della Northeastern University (NEU). Il laboratorio IoT dell'Imperial College è gestito da me e dal Professore Hamed Haddadi, mentre quello di NEU è mantenuto dal ricercatore italiano Daniel Dubois e dal Professore David Choffnes.

La nostra metodologia di ricerca si basa sulla raccolta del traffico Internet prodotto da questi dispositivi e l'esecuzione automatica di esperimenti ripetibili su larga scala. La Figura 1 mostra i laboratori in Gran Bretagna e Stati Uniti.

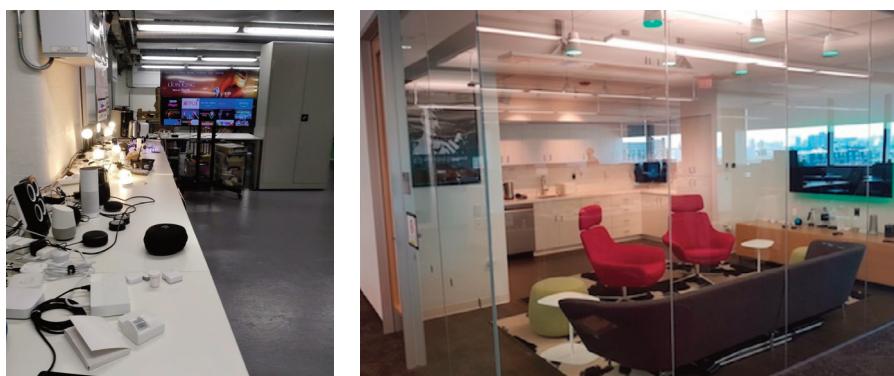


Figura 1: Laboratori IoT in Gran Bretagna e Stati Uniti.

La raccolta dei dati avviene sul router, il router distingue il traffico per dispositivo e per esperimenti; quindi il comportamento del dispositivo è completamente isolato.

Come mostrato nella Figura 2, da una prima indagine, abbiamo visto che la maggior parte del traffico dal laboratorio del Regno Unito va negli Stati Uniti o in Cina.

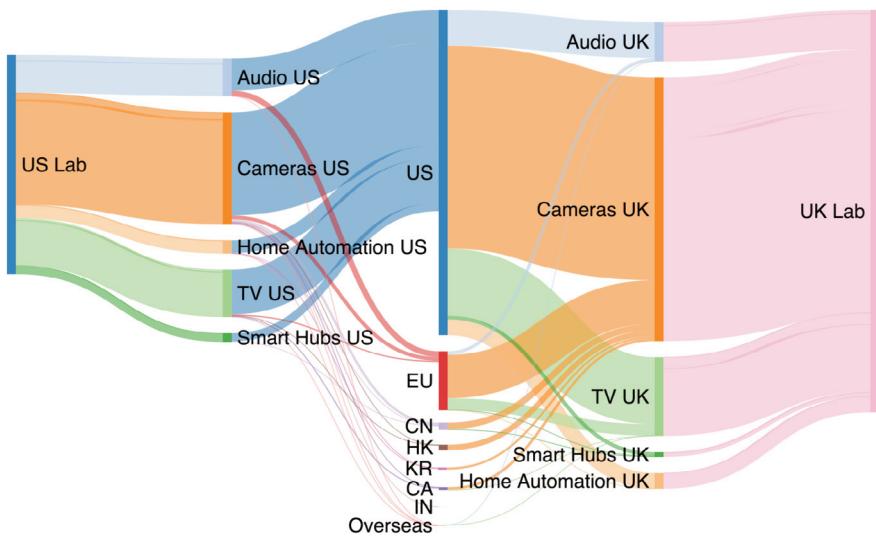


Figura 2: Diagramma del traffico Internet dei dispositivi.

Il traffico proveniente da molte categorie di dispositivi IoT viene inviato al di fuori delle giurisdizioni sulla privacy del nostro laboratorio.

Abbiamo riscontrato altre violazioni della privacy, ad esempio:

- 1) Alcuni citofoni intelligenti registravano ad ogni movimento e rimandavano la registrazione al server cloud di un altro paese anche se questo era stato disabilitato nell'app.
- 2) Le smart TV contattavano Facebook, Netflix, Google e alcuni tracker pubblicitari.
- 3) Gli altoparlanti intelligenti si attivavano senza pronunciare la parola chiave.

Abbiamo poi studiato in maniera più approfondita il comportamento degli altoparlanti intelligenti, per capire se si attivavano senza il permesso dell'utente.

Dai nostri esperimenti è emerso che gli altoparlanti intelligenti spesso si attivano in modo del tutto inaspettato, con parole chiave simili alla parola

chiave di attivazione, arrivando a attivarsi in modo errato per un massimo di 10 secondi.

Abbiamo scoperto inoltre che la maggior parte del traffico non viene inviato al produttore, ma a “terze parti”, come tracker e inserzionisti.

Spesso il contratto stabilito con il produttore consente loro di trasferire i tuoi dati a parti terze, ma l’utente non ne è a conoscenza, in quanto i termini e le condizioni sono troppo vaghe. Ciò produce un rischio per la privacy.

I problemi principali sono molteplici:

- 1) Profilazione - Basata sui dispositivi e sul traffico dai dispositivi. Terze parti possono creare un profilo unico dell’utente. Preferenze, interessi, è facile capire cosa piace all’utente e influenzare scelte future.
- 2) Il rischio maggiore è la cosiddetta “influenza di massa”.
- 3) Il segnale vocale è anche una ricca risorsa per aziende terze, poiché rivela diversi possibili stati di un utente, come stato emotivo, livelli di stress, condizione fisica, età, sesso e tratti personali. I fornitori di servizi possono creare un profilo molto accurato della categoria demografica di un utente, delle preferenze personali e questo può compromettere la privacy.

Quando pensiamo al futuro di questi dispositivi, sappiamo che saranno molto più sofisticati. Cosa succederà quando questi dispositivi diventeranno più simili a protesi cognitive? Aiutando l’utente a prendere decisioni sugli argomenti più intimi. Con l’accesso ai dati dell’utente le piattaforme tecnologiche impareranno le preferenze, anticiperanno i bisogni e comportamenti, monitoreranno la salute. Ma in realtà in questo futuro potrebbero emergere piattaforme che usano i dati dell’utente per il motivo sbagliato.

Nella mia visione del futuro dei dispositivi IoT, il controllo sarà di nuovo nelle mani del consumatore. L’utente sarà consapevole di quando le informazioni vengono utilizzate in modo negativo o per scopi poco chiari.

Tutti i dispositivi IoT in uso saranno certificati e affidabili con soluzioni non più presenti nel cloud ma vicino agli utenti, nell’edge.

I produttori dovranno dichiarare le destinazioni che i dispositivi stanno contattando e i motivi per cui stanno contattando destinazioni specifiche (in particolare terze parti). I certificati includeranno sicurezza, privacy, consumo energetico. La Figura 3 mostra un prototipo di certificato IoT.

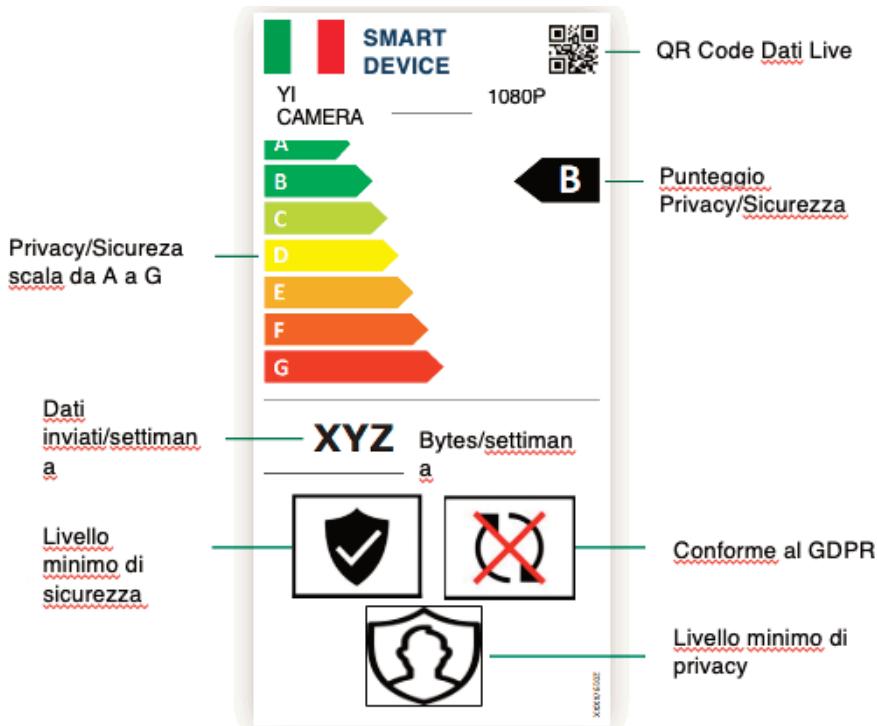


Figura 3: Prototipo di certificato IoT.

Ad Imperial stiamo inoltre sviluppando un software che permette di proteggere la privacy e la sicurezza dell'utente. Dalla nostra analisi è emerso che parte del traffico IoT è essenziale per far funzionare il dispositivo e parte non è essenziale, abbiamo quindi sviluppato un software che permette di “bloccare” alcune comunicazioni non essenziali e continuare a utilizzare perfettamente il dispositivo. Questo software funzionante nel router di casa prende il nome di IoTrim (Figura 4).

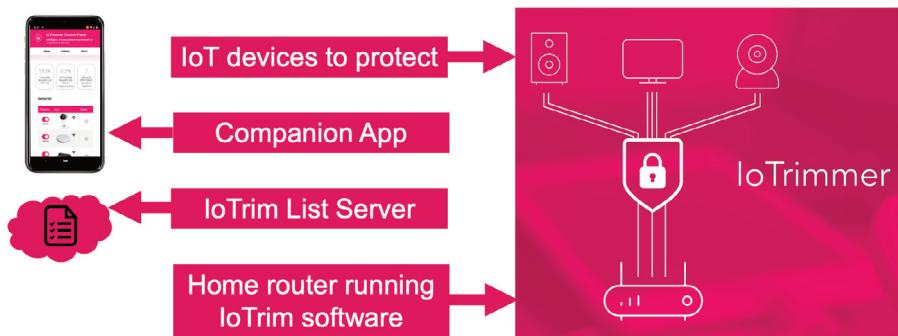


Figura 4: IoTrim.

IoTrim, utilizzando tecniche di intelligenza artificiale, identifica automaticamente tutti i dispositivi collegati al router degli utenti e il traffico non essenziale, proteggendo così la privacy e la sicurezza dell’utente e mantenendo le connessioni IoT private e sicure.

INNOVAZIONE, AI & IoT: RIFLESSIONI DEI PROFESSIONISTI

Dottore Commercialista Paola Zambon

*Tavolo congiunto GDPR Ordine Dotti Commercialisti
ed Esperti contabili, Avvocati ed Ingegneri di Torino*

Nella sessione dedicata all’IoT ed all’IA ed all’innovazione è intervenuta Paola Zambon che, a nome del Tavolo congiunto GDPR degli Ordini Professionali di Torino (Dotti Commercialisti, Avvocati, Ingegneri), ha apportato riflessioni in tema di IA ed IoT dei professionisti del Tavolo stesso.

La relatrice ha esordito ringraziando le autorità presenti ed apportando il saluto dei presidenti degli Ordini professionali e ha quindi ricordato che Tavolo stesso per primo in Italia è nato per apportare supporto a professionisti ed imprese nei chiarimenti operativi del GDPR in linea con le migliori interpretazioni del diritto di impresa e seguendo sempre le linee dell’Autorità Garante.

La tecnologia dovrebbe sempre essere posta al servizio delle persone in piena sicurezza e nel rispetto dei valori e dei diritti fondamentali dell’UE, anche secondo il più recente indirizzo europeo, nonostante il sempre più stretto interfacciamento tra uomo-macchina-ambiente.

La trasformazione digitale antropocentrica e sostenibile, dunque, è ciò che le imprese si prefiggono di raggiungere con il valore aggiunto che possono apportare i sistemi di intelligenza artificiale, taluni anche con l’utilizzo dei big data, ma vi sono ancora cammini da percorrere su alcune problematiche (es.: la carenza del reperimento delle competenze adeguate sul mercato (sia di tecnici che di professionisti), i pericoli della manipolazione sociale e della sorveglianza di massa).

Il principio di responsabilizzazione deve riguardare sia le imprese che le persone, oggi rese sempre più informate sui rischi derivanti dal trattamento dei propri dati personali ma spesso ancora poco consapevoli degli effetti che gli stessi possono avere nella loro vita, sia per sottovalutazione che per l’opacità stessa dei modelli presenti sul mercato.

Il diritto dell’impresa è ormai da anni permeato sempre più da agenti intelligenti e da sistemi di intelligenza artificiale, in cui il modello europeo si

prefigge essere antropocentrico, etico, equo, sicuro, affidabile e sostenibile. In tale ottica, la professionista evidenzia che il quadro macroeconomico delle aziende italiane non gode di ottimo posizionamento internazionale poiché gli investimenti privati massivi sono soprattutto effettuati dall'estero (es. USA, Cina). La circolazione dei dati avviene ed è avvenuta soprattutto tramite l'utilizzo di IoT, poiché anche a causa della pandemia, le persone hanno cambiato abitudini e stili di vita ed è cresciuto esponenzialmente il ricorso a piattaforme non europee per molti tipi di servizi. Non può fare a meno di notare che la "dichiarazione sui diritti digitali" a livello europeo innesta un'importante pietra miliare, ad integrazione di principi già esistenti da considerarsi un tentativo di innovazione europea alla ricerca del compromesso tra modelli internazionali diversi per cultura e per differente status di evoluzione tecnologica. I nuovi «*virtual world*» devono incorporare i valori europei sin dall'inizio in modo che le persone si possano considerare protette come se fossero nel mondo reale.

La definizione stessa di intelligenza artificiale è molto dibattuta e di importanza strategica sul mercato. Nella ricerca di "standard" per tale tematica da attuare con particolare attenzione all'uomo, si ritiene essenziale il coinvolgimento dei Professionisti che abbiano maturato esperienza operativa su tali tematiche anche a fianco di PMI (che spesso faticano proprio ad inserirsi in tali mercati).

Ai fini dell'intervento, pertanto, dopo aver illustrato gli indubbi pregi che la tecnologia e l'IA possono apportare (es. nella ricerca scientifica inerenti alla salute, all'agricoltura, all'ambiente, ecc.), ha focalizzato l'attenzione su alcuni ambiti di riflessione che possono impattare anche sulla **corretta governance delle imprese**, sempre più collegate a tali sistemi, sebbene non sempre accompagnata da una adeguata conoscenza del GDPR ed in generale delle norme ad essi applicabili.

Tali macrotematiche sono:

1. la corretta governance per l'impresa che attua/adotta sistemi di IA
2. design etico e privacy by default e trasparenza algoritmica
3. la non discriminazione nei sistemi di IA e l'"innesto" della cultura della diversità e l'inclusione
4. la sostenibilità.

La corretta governance per l'impresa che attua/adotta sistemi IA

Cosa può essere ritenuto essenziale in una società che produce o adotta sistemi di intelligenza artificiale	Alcune problematiche sulle quali riflettere
<ul style="list-style-type: none">- Principi Privacy by design e by default- Diritto all'informazione degli interessati e applicazione del principio di trasparenza- Intervento umano nelle decisioni automatizzate- Consapevolezza degli utenti delle informazioni di profilazioni ottenute dai metadati incrociati (reazioni emotive, capacità cognitive, salute mentale, preferenze, gusti di ogni tipo, consumi, ecc.)- Servizio garantito (per non rischiare la mancata disponibilità dei dati che potrebbe essere molto pericolosa)- Accountability- Applicazione di garanzie di qualità e di design etico	<ul style="list-style-type: none">- Problemi legati alle skills: spesso mancano le competenze ed i profili adeguati- Problemi legati alla sicurezza: un attacco agli IoB può mettere a serio rischio la salute delle persone, anche la loro vita, sorveglianza di massa- Problemi legati alla socialità: manipolazione sociale, modifica e influenza sul comportamento umano, ecc.- Problemi legati alla concorrenza: il controllo sui dati IoT potrebbe creare un rischio di vendor lock-in e di dipendenza degli utenti da pochi produttori- Problemi legati alla sostenibilità ambientale: il consumo di energia previsto questi servizi porta ad un aumento di CO2- Problemi legati all'inclusione: spesso le donne non hanno competenze in IA, discriminazioni algoritmiche, disinformazione, ecc.

Il “**design etico**” in tema di imprese governate da o adottanti sistemi di intelligenza artificiale dovrebbe essere inherente non solo ai noti principi della *privacy by design e by default*, ma conglobare anche un realistico modello implementativo di etica, in modo che risulti affidabile. I modelli organizzativi in tal senso spesso riportano codici etici che non funzionano per diversi motivi: carenza di risorse atte a farlo funzionare, opacità nel processo decisionale, mancanza di indipendenza con l’organo di amministrazione e, spesso, ignoranza delle norme applicabili con presenza (se non assenza) di comitati che, se funzionano, non vengono ascoltati. In questo senso come Tavolo sia in qualità di giuristi di impresa (commercialisti ed avvocati) che di tecnici (ingegneri) è notevole il valore aggiunto che possiamo apportare al mercato anche a livello di responsabile consapevolezza.

Inoltre, si rimarca il focus sull’importanza del corretto modo di contemperare il metodo con il quale il training effettuato incida sulla complessità decisionale e sulla **trasparenza algoritmica** (anche per scongiurare approcci GiGo-istici, che sarebbero peraltro anche contrari ai principi di responsabilità sociale) di consueto tutelata dal segreto commerciale con l’opacità dei modelli decisionali rinvenibili sul mercato, evitando anche l’utilizzo di dark pattern che rendono volutamente difficile agli utenti comprendere i rischi nei quali potrebbero incorrere.

L’algorazia non dovrebbe portare peraltro alla disinformazione: è importante il ruolo che possono avere anche i professionisti per segnalare contenuti tecnici non appropriati soprattutto a danno delle società.

Un’altra grande sfida è rappresentata dal **diritto alla parità di genere** ed in generale al divieto di discriminazione che spesso si ritrova violato nell’applicazione dell’IA. «Gli algoritmi e l’apprendimento automatico ad essi correlato, se non sufficientemente trasparenti e robusti, rischiano di riprodurre, amplificare o contribuire a pregiudizi di genere di cui i programmatori possono non essere a conoscenza o che sono il risultato di una specifica selezione di dati.» Ad esempio, gli studi effettuati su campioni clinici e sanitari si basano di consueto su soggetti maschi bianchi (dunque è probabile che non siano adatti ad altri generi e alle persone di diverso colore).

Anche da quanto emerso dall’esperienza dell’Associazione ICT

Dott.Com ai cui eventi il Tavolo partecipa, il pregiudizio di genere nel processo decisionale algoritmico non si esplica solo in mancanza di adozione di corrette valutazioni da effettuare a livello progettuale, ma si ritrova anche sul mercato per la mancanza di diversità tra i professionisti che progettano, programmano, ingegnerizzano ed effettuano manutenzioni su tecnologie di intelligenza artificiale. Si segnala inoltre la difficoltà oggettiva sia in termini di addestramento che di monitoraggio sui processi collegati a sistemi di IA, quali ad esempio criteri consolidati nella misurazione di “bias” multimodali o la difficoltà di esercitare il diritto all’oblio nel *machine learning*. In molte imprese tecnologiche, la leadership è unicamente appartenente al genere maschile e non vi è conoscenza né competenza in tema di diversità e di inclusione.

Alcuni agenti intelligenti hanno anche un grande impatto sociale ed il rischio di sorveglianza sociale “di genere” è sempre alle porte. Ad esempio, negli USA alcune donne hanno disinstallato le app relative al ciclo mestruale per non poter essere libere di abortire (in alcuni Stati l’aborto è considerato illegale). Alcune società hanno così deciso di effettuare la cancellazione dalla cronologia della geolocalizzazione quando la persona si reca in una clinica per l’aborto, un rifugio contro la violenza domestica o altri luoghi simili.

Infine, nell’ottica della **sostenibilità**, si ritiene utile comprendere anche l’impatto ambientale e sociale, anche in relazione al mutamento dei profili e dei metodi di lavoro, che il sistema di intelligenza artificiale, adottato da un’impresa, apporta alla collettività e dunque anche valutare i benefici che produce rispetto al consumo di energia previsto per questi servizi che di consueto portano ad un aumento di CO₂ (rischio climatico ed ambientale). In tale ottica, i Commercialisti sono già avvezzi a trattare le informazioni non finanziarie relative alle imprese che, nel principio di continuità aziendale, saranno sempre più virate agli obiettivi Esg, nel più ampio quadro della **responsabilità sociale dell’impresa** finora lasciata perlopiù alla libera discrezionalità imprenditoriale, ma che, con l’incessante fiorire di norme che impattano sulla trasformazione digitale dell’impresa stessa, sta diventando sempre più complessa. Saranno importanti anche le informazioni concernenti il capitale intellettuale, umano, sociale e relazionale.

E’ importante inoltre coinvolgere anche i Professionisti nell’adozione

delle norme tecniche in quanto si ritiene essenziale la presenza di competenze trasversali per evidenziare alcuni aspetti che di consueto non vengono valutati dai tecnici quali ad esempio:

- **qualità del dato ed accountability:** non dovrebbe essere associata a mere norme tecniche proposte sul mercato ma anche alla sostenibilità, all'inclusione tenendo conto dell'impatto informativo non finanziario. Il data scientist (raro a trovarsi nel mercato) ha bisogno di essere affiancato da figure professionali che possano trasferirgli altre competenze anche nella costruzione della «data policy»;
- **conservazione:** di consueto questo aspetto viene ampiamente sottovalutato anche in termini di adeguamento normativo tecnico (non solo in riferimento alla normativa sulla privacy)
- **standard sì ma con attenzione:** rischio del proliferare di troppe proposte di standard e troppi interpreti sul mercato: andrebbero attentamente valutati. Mentre alcuni sono utili, altri potrebbero diventare strumenti normativi di fatto rigidi, disattendendo il concetto di «accountability» stesso che potrebbero portare alla fioritura di nuovi casi alla Corte di Giustizia Ue. Importante comprendere chi valuterà di fatto la conformità alcuni sistemi, specie se inerenti l'IA. Infine, i dati possono portare un valore aggiunto se sono costruiti da team adeguati (non solo tecnici ma anche professionisti con esperienza nella gestione del dato e nella privacy).

Infine, ricordando come i Professionisti ed in particolare i Dottori Commercialisti, gli Avvocati e gli Ingegneri di Torino sono disponibili e pronti ad aiutare le pmi alla trasformazione digitale, antropocentrica e sostenibile, si è rinviato al convegno del 18 novembre 2022 presso il Politecnico di Torino organizzato come sempre dall'Associazione ICT Dott.Com al quale ha partecipato l'Autorità Garante (Dr Agostino Ghiglia), evento nel quale peraltro sono stati ripresi alcuni di tali concetti.

PRIVACY E GESTIONE DEI DATI, VALORE E RISCHI DI UNA SINERGIA

Dott. Marco Gay

Presidente Confindustria Piemonte e ANITEC-ASSINFORM

Gentili colleghi, autorevoli relatori,

è un vero piacere essere qui con voi oggi. Il 25° anniversario dell'istituzione del Garante per la protezione dei dati personali ci dà l'occasione di riflettere e confrontarci sul futuro che i dati avranno nell'economia e nella società. Ciò che vorrei mettere a fuoco è il ruolo che avrà l'impresa nel proteggerli e valorizzarli.

La transizione digitale coinvolge in modo pervasivo la società e l'economia. Dalla città, alla fabbrica, all'abitazione, prodotti e servizi sono sempre più evoluti, versatili ed efficienti.

Rispetto solo a pochi anni fa la mole di dati che produciamo è impressionante. Questo soprattutto a causa di IoT e dispositivi connessi, tecnologie diffusissime sia in ambito industriale che nella vita di tutti i giorni.

Non è aumentato solo il volume dei dati, ma anche la nostra capacità di sfruttarli. Le nuove tecnologie hanno messo le basi per la nascita e lo sviluppo della cosiddetta "Data Economy".

Sfruttare i dati, in modo sempre più fine ed efficace, va ben oltre la loro monetizzazione, abbiamo a che fare con il concetto, più ampio, di creazione di valore. Una conseguenza avversa della possibilità di creare valore dai dati è l'aumento del rischio cibernetico. Per questo motivo bisogna moltiplicare gli sforzi per proteggere i dati che custodiamo.

In questo quadro, innovazione e regolazione sono due elementi indispensabili, che, per quanto in tensione, hanno bisogno di sostenersi a vicenda.

L'Unione europea ha avviato da tempo la costruzione di una sua "*costituzione digitale*". Si è partiti con il GDPR, il Regolamento sui dati personali che si è affermato come standard a livello globale sul trattamento dei dati, e si è proseguito fino ad arrivare a proposte ambiziose come il *Data Act* e l'*AI Act*.

Il Regolamento IA rappresenta il primo tentativo di regolare l'Intelligenza Artificiale a livello globale. L'obiettivo è - da un lato - di

stimolare l'innovazione nell'UE e - dall'altro - creare un ambiente di sviluppo affidabile e credibile per i cittadini. Un ecosistema dell'IA che metta l'"uomo al centro".

È innegabile che l'Unione europea abbia scelto di agire sulla regolazione per partecipare alla corsa iniziata da USA e Cina, due superpotenze globali che oggi sono molto più avanti su ricerca investimenti e brevetti.

Allo stesso tempo rimane un grosso rischio di inibire l'innovazione, e in particolare di sommergere PMI e Start-Up innovative di costi regolativi e burocrazia. Come sempre, quando si tratta di regolazione e di innovazione, per una policy che funzioni, il solo regolare non basta ed è anzi dannoso.

Difatti, gli strumenti più promettenti per la protezione della privacy e per la sicurezza delle nostre vite online provengono dalla ricerca scientifica e dalle applicazioni tecnologiche di frontiera, come le soluzioni avanzate di IA in ambito Cybersecurity, l'Edge computing e i dati sintetici.

- L'IA viene sempre più adottata nella Cybersecurity. Sappiamo bene come questa materia oggi sia centrale per l'attività di qualsiasi impresa, anche le meno digitalizzate. Nei casi di attacchi avanzati le soluzioni di IA possono contribuire a individuare anomalie che fanno sospettare un attacco e permettono un rilevamento tempestivo.

- In ambito di calcolo e elaborazione dati, si sta affermando il paradigma dell'Edge Computing, una tecnologia che garantisce importanti vantaggi in termini di protezione dei dati. Le informazioni restano nel perimetro aziendale, non necessitano un invio in aree centralizzate per essere elaborati ma possono essere processate direttamente vicino all'utente.

- I dati sintetici sono sicuramente una soluzione di nicchia e di frontiera ma hanno un mercato in grandissima crescita. Le aziende, non li utilizzano solo per allenare algoritmi di IA più precisi e performanti, ma anche per migliorare la compliance in materia di privacy. C'è una differenza abissale tra utilizzare dati sensibili, come quelli biometrici, provenienti da persone reali e dati biometrici sintetici generati da una rete neurale.

In conclusione, la sicurezza delle nostre vite digitali non passa solo dalla regolazione, che ci deve essere ma che deve avere contorni definiti e non ostativi della libertà imprenditoriale, ma anche, e soprattutto, dall'innovazione.

In questo senso l'industria ICT ha una funzione, di fatto, sociale. Essere abilitatori del progresso significa impegnarsi per garantire a tutti i cittadini le tecnologie più all'avanguardia e i più elevati standard di sicurezza in tutti i prodotti.

TERZA SESSIONE



IL GARANTE DEL FUTURO



- INTERVENTO DEL Prof. Pasquale Stanzione

Presidente del Garante per la protezione dei dati personali

- SANITÀ DIGITALE E PROTEZIONE DEI DATI PERSONALI:

UN BINOMIO POSSIBILE

Prof.ssa Ginevra Cerrina Feroni

Vice Presidente del Garante per la protezione dei dati personali

- METAVERSO, PRIVACY E FUTURO

Prof. Guido Scorza

Componente del Garante per la protezione dei dati personali

TERZA SESSIONE*

IL GARANTE DEL FUTURO

Prof. Pasquale Stanzione

Presidente dell'Autorità Garante per la protezione dei dati personali

Oggi abbiamo parlato dell'anniversario dei 25 anni del Garante.

Elemento comune alle varie relazioni è la consapevolezza di quanto questi 25 anni siano stati fondamentali nel delineare un governo dell'innovazione sostenibile in termini democratici. La stessa protezione dati ha subito un'evoluzione significativa, dal diritto di essere lasciati soli a diritto di autodeterminazione informativa, che si esprime nel governo sulla circolazione dei nostri dati personali. Il passaggio dalla privacy tradizionalmente intesa - come divieto d'ingerenza nella sfera privata - a diritto alla protezione dei dati è stato un po' il filo rosso sotteso al dibattito. Si è sottolineato il valore dei dati personali quali frammenti del nostro io, diviso (nella frammentazione che ne provoca la rete) in tante micro-identità, riferite a una parte (e soltanto una parte) di noi, che ci rappresenta ma non del tutto: elettore, consumatore, minore, detenuto, malato, vittima e così via.

La sfida di oggi è restituire integralità alla persona così frammentata e porla al centro dell'evoluzione tecnologica. Non a caso in sede di presentazione della relazione annuale si parlerà, il prossimo 7 luglio, di *umanesimo digitale*, ovvero dell'esigenza di funzionalizzazione dell'innovazione (che altrimenti sarebbe paradossalmente regressiva) alla tutela della persona. Presupposto di questo obiettivo è il governo consapevole della tecnica da parte dell'uomo, che non deve certo subire ma guidare l'innovazione, che in questo senso è un bene comune. E lo è nella misura in cui valorizzi diritti e libertà e non ne legittimi o, peggio, non ne amplifichi le violazioni (come avvenuto per le conseguenze discriminatorie dell'uso di alcuni algoritmi).

* Il dott. **Federico Monga**, Vice Direttore de *La Stampa*. ha intervistato i membri del Collegio del Garante

Determinanti, a tal fine, sono i principi di trasparenza, non discriminazione e diritto alla spiegazione della decisione algoritmica sanciti dal Gdpr.

Traendo, dunque, le conclusioni dei vari interventi possiamo dire che il progresso va promosso ma con atteggiamento distante tanto dallo scientismo acritico e dal soluzionismo tecnologico, quanto dal neoluddismo. L'innovazione necessita dunque di un vero e proprio umanesimo digitale, che valorizzi il personalismo su cui si fonda la nostra Costituzione.

Radici e orizzonti della protezione dei dati

Riflettere sull'evoluzione della disciplina di protezione dati implica, al contempo, una riflessione sul potere e sullo Stato di diritto oggi, sulla capacità del secondo di assicurare un governo dell'innovazione che ne rifletta il sistema assiologico, affiancando dunque, alla *rule of law*, un altrettanto ineludibile *rule of technology*.

Come il costituzionalismo moderno si è affermato mediante la progressiva costruzione dei limiti al potere statuale in funzione delle garanzie individuali, così oggi il processo di governo dell'innovazione non può prescindere dalla definizione di alcune regole essenziali a tutela della persona, rispetto al nuovo assetto di poteri indotto dal digitale.

Per comprendere appieno le implicazioni del potere performativo della tecnica sulla persona, si possono assumere come paradigmatiche alcune tematiche essenziali: l'identità e la sua rappresentazione in rete; la costruzione della personalità e la formazione dell'opinione pubblica; la tenuta delle garanzie individuali di fronte all'algocrazia.

Il primo profilo consente, infatti, di evidenziare come il digitale abbia scardinato non soltanto il sistema di allocazione tradizionale del potere, ma anche il processo di costruzione dell'identità e, quindi, il suo rapporto con la libertà.

Se il termine ‘identità’ è un *singularia tantum* è perché esso non è mai stato concepito che al singolare, rappresentato com’è stato da coordinate tendenzialmente immutabili tra cui il nome. Le nuove tecnologie hanno, invece, reso il termine “identità” necessariamente plurale, affiancando

all'identità fisica anche un caleidoscopio di identità digitali che concorrono, fin quasi a prevalere, sulla prima (l'utente, l'elettore, il consumatore ecc.).

Su questo terreno, la protezione dati ha svolto un ruolo centrale di "ricomposizione dell'Io diviso", polverizzato nei mille frammenti dispersi in rete, a garanzia della rappresentazione integrale della persona. E', questo, un risultato cui ha concorso anche l'elaborazione pretoria del diritto all'oblio, quale strumento di tutela rispetto alla cristallizzazione dell'io in un dettaglio spesso distorsivo.

Il potere performativo della tecnica sulla persona non si limita, tuttavia, alla sua rappresentazione ma giunge sino a toccarne quell' "*inner world*", quel foro interno ritenuto presidio invalicabile d'intangibilità in quanto presupposto essenziale di autodeterminazione: la libera formazione della coscienza individuale. La gerarchia e la selezione delle notizie decisa dagli algoritmi, che mostra o evidenzia solo alcuni contenuti e non altri, sono un esempio paradigmatico di come le nuove tecnologie condizionino lo stesso processo formativo dell'opinione pubblica.

Paradossalmente, una società, quale quella digitale, potenzialmente in grado di garantire la massima informazione, rischia invece di limitare artificiosamente l'accesso alle notizie, alimentando conformismo e insidiando l'autodeterminazione informativa. L'informazione rischia così di degenerare in "*auto-comunicazione di massa*" (Manuel Castells) e il *nudging* politico, reso possibile dalla propaganda ritagliata sul profilo di elettore attribuito all'utente dall'algoritmo, come nel caso Cambridge Analytica, rischia di destrutturare dall'interno le dinamiche democratiche.

Anche rispetto a questo tipo di distorsioni del processo formativo della coscienza individuale - con implicazioni importanti sulla vita pubblica - la disciplina di protezione dati offre alcuni strumenti, soprattutto preventivi, di tutela. Prima tra tutti è la previsione di un limite essenziale al controllo algoritmico, rimesso in parte alla volontà individuale mediante il dispositivo consensualistico e, in parte, alla valutazione eteronoma della non abusività dello sfruttamento commerciale dei dati individuali. Sono essi, infatti, la risorsa principale dei nuovi poteri privati, protagonisti di quella forma di capitalismo estrattivo proprio dell'economia delle piattaforme.

Le garanzie accordate dalla disciplina privacy sono quantomai necessarie rispetto a quello che può rappresentare, se non adeguatamente modulato, un binomio capace di accentuare le diseguaglianze: la funzionalità della tecnica al consolidamento di rapporti sociali asimmetrici e all'esercizio del potere, sganciato da un adeguato sistema di responsabilità. La sospensione degli *account social* dell'allora presidente Donald Trump simboleggia, in maniera paradigmatica, l'incidenza del potere privato delle piattaforme sulla garanzia di un diritto fondamentale quale quello alla libertà di espressione. Rispetto al rischio di rimettere alle clausole contrattuali il perimetro di esercizio delle libertà in rete, la disciplina di protezione dati sancisce alcuni principi essenziali, volti a contrastare l'abuso del potere privato delle piattaforme. Principi, questi, valorizzati e affiancati dai nuovi introdotti con il *Digital Services e il Digital Markets Act*, volti alla complessiva responsabilizzazione delle piattaforme in funzione di tutela (soprattutto) della persona.

Ma un governo antropocentrico dell'innovazione è necessario anche e soprattutto rispetto all'uso, sempre più frequente, degli algoritmi nell'ambito delle politiche pubbliche. L'esperienza recente dimostra quanto la tecnica sia ormai divenuta un ineludibile strumento di governo dell'emergenza, della complessità sociale, dei bisogni emergenti. Si tratta di uno strumento che può essere tanto più prezioso se ben governato, ma anche potenzialmente dirompente se privo dei limiti necessari.

Questo vale soprattutto (ma non solo) per il ricorso all'I.A. nell'esercizio di attività di contrasto, ove la potenza computazionale è strumentale al monopolio della violenza legittima.

Queste considerazioni sono peraltro sottese agli stringenti limiti posti dall'*Artificial Intelligence Act* al riconoscimento facciale in luoghi pubblici da parte delle autorità di contrasto, idoneo più di altri a degenerare in forme di sorveglianza di massa. Ma la disciplina di protezione dati già prevede, per l'uso dell'i.a. nelle attività di contrasto, cautele importanti che hanno indotto il Garante a ritenere inammissibile un sistema di riconoscimento facciale a fini di pubblica sicurezza, carente delle garanzie necessarie a ricondurre misure altrimenti massive nel solco della proporzionalità.

Ed è significativa, in tal senso, la moratoria sull'uso del riconoscimento

facciale approvata in sede di conversione del dl 139, che pur non precludendo astrattamente e del tutto il riconoscimento facciale da parte delle autorità di contrasto, ne subordina l'ammissibilità al parere favorevole del Garante, così da assicurarne che ogni possibile utilizzo inscriva sempre, al suo interno, le necessarie garanzie privacy.

Già oggi, infatti, la disciplina di protezione dati fornisce alcuni criteri regolativi essenziali per uno sviluppo dell'I.A. coerente con i valori dell'ordinamento europeo e dei principi costituzionali: in primo luogo il primato della persona e della sua dignità, tanto più rilevante rispetto alla svolta ingiuntiva della tecnica, sempre più demiurgica, predittiva e quindi performativa. A fronte di un'innovazione così rivoluzionaria (ma anche, potenzialmente, socialmente regressiva), da invertire quasi il rapporto strumento-agente che ne dovrebbe orientare i rapporti con l'uomo, è infatti determinante lo statuto giuridico dell'I.A. delineato dalla disciplina privacy, per porre davvero la tecnica "al servizio dell'uomo". Si pensi ai principi di non esclusività della decisione automatizzata (che vieta, salvo la sussistenza di garanzie adeguate, la delega integrale all'algoritmo di decisioni significative sull'uomo), di non discriminazione, di comprensibilità (e quindi anche sindacabilità) delle valutazioni algoritmiche, volti a contrastare il rischio di *bias*.

In questa strategia di "umanizzazione" e funzionalizzazione della tecnica alla libertà, la disciplina di protezione dati è destinata a giocare un ruolo primario, anche al di là dell'i.a.: di limite e di orizzonte di senso.

Contribuiamo quindi tutti, con il rispetto delle sue norme e la consapevolezza della sua rilevanza, a promuoverne il valore.

SANITÀ DIGITALE E PROTEZIONE DATI PERSONALI:

UN BINOMIO POSSIBILE

Prof.ssa Ginevra Cerrina Feroni

Vice Presidente dell'Autorità Garante per la protezione dei dati personali

Il binomio sanità digitale e protezione dei dati personali è possibile. Lo dimostrano i numerosi interventi del Garante, volti ad agevolare uno sviluppo equilibrato e sostenibile dei servizi sanitari offerti ai cittadini, che tengono conto della tutela dei diritti fondamentali dell'individuo alla luce del progresso sociale e degli sviluppi scientifici e tecnologici.

Esempi positivi di questo bilanciamento sono testimoniati dai sistemi informativi e dalle soluzioni tecnologiche introdotte nel contesto emergenziale per la gestione delle vaccinazioni (Piattaforma informativa per l'attuazione del piano strategico vaccini anti Sars Cov 2) e delle certificazioni verdi Covid-19 (Piattaforma Nazionale Digital Green Certificate -PNDGC), su cui l'Autorità ha reso i propri pareri (rispettivamente in date 13 gennaio 2021 e 9 giugno 2021).

Si tratta di sfide vinte, in cui si è dimostrato che un sistema informativo sanitario efficace, che consente una immediata disponibilità di informazioni corrette e aggiornate, può essere realizzato con modalità tali da assicurare la protezione dei dati e i diritti a questi connessi. Sotto questo profilo, il Garante si è dimostrato disponibile ad accompagnare le Amministrazioni impegnate nella realizzazione di importanti iniziative riorganizzative quali, ad esempio, quelle derivanti dall'attuazione dei progetti per il PNRR.

Ovviamente nel rispetto dell'indipendenza del suo ruolo di controllo sull'attuazione della normativa europea ed interna in materia di protezione dei dati personali. Una missione, non un vezzo - è utile ribadirlo - di servizio ai cittadini e salvaguardia dei loro diritti e libertà personali che potrebbero essere profondamente impattati da un uso distorto delle informazioni personali e, in special modo, proprio di quelle di carattere sanitario.

Nei pareri resi il 22 agosto 2022 sui decreti relativi al Fascicolo Sanitario Elettronico (FSE) e all'Ecosistema dei Dati Sanitari (EDS), per esempio, molti sono stati gli elementi di criticità riscontrati, la maggior parte

dei quali è derivata dal fatto che si tratta di sistemi di cui ancora non si ha contezza circa funzioni e possibili utilizzi.

Come noto, la disciplina europea sulla protezione dei dati dispone che la base giuridica del trattamento debba indicare quali dati trattare, come trattarli, chi può trattarli, indicando le misure tecniche e organizzative da seguire. In questa prospettiva i decreti sui quali si è espressa l'Autorità avrebbero dovuto dare attuazione ad un progetto chiaro, nell'ambito del quale considerare anche l'impatto *privacy* mediante una adeguata “valutazione dei rischi”. Ed invece essi sono risultati privi di tali elementi, contenendo formulazioni generali e generiche, di difficile attuazione, che avrebbero generato confusione proprio in quei settori - come quello sanitario - in cui la chiarezza delle procedure è un elemento fondamentale per la sicurezza del paziente e la responsabilità medico professionale. Consentire l'accesso a informazioni incomplete, su cui non è garantito l'aggiornamento e la costante disponibilità del dato, non è solo un elemento di criticità per la protezione dei dati, ma anche per la qualità delle cure prestate, soprattutto in emergenza.

Il decreto sull'EDS è stato, ad esempio, valutato dall'Autorità come una “scatola vuota” in cui si annunciano servizi per i medici, personalizzati sul singolo paziente, ma senza indicare quali sono questi servizi e sulla base di quali dati personali sono elaborati. Considerazioni in parte analoghe sono state espresse sul FSE: il decreto avrebbe dovuto contenere, come prescrive la legge, indicazioni concrete sull'uso del fascicolo, ma sono ancora molti gli spazi in bianco che lasciano anche tra gli operatori sanitari dubbi e incertezze. Di talché, il Garante non ha potuto pertanto far altro che rinviare al Governo i progetti chiedendo di ricevere le necessarie delucidazioni sulla mancanza di elementi essenziali che, invece, sono stati assicurati persino nei momenti più intensi della pandemia, ovvero la progettualità e la condivisione.

Merita segnalare che il tema dei dati sanitari ha assunto una dimensione sovranazionale considerato che lo scorso 3 maggio la Commissione ha pubblicato la proposta di Regolamento (del Parlamento europeo e del Consiglio) sulla legge europea sullo spazio dei dati sanitari, il c.d. EHDS - *European Health Data Space*.

In estrema sintesi, tale proposta mira a rafforzare il controllo delle

persone sui propri dati personali, conferendo alcuni nuovi diritti agli interessati rispetto ai loro dati sanitari elettronici ed a facilitare l'uso di detti dati sfruttando appieno il potenziale offerto dalla circolazione, lo scambio e il riutilizzo sicuro e protetto di essi. Ciò allo scopo sia di erogare una migliore assistenza sanitaria, anche transfrontaliera, nei confronti della persona cui i dati si riferiscono (“uso primario”), sia di supportare la definizione delle politiche sanitarie, agevolare la ricerca scientifica, favorire lo sviluppo della medicina personalizzata, produrre statistiche ufficiali, nonché l’innovazione in generale in campo sanitario, ivi compreso lo sviluppo di algoritmi, sistemi di IA e app di sanità digitale (“uso secondario”). È vietato, invece, l’uso dei dati sanitari elettronici per una serie di finalità ulteriori, quali l’adozione di decisioni pregiudizievoli per le persone o finalizzate ad escludere le persone da benefici assicurativi o ad aumentare i premi assicurativo, la pubblicità commerciale e lo sviluppo di servizi e prodotti pericolosi per le persone e le società in generale.

La proposta solleva, tuttavia, una serie di preoccupazioni di carattere generale per gli aspetti relativi alla protezione dei dati personali, messe ben in luce dal Comitato europeo per la protezione dei dati (EDPB) e dal Garante europeo della protezione dei dati (EDPS) in un articolato parere congiunto (3/2022), adottato il 12 luglio 2022, in cui si è invocata maggiore chiarezza circa gli utilizzi concretamente possibili dei dati sanitari in tale spazio di condivisione ed una migliore delimitazione e circoscrizione delle attività possibili. In particolare, l’attenzione si è concentrata sul capo IV della proposta, che mira a facilitare l’uso secondario dei dati sanitari elettronici. Il ri-utilizzo dei dati sanitari dei cittadini europei, pur potendo generare benefici per il bene pubblico, non può ritenersi privo di rischi per i diritti e le libertà delle persone con specifico riferimento alla protezione dei dati personali.

E dunque? Quali prospettive per la sanità digitale nell’ottica della protezione dei dati personali?

Partiamo dalla considerazione che *privacy* e sanità hanno un linguaggio comune. Molte delle misure richieste e ottenute dall’Autorità in questi anni hanno riguardato l’introduzione di strumenti che consentono, nel facilitare l’uso della tecnologia in sanità, di avere certezza della qualità e dell’esattezza dei dati cui hanno accesso i sanitari. Reperire informazioni sanitarie in tempo

reale è senz'altro un vantaggio nel percorso di cura di un paziente, ma la velocità di collegamento non deve essere realizzata a discapito della correttezza del dato e della certezza sull'aggiornamento dello stesso e sulla sua integrità. Questi sono elementi su cui il Garante pone molta attenzione come dimostrano i pareri sul Sistema informativo trapianti (30 marzo 2017) o sulle Dichiarazione anticipate di trattamento (29 maggio 2019).

Quando l'Autorità esprime il proprio parere su proposte normative che vanno ad innovare i sistemi informativi sanitari non si limita a verificare la robustezza delle misure informatiche, la sicurezza dei sistemi e delle piattaforme, ma valuta innanzitutto la correttezza del trattamento e la tutela dei diritti fondamentali del paziente che passano anche per un trattamento di dati esatto, aggiornato e non alterato. In questo senso a differenza di quanto pensa qualche, anche illustre, disinformato, la protezione dei dati non è ostacolo e freno all'innovazione ed al progresso tecnologico in campo sanitario, ma ne può anzi essere acceleratore e guida virtuosa.

Semmai il nodo cruciale è che i problemi della sanità digitale in Italia sono strutturali.

Atteniamoci ai dati. Il sistema FSE è formalmente attuato in tutte le Regioni completamente o quasi, ma sostanzialmente resta sulla carta. Con l'eccezione di Emilia Romagna, Lombardia e Lazio la media dei pazienti che ha prestato il proprio consenso all'alimentazione del FSE stagna attorno al 6% con ben 10 Regioni in cui il consenso non è stato prestato da nessun paziente. Quanto ai medici, escluse Sicilia, Umbria e Valle d'Aosta, nelle altre Regioni lo 0% alimenta il profilo sanitario dei pazienti ed in ben 8 Regioni nessun medico o quasi consultano il FSE.

Resta poi la questione della formazione e dell'informazione su cui c'è moltissimo da fare. Ciò che manca, per poter giovarsi di tutto questo innovativo e complesso armamentario tecnologico disponibile, è un'adeguata istruzione degli utenti a tutte le sue potenzialità ed alle modalità di utilizzo ed accesso.

Una riorganizzazione logistica della sanità pubblica, un rinnovamento delle sue infrastrutture informatiche e di rete, la previsione di un'interoperabilità dei sistemi, nonché una profonda opera di formazione del

personale a tutti i livelli, appaiono come elementi imprescindibili al fine di favorire un corretto posizionamento dei tasselli che compongono la medicina digitale e del potenziale che questo strumento può esprimere ma che, invece, troppo spesso rimangono schiacciati dai vincoli infrastrutturali e di bilancio esistenti.¹

L'occasione per mitigare, in parte, i ritardi del Paese relativamente alla digitalizzazione e all'utilizzo dei sistemi informativi e, conseguentemente, di ipotizzare una riforma più strutturale della Sanità sia pubblica che privata con un forte impulso alla telemedicina, dovrà essere il PNRR in cui oltre 40 miliardi sono previsti per la digitalizzazione e una buona parte dei 18 miliardi della sanità saranno disponibili per le cure a casa e ai processi ad essa collegati.

Ricordiamo però che quando si parla di sanità digitale la finalità di cura non cambia. A cambiare invece, più o meno direttamente e da angoli visuali diversi, è tutto ciò che vi è intorno: le modalità con cui la prestazione medica viene erogata, il rapporto tra chi fornisce e chi beneficia della stessa e l'organizzazione ed erogazione dei servizi correlati, con la conseguenza di rimarcare con forza la felice espressione per cui prendersi cura del paziente significa prendersi cura anche dei suoi dati, non più soltanto del corpo fisico come Ippocrate e Galeno, ma anche di quello digitale.

1) Cfr. R. Balduzzi, *Alcune conclusioni: la difficile equivalenza dei sottosistemi sanitari regionali*, in E. Catelani, G. Cerrina Feroni, M.C. Grisolia, *Diritto alla salute tra uniformità e differenziazione: modelli di organizzazione sanitaria a confronto*, Giappichelli, Torino 2011, pp. 149 ss.

METAVERSO, PRIVACY E FUTURO

Prof. Guido Scorza

Componente dell'Autorità garante per la protezione dei dati personali

Nell'interrogarci sul Metaverso, la privacy e il futuro credo sia indispensabile volgere, prima di tutto, lo sguardo al passato, alla storia di Internet e degli esercizi di governo del fenomeno tecnologico che, sin qui, ha cambiato più di ogni altro le nostre vita, la società in cui viviamo, i mercati, la politica e il mondo intero.

Internet è nata nella dimensione pubblica, nell'ambito di un progetto militare, per la precisione. Si chiamava, come molti di noi ricordano, Arpanet e sarebbe dovuta servire a garantire la comunicazione anche in caso di un attacco bellico.

È poi approdata al mondo dell'università e della ricerca e, solo successivamente, è stata letteralmente privatizzata e trasformata, essenzialmente, in uno strumento di mercato nel quale i poteri privati erodono in maniera sempre più penetrante i poteri pubblici, appropriandosi di ruoli, competenze e funzioni che dovrebbero essere appannaggio esclusivo di questi ultimi.

Il Metaverso non sappiamo cosa sarà e, anzi, in effetti, allo stato non sappiamo neppure se sarà necessario parlarne al singolare o al plurale.

C'è, tuttavia, una certezza nell'indagare sulle sue origini e ce la offre Google Trends, il servizio di Google che monitora le interrogazioni degli utenti sul motore di ricerca: sostanzialmente nessuno, in tutto il mondo, ha interrogato il motore di ricerca utilizzando l'espressione "metaverso", fino a quando il 28 ottobre del 2021, Mark Zuckerberg, fondatore e patron di Facebook, non ha annunciato che la sua azienda avrebbe cambiato nome in Meta perché il mondo stava facendo rotta verso il "Metaverso".

Da quel momento, il grafico delle ricerche su Google utilizzando la parola "metaverso", suggerisce che centinaia di milioni di persone in tutto il mondo hanno iniziato a interessarsi di un futuro, battezzato Metaverso dal numero uno di una società che aveva appena scelto di chiamarsi Meta.

Se c'è, dunque, una ragionevole certezza rispetto al Metaverso che verrà

è che sarà un luogo-non luogo più privato di Internet sin dai suoi primi istanti di vita.

Insomma, a differenza di quanto originariamente accadeva per Internet, per accedere al Metaverso - o, se ce ne saranno diversi ai metaversi - dovremo necessariamente accettare delle condizioni generali di contratto che stabiliranno, proprio come accade oggi quando iniziamo a usare un social network o un altro servizio digitale, cosa potremo fare e non fare nel metaverso o nei metaversi.

Il metaverso sarà, dunque, un enorme giardino privato il cui proprietario detterà le regole che miliardi di utenti di quel giardino dovranno rispettare e le regole in questione, a differenza delle leggi emanate da Governi e Parlamenti, saranno regole insuscettibili di essere violate giacché a presidiarne il rispetto da parte di tutti ci saranno algoritmi e software che, semplicemente, impediranno ogni violazione futura.

Si tratta di una prima considerazione della quale non si può non tenere conto nell'affrontare le questioni giuridiche connesse alla vita nel metaverso perché, nella sostanza, suggerisce che lo spazio di azione per i poteri pubblici sarà ancora più limitato di quanto sia oggi nella dimensione digitale e che quello per i poteri privati sarà, sostanzialmente, illimitato.

Saremo, insomma, liberi per contratto o, magari peggio, non saremo liberi per contratto perché, appunto, il contratto in questione comprimerà in maniera significativa i nostri diritti e le nostre libertà.

Un bel problema da governare se si vuole scongiurare il rischio che quello che potrebbe essere destinato a divenire, in un universo temporale modesto, l'ambito naturale di vita dell'uomo sia pressoché completamente sottratto alle regole, al governo e alla giustizia che hanno sin qui plasmato le nostre democrazie.

E, il problema nel problema, è che, verosimilmente, nessuno di noi conoscerà effettivamente le regole da rispettare per vivere nel metaverso perché, proprio come accade oggi con i termini d'uso e le informative sulla privacy, tutti accetteremo le condizioni contrattuali in questione senza leggere assolutamente nulla.

Se si vuole scongiurare il rischio di un'ecatombe dei diritti, quindi, è,

innanzitutto, indispensabile identificare, almeno, nuove e più efficaci forme di accettazione dei contratti nella dimensione digitale che siano capaci di garantire un'effettiva consapevolezza da parte di chi decide di aderire a un contratto per l'accesso al metaverso.

Certo non basterà se, come è verosimile, essere nel metaverso sarà per la più parte di noi un'esigenza pressoché irrinunciabile un po' come accade oggi per l'utilizzo di molti servizi digitali e se ci sarà un solo metaverso o un numero esiguo di metaversi nei quali "valga la pena" essere.

Nella sostanza, infatti, rischiamo di non avere una reale libertà di scelta da esercitare.

Ma alla ricerca di alcune certezze attorno alle quali costruire una prima riflessione su privacy, metaverso e futuro, sembra importante anche fermarsi a riflettere su un'altra questione: il metaverso - qualunque cosa sia o sarà - rappresenterà - e, in effetti, già rappresenta - un'esperienza enormemente più immersiva rispetto all'Internet di oggi nella quale, pure, già viviamo discretamente immersi.

Questa immersione, nel caso del metaverso, sarà essenzialmente dovuta alla circostanza che il metaverso sarà tridimensionale e multisensoriale.

Si tratta di alcuni attributi caratteristici della dimensione della quale ci stiamo occupando che la renderanno preziosissima in una molteplicità di ambiti professionali e, più in generale, della vita dell'uomo: penso alla medicina, alla formazione e educazione, agli interventi di manutenzione specializzata a distanza, alla ricerca, alla sicurezza e a decine di altre possibili forme di impiego.

Ma tridimensionalità e multisensorialità hanno un presupposto difficilmente revocabile in dubbio: per vivere qualsiasi genere di esperienza nel metaverso sarà indispensabile condividere una quantità di dati personali significativamente superiore a quella che oggi condividiamo per esistere nella dimensione digitale.

E, quindi, questo significa che la disciplina sulla protezione dei dati personali, nella dimensione del metaverso prossimo venturo, sarà ancora più centrale e rilevante di quanto sia oggi.

Già oggi, in fondo, nella dimensione digitale, siamo i nostri dati perché

sono i nostri dati che ci rappresentano, ci danno forma, ci fanno conoscere, ci raccontano e sono alla base di ogni nostra relazione nella dimensione personale e in quella professionale, in quella commerciale e in quella politica.

E tutto questo sarà ancora più vero negli anni che verranno nel metaverso prossimo venturo.

Che fare davanti a queste certezze nel tentativo e con la speranza di governare il fenomeno che ci attende? Difficile rispondere a questa domanda mentre i contorni di quel fenomeno sono ancora evanescenti, sfumati, poco nitidi e in continua evoluzione.

Ma alcune ipotesi, probabilmente, si possono già azzardare.

La prima è che è indispensabile che i poteri pubblici si riappropriino progressivamente almeno di parte dei ruoli, delle competenze e delle funzioni che hanno ceduto ai soggetti privati nel governo di Internet perché se questo non avviene ci si ritroverà, inesorabilmente, tutti ospiti di una più o meno lunga serie di giardini privati nei quali le regole delle relazioni personali, professionali, economiche e politiche le deteranno i mercati nel nome del profitto.

È uno scenario a tinte fosche per i diritti e per l'umanità.

La seconda è che occorre ripensare interi sistemi di regolamentazione - e tra questi quello in materia di protezione dei dati personali - nell'ambito dei quali si è, sin qui, pensato di riequilibrare le posizioni di forza, tra soggetti deboli e soggetti forti, imponendo a questi ultimi una serie più o meno stringente di obblighi di informazione.

Questi obblighi non funzionano più o, almeno, non funzionano per come sono attualmente declinati, in una dimensione più formale che sostanziale: nessuno legge più i termini d'uso dei servizi e delle piattaforme digitali né le informative sulla privacy.

Quello che sta accadendo, quindi, è che garanzie introdotte nel nostro ordinamento per riequilibrare le posizioni di forza stanno producendo l'effetto contrario, stanno rendendo più forti i forti e più deboli i deboli.

I primi, infatti, possono difendersi davanti alle contestazioni dei secondi sostenendo di aver fornito tutte le informazioni necessarie a norma di legge e i secondi non possono contestare nulla di più avendo, in qualche modo,

scelto di non leggere ma di procedere alla scelta loro proposta che si sia trattato di aderire a un contratto o di fornire questo o quel consenso al trattamento dei loro dati personali.

Uno strumento di perequazione è, insomma, diventato uno strumento di sperequazione.

E se non si inverte la rotta il destino è segnato: nel metaverso ancora di più di quanto già non accada saremo liberi di dire e di fare ciò che ci sarà concesso dire e fare non solo sulla base di regole scritte in uno studio legale e non in Parlamento ma di regole che neppure conosciamo.

E c'è poi, tra quelle che è già possibile intravedere all'orizzonte, un'ultima questione non di poco conto: essere nel metaverso significherà scambiare dati contro servizi, condividere tessere del mosaico della nostra identità personale con altri utenti e con i gestori delle piattaforme e dei servizi, significherà, insomma, accettare definitivamente l'idea - che non abbiamo ancora accettato - secondo la quale i dati, inclusi quelli personali, sono beni giuridico-economici eguali a ogni altro, eguali al denaro, all'oro, all'argento o al petrolio.

Ma sappiamo - o, almeno, dovremmo sapere - che non è così perché i dati personali sono anche e, anzi, soprattutto tessere della nostra identità personale e, in questo senso, frammenti di un diritto fondamentale che è garanzia di altri diritti e libertà.

Che fare, allora?

Troppò presto per dirlo senza il rischio di sbagliare ma, probabilmente, se può discutersi della circostanza che taluni dati personali comuni possano - o, forse, persino debbano - circolare liberamente anche nelle dinamiche di mercato, questo non può essere vero per i dati particolari, per quelli relativi alla nostra salute, alle nostre abitudini sessuali, alla nostra fede religiosa, al nostro orientamento politico, per i dati biometrici, quelli genetici o quelli giudiziari.

Questi dati vanno sottratti con determinazione al mercato.

E, allo stesso modo, si deve impedire che i più fragili, a cominciare dai bambini, dispongano inconsapevolmente dei loro dati personali nella dimensione del mercato.

Niente di tutto ciò, naturalmente, basterà a rendere l'immersione del mondo nel metaverso un'esperienza scevra da quei rischi che rappresentano l'altra faccia di qualsiasi innovazione ma si tratta di accortezze che potrebbero, almeno, valere a abbattere i rischi che fanno da necessario contraltare alle opportunità.

Ma c'è un aspetto che è più importante di ogni altro: l'educazione di massa al metaverso.

È un fatto indispensabile, una precondizione essenziale perché i benefici collettivi siano superiori ai malefici e si tratta di qualcosa che è mancata davanti alla rivoluzione di Internet che ha dato - e sta dando - al mondo tantissimo ma in maniera disomogenea: tanto di più a pochi - i più edicati al digitale - e molto di meno a molti, i meno educati al digitale.

E, soprattutto, sta lasciando tanti completamente indietro, li sta rendendo cittadini di serie "b", li sta relegando al ruolo di comprimari in una società nella quale dovrebbero, naturalmente, essere protagonisti come tutti gli altri.

Questo non possiamo lasciare che accada ancora, che accada anche nel metaverso.

E in questo senso serve un'autentica dichiarazione di guerra all'analfabetismo digitale analoga per dimensioni, determinazione, convinzione e obiettivi a quella che, anche in Italia, si dichiarò nel secondo dopoguerra all'analfabetismo letterario: leggi speciali, risorse economiche adeguate, decine di migliaia di corsi messi a disposizione delle persone comune, i media, vecchi e nuovi, coinvolti per seminare cultura.

Se non accetteremo questa idea, la società che ci aspetta e le sue opportunità, ancora una volta, non saranno per tutti ma solo per qualcuno e il futuro sarà meno democratico del passato che ci butteremo alle spalle.

QUARTA SESSIONE



L'ERA DELLA CYBERWAR



- INTERVENTO DEL Sen. Adolfo Urso
- CYBER-RESILIENCE: L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE
 - Dott.ssa Annunziata Ciardi**
- LA DIFESA E IL CYBERSPACE
 - Gen. C.A. Carmine Masiello**
- LE SFIDE GLOBALI DEL CYBERCRIME, COME DIFENDERSI E IL RUOLO DELLA GUARDIA DI FINANZA
 - Col. Marco Menegazzo**

QUARTA SESSIONE* L'ERA DELLA CYBERWAR

Sen. Adolfo Urso

Presidente del COPASIR

Ringrazio gli amici dell'Autorità che mi hanno invitato in questo meeting, Autorità che è stata auditata dal nostro Comitato parlamentare per la Sicurezza della Repubblica proprio in merito a questioni inerenti la cybersicurezza.

Se per data di inizio del mio incarico consideriamo l'inizio della legislatura, quando entrai nel Copasir come vicepresidente, allora il presidente era l'attuale ministro Guerini, perché il Partito democratico era all'opposizione, possiamo dire che in quel momento ci rendemmo conto del fatto che l'Italia era molto indietro rispetto ad altri Paesi e proprio per questo Guerini decise e, il Comitato condivise, di fare la prima indagine conoscitiva della legislatura che si concluse con una Relazione al Parlamento sulla sicurezza cybernetica e la protezione informatica, che è stata la prima Relazione del Comitato al Parlamento in questa legislatura.

In quella Relazione, individuammo la questione, i ritardi del nostro Paese e chiedemmo in maniera esplicita, per esempio, l'estensione della Golden power al settore delle telecomunicazioni del 5G, cosa che avvenne in breve tempo, così come chiedevamo l'inibizione alla tecnologia cinese della parte centrale del 5G, cosa che ancora non è avvenuta. Nella stessa Relazione chiedevamo anche che si colmasse il ritardo rispetto agli altri Paesi europei, soprattutto rispetto a Francia e Germania, con la creazione di un'Agenzia o di un Istituto; poi fu scelta la formula dell'Agenzia per la cyber sicurezza nazionale, cosa che è avvenuta purtroppo con un po' di ritardo.

Per cui quando fui nominato al Copasir, il quadro era particolarmente preoccupante. Nel corso di questi anni grazie all'impulso del Comitato e

* La sessione è stata moderata dal dott. **Fausto Carioti**, Vice Direttore di Libero

a quella Relazione iniziale, molte lacune sono state colmate e l’Italia si è attrezzata sempre più e meglio.

Se per data di inizio mettiamo la data dell’incarico del sottoscritto alla presidenza del Copasir il 9 giugno 2021, anche in quel caso c’è una coincidenza significativa. E ricordo che il primo atto che mi arrivò, ancora eravamo in seggio elettorale, fu il decreto per l’Agenzia della cyber sicurezza nazionale. Il pre-Consiglio l’aveva approvato e il giorno dopo toccava al Consiglio dei Ministri, ci accorgemmo in quel momento che non vi era una Autorità di controllo; il testo approvato nel pre-Consiglio non prevedeva un’Autorità di controllo parlamentare. Allora ci siamo confrontati con il Governo, abbiamo convocato il sottosegretario alla Intelligence Gabrielli, giunto in Comitato prima del Consiglio dei Ministri, e ci siamo confrontati su quale fosse la modalità migliore.

Il testo poi approvato dal Consiglio dei Ministri, a differenza di quello approvato in pre-Consiglio, individuava proprio nel Copasir il Comitato di controllo della nascente Agenzia, così che essa oggi è sottoposta al nostro controllo, così come lo sono le Agenzie di Intelligence. Questo perché il Copasir, istituito con legge di iniziativa parlamentare approvata all’unanimità nel 2007 , a differenza del precedente organismo che era il COPACO, non si occupa soltanto del controllo sull’operatività dei Servizi segreti e sull’operatività del Governo nel campo dell’Intelligence, ma come dice la sua stessa denominazione, si occupa del controllo dell’attività dell’Intelligence, del Governo nell’operato dell’Intelligence, ma anche dell’operato del Governo in tutto il campo della Sicurezza nazionale. Per questo fin dall’inizio la Cyber è stata considerata elemento fondamentale della Sicurezza nazionale e l’Agenzia per la Sicurezza nazionale pur non essendo un’Agenzia di Intelligence ma un’Agenzia laica, che opera nel campo dell’Amministrazione pubblica, è stata sottoposta al nostro controllo. Perché appunto, il Comitato sovrintende in senso vasto, alla Sicurezza nazionale.

Abbiamo udito più volte il direttore Baldoni e anche il vicedirettore Ciardi per competenze che ricadono nei loro rispettivi ambiti, così come il direttore della Polizia postale.

L’analisi riguarda il contesto globale in cui l’Italia agisce per tutelare

la propria Sicurezza nazionale, la privacy dei propri cittadini dalle incursioni hacker, che non sono soltanto le incursioni di una guerra, ma anche le incursioni di un'attività criminale, perché possono essere messi in essere a fini estorsivi, a fini terroristici, ma anche configurate come aggressioni statuali.

La teoria che la Cyber potesse essere utilizzata al fine di potenza statuale o di aggressione statuale, è una teoria che è stata elaborata ed è stata evocata la prima volta dall'attuale Capo di Stato Maggiore della Difesa russa Gerasimov, quando nel 2013 elaborò una dottrina militare, pubblicata nelle riviste specializzate, sostanzialmente configurando una guerra permanente con tutti i mezzi, per affermare la potenza russa rispetto all'Occidente.

In questa guerra permanente Gerasimov cita non a caso l'*Information War*, cioè una guerra che tende sostanzialmente a condizionare l'opinione pubblica utilizzando anche la cyber. Esattamente nel 2013, data non causale visto che nel 2014 si verifica la prima invasione russa che porta l'annessione della Crimea e la creazione delle Repubbliche cosiddette indipendentistiche. Nell'elaborare questa teoria che poi diventa anche pratica, essa ha il fine sostanziale di prendere l'assoluto controllo della Rete interna. Nel 2013 quando Gerasimov elabora la dottrina militare della guerra permanente o della guerra ibrida, internet era considerato il veicolo della libertà, e anche su l'internet russo, la gran parte delle notizie si riferivano al desiderio di libertà: i cittadini russi pubblicavano notizie che parlavano delle loro aspirazioni, di affermare il loro desiderio di libertà; ciò accadeva anche se in misura minore, in Cina.

Ebbene, i regimi si resero conto di quanto fosse pericoloso per loro l'espansione del diritto di libertà che la Rete consentiva ai singoli cittadini che utilizzavano i vari strumenti della Rete. Per questo in Russia come in Cina con sistemi diversi, si è preso innanzitutto il controllo totale della propria Rete e oggi in Russia, la quasi totalità delle notizie che passa sulla Rete sono notizie che evocano la narrazione del Regime, cioè la velina che viene costruita, elaborata al Cremlino e propagata sulla Rete interna, ma poi grazie ai troll, alle fake news, ai falsi profili social, anche divulgata all'esterno.

Questo è accaduto contemporaneamente sia in Russia che in Cina. Basta guardare a quello che dice la legge sulla Sicurezza nazionale per quanto

riguarda il controllo dell'Informazione che viene veicolata su internet; ci vuole qualcuno che certifichi chi può pubblicare e cosa si può pubblicare: totale controllo dell'opinione pubblica interna, quest'ultima anche per reprimere ogni forma di dissenso. Hanno costruito una macchina offensiva per penetrare nelle democrazie occidentali, condizionarle ed inquinare, per avvelenare i pozzi della democrazia, che sono il confronto democratico, la libertà di informazione, il pluralismo e in qualche modo sottomettere le democrazie occidentali.

Ci sono anche altri strumenti, come gli attacchi hacker, il blocco delle linee elettriche in alcuni Stati americani, magari anche a fini estorsivi, ma vi può essere anche una minaccia statuale; se viene bloccata la rete idrica in Israele, piuttosto che negli Stati Uniti, sicuramente in qualche misura si reca un danno superiore ad un attacco missilistico. Proprio perché gli attacchi hacker alcune volte sono camuffati da attacchi estorsivi da parte di criminalità "comune"; ma si tratta di attacchi statuali. Per questo l'Alleanza Atlantica, ha inserito la cyber come dominio bellico.

Quando studiamo la storia, ci rendiamo conto che qualche millennio fa i domini bellici erano due: la terra ed il mare. Nel tempo, e forse è stata un'invenzione in qualche misura italiana, è stato inserito il cielo come uno dei domini bellici. Dopo questi tre domini è stato inserito lo spazio, e poi è stata inserita la cyber. Quest'ultimo è il più pervasivo, perché attraverso la cyber, s'invasano gli altri domini che della cyber hanno un assoluto bisogno.

Questo significa che un attacco su vasta scala ad uno dei Paesi dell'Alleanza Atlantica, può essere configurato come un attacco di altra natura sulla base del quale attivare il cd "articolo quinto".

Per questo credo che l'Alleanza Atlantica e anche noi come Paese, dobbiamo attrezzarci in maniera ancora più significativa non soltanto per prevenire con l'Intelligence, tutelarci con le Agenzie e altre forme di difesa che abbiamo, ma anche per capire come di fronte ad un attacco cyber che fosse configurato come un attacco statuale si possa reagire, secondo le normative che dobbiamo condividere con gli altri Paesi dell'Alleanza Atlantica.

Questa è la questione su cui tutti dobbiamo in qualche misura adeguarci, perché a differenza degli altri domini, quello della cyber riguarda

ciascuno di noi, il nemico può entrare dal mio cellulare, attraverso il pc. Ciascun cittadino deve assumere quella consapevolezza e attrezzare la propria difesa quotidiana, casalinga in modo da tutelare lo spazio comune di noi tutti.

Tutti noi ci auguriamo che la guerra in Ucraina finisca e che Putin fermi la distruzione che è in atto, ma dobbiamo sapere che se anche ciò accadesse, la guerra permanente iniziata nel 2013 non finirà il giorno dopo, continuerà sotto forma diversa o forse aumenterà con intensità sugli altri domini. Prepariamoci anche a questo.

CYBER-RESILIENCE: L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Dott.ssa Annunziata Ciardi

Vice Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale

Noi paghiamo un prezzo per una rivoluzione che forse non ha eguali nella storia.

Questa è stata una rivoluzione non solo tecnologica, ovviamente, e neanche solo culturale, in qualche modo è stata una rivoluzione antropologica che ci ha messi in un nuovo rapporto con l'esistente, con il reale.

La dimensione digitale “ci coinvolge tutti e in tutto”. Questa è la caratteristica fondamentale di questo spazio cyber che è entrato in ogni interstizio della nostra vita. Noi ci muoviamo ormai costantemente su una trama digitale anche quando non ne siamo perfettamente consapevoli, anzi, anche quando crediamo di non essere in qualche modo esposti.

La dimensione digitale è una dimensione della quale sicuramente oggi nessun paese che voglia competere sulla scena internazionale economicamente, socialmente, culturalmente può fare a meno.

La transizione digitale è una necessità fondamentale per un paese che voglia correre, ma tutto questo ha anche un rovescio della medaglia: il profilo della sicurezza. È un profilo molto importante e nella dimensione digitale è un profilo estremamente delicato.

La società digitale è una società decisamente performante ma molto vulnerabile: ha tantissimi aspetti di delicatezza e, peraltro, in questo ultimo periodo, sono stati assolutamente accentuati dai due cigni neri che hanno colpito il globo: prima la pandemia e poi la guerra.

Quando c'è stato, purtroppo, il dramma della pandemia io ero in un'altra vita professionale e combattevo il cybercrime con la Polizia Postale. Ho avuto modo di vedere in diretta la crescita esponenziale tutti i reati cyber, mentre di converso i reati tradizionali subivano una contrazione importantissima. Si erano quasi azzerate le rapine, soprattutto nei tempi del lockdown duro, così come gli scippi ecc..., mentre i reati cyber erano tutti schizzati con percentuali da brivido.

Poi la guerra, che ha fatto deflagrare tutta una serie di problemi, perché oggi la guerra si combatte anche nel dominio cyber.

A tutto questo aggiungiamo anche che la situazione del nostro paese non era tra le più rosee.

L'Agenzia della Cybersicurezza Nazionale da giugno in poi sta accelerando tantissimo i suoi passi ma è evidente che un problema strutturale e complesso come il problema della digitalizzazione e il conseguente problema di sicurezza sono problemi che non possono essere risolti nello spazio di un paio di mesi.

Paesi ben più attrezzati del nostro, sotto il profilo della sicurezza digitale, si sono scontrati ultimamente con tantissimi problemi. Pensiamo agli Stati Uniti con l'oleodotto Pipeline o Israele colpito da attacchi DDos verso i suoi principali siti e parliamo di due paesi per i quali la sicurezza digitale è stata coltivata in modo assolutamente preferenziale e sicuramente in modo molto anticipato rispetto al nostro paese.

L'Agenzia è nata a giugno del 2021 ed è diventata operativa con i primi due dipendenti a settembre. Parliamo di pochissimi mesi. Attualmente siamo un centinaio di persone e dovremmo per norma diventare 300 entro il prossimo anno e 800 entro il quadriennio. È prevista, quindi, una progressione accelerata proprio per curare la resilienza del paese.

Ovviamente l'agenzia non nasce in un deserto di iniziative, mancava però un tassello fondamentale: quello della resilienza.

La resilienza cybernetica deve assicurare che un paese, anche in caso di attacco, non solo possa lavorare per prevenirlo, per aumentare le difese delle infrastrutture critiche, cioè quelle che erogano servizi essenziali per il paese, ma anche possa reagire in modo rapido una volta che è stato colpito.

L'agenzia nasce per contrastare tutte queste minacce che sono più diffuse, più diversificate, più sofisticate attraverso tutta una serie di elementi. In Italia, secondo i dati che abbiamo dalle forze dell'ordine, nell'ultimo anno gli attacchi cyber significativi, quindi non tutti gli attacchi cyber, ma solo quelli diretti verso infrastrutture critiche, quindi verso i servizi essenziali del nostro paese, sono aumentati del 35%. Parliamo di percentuali di aumento enormi perché la tecnologia evolve rapidamente.

Bisogna in qualche modo assolutamente contemperare la transizione tecnologica e la transizione digitale in una crescita sostenibile del paese digitale. Dobbiamo dotarci di capacità, istituzioni, risorse e competenze utili ad aumentare la resilienza del paese. Mi è stato domandato se fosse adeguata la dotazione di soldati del Cyber che abbiamo nel paese. Rispondo senza mezzi termini: “No!”. Nel nostro paese, un po' in tutto il globo in effetti, le professionalità non ci sono.

Uno dei compiti dell'Agenzia è stimolare la crescita di professionalità utili a contrastare la minaccia cyber, la minaccia rivolta alle società digitali. È un tipo di preparazione che non è stata coltivata a sufficienza. Quelle poche risorse estremamente pregiate che avevamo spesso hanno scelto in passato la strada dell'estero. Anche per questo uno dei compiti dell'Agenzia è quello di stimolare la crescita di queste professionalità, di stimolare i rapporti con le università affinché attuino un circuito virtuoso perché la preparazione del nostro paese possa attingere a professionalità utili in questo campo. D'altra parte l'Agenzia ha poi tutta una serie di compiti che senza figure professionali non potrebbero essere attuati.

Da una parte la prevenzione e la mitigazione di attacchi già avvenuti, dall'altra l'indipendenza tecnologica.

Quando noi parliamo di sicurezza non possiamo tacere di un problema di dipendenza tecnologica totale che non solo il nostro paese ma io direi tutto il continente europeo soffre. Noi siamo dipendenti, pur essendo dei grandi utilizzatori di tecnologia, da Paesi che sono molto più avanti di noi in questo campo.

L'indipendenza tecnologica è non solo un volano di sviluppo economico quanto mai importante in questo momento, ma anche un fattore di sicurezza. È indubbio che avere una tecnologia propria ci mette al riparo, ci fa gestire meglio determinati aspetti. L'Agenzia deve in qualche modo stimolare la crescita di una indipendenza tecnologica Europea prima, in collaborazione con gli altri paesi europei, ed in ultima istanza anche quella italiana.

In più la crescita di consapevolezza nel paese è importante. La “cura della sicurezza” deve essere domestica, del singolo, una consapevolezza che deve investire ciascuno di noi. Un'azienda, una regione può anche investire molto

per sicurezza ma se poi un dipendente porta a casa la sua postazione aziendale e viola delle regole fondamentali di cybersicurezza è evidente che mette in serio pericolo tutte quelle misure che l'azienda faticosamente ha cercato di tirar su. Quindi la consapevolezza deve investire ciascuno di noi e che comprensibilmente tutti noi fatichiamo ad avere proprio perché la rivoluzione digitale è stata velocissima. Basti pensare che nel 2009 soltanto il 15% degli italiani avevano uno smartphone, il telefono veniva utilizzato solo per telefonare. Oggi, a distanza tutto sommato di un pugno di anni, oltre 129% degli italiani ha un dispositivo mobile a disposizione potenzialmente connesso 24 ore su 24.

Questo dà la misura di quanto la tecnologia e la digitalizzazione hanno avuto una crescita convulsa ed è ovvio che si fatichi a metabolizzare un cambiamento di questo tipo, si fatichi a metabolizzare l'importanza dell'adozione di modelli di sicurezza che sono ormai fondamentali nella nostra vita e nella tutela dei nostri dati che sono in rete e che sono la nostra vita in rete. La sicurezza digitale, la cybersicurezza, oggi è sempre di più la sicurezza a tutto tondo delle nostre vite.

LA DIFESA E IL CYBERSPACE
Gen. C.A. Carmine Masiello
Sottocapo di Stato Maggiore della Difesa

Domanda del moderatore dott. Fausto Carioti: Allora parliamo di soldati e il caso vuole che qua accanto a me ci sia il generale Masiello, Sotto Capo di Stato Maggiore della Difesa. Generale.

Buonasera, anche a Lei chiedo di illustrarci intanto la Sua Istituzione quale parte, quale ruolo svolge all'interno della cyber guerra? E poi le chiedo cosa è cambiato dal 24 febbraio?

Gen. C.A. Masiello: Grazie, saluto tutti, saluto l'Autorità. Innanzitutto un grazie per aver invitato la Difesa a questo consesso, è un segno di attenzione non soltanto per il mondo che rappresenta, ma anche il segno che si è capito che la Difesa ha una parte attiva in questo mondo cyber , ed è uno degli attori, lasciatemi dire, fondamentale e questo, e mi riallaccio subito alla prima domanda che mi ha posto quando mi ha chiesto cosa avevo trovato nel mio lavoro: allora io mi occupo di cyber in senso lato, più o meno da 5- 6 anni, quando sono stato assegnato a Palazzo Chigi quale consigliere militare del Presidente del Consiglio, e a quel tempo presiedevo il nucleo di sicurezza cibernetica, quindi è stato il mio primo contatto con il mondo cyber. E devo dire, e riecheggio un po' le parole del Presidente Urso, che sin da quei tempi era evidente che la situazione nel nostro paese non era ottimale e che andavano prese delle misure, cose che poi sono state fatte nel tempo con la creazione della CN e del perimetro eccetera.

Adesso io mi occupo allo Stato Maggiore della Difesa, attraverso le unità alle mie dipendenze, della definizione della policy cyber della difesa e dello sviluppo delle nuove capacità in ambito difesa. La difesa, però non è nuova al fenomeno cyber, per noi il problema della sicurezza delle reti, diciamo un po' endemico, fa parte della nostra formazione.

Noi siamo un po' fissati, cresciamo con questo problema della sicurezza e quindi siamo diciamo avvantaggiati rispetto al resto della Comunità. In secondo luogo siamo abituati a parlare con i nostri alleati, siamo abituati a

guardare a quello che succede negli altri paesi, in maniera veramente direi quasi esagerata e, questo non soltanto nell'ambito delle alleanze, ma guardiamo un po' in tutto il mondo. Il terzo punto, lasciatemelo dire, che noi la dottrina Gerasimov l'abbiamo studiata: per noi era importante capire cosa stava succedendo dall'altra parte della barricata, se così si può usare questo termine.

Quindi, a fronte di questa situazione abbiamo ristrutturato tutta la nostra governance, e questo in linea con quello che stava succedendo nel resto del paese; quindi abbiamo essenzialmente due leve, una leva che è quella che ricade sotto la mia competenza e poi una leva invece operativa che è quella di condurre effettivamente le operazioni cibernetiche, quindi questo è un po' in sintesi quello che fa la difesa. Io vorrei sottolineare qualche punto. Il primo punto è stato già trattato e lo dico subito è la condivisione, la sinergia, dico io.

La tematica cyber non può essere affrontata in maniera separata dai singoli attori in questo paese. Bisogna fare uno sforzo che è difficile in Italia, uno sforzo per guardare al problema in maniera coordinata, quindi ci vuole sinergia nell'attività e poi soprattutto ci vuole condivisione perché nel mondo cibernetico c'è poca voglia di condividere.

C'è poca voglia di condividere perché non si vuole far vedere che si è stati penetrati o far vedere che si è sbagliato e non si vuol far vedere che magari si ha qualcosa in più degli altri. E questo fa parte delle regole della concorrenza, ma questa è la cosa peggiore che si può fare, perché il fatto di non condividere con gli altri le problematiche che si sono subite, porta inevitabilmente o può portare altri a soffrire dello stesso problema, e quindi bisogna fare uno sforzo in questo senso, cosa che non è sempre agevole perché è un problema culturale.

Per quanto riguarda il 24 Febbraio, perché questo forse è il punto che più attiene al lavoro che facciamo: il lavoro operativo, ha segnato sicuramente uno spartiacque, la prima cosa che mi sento di dire è che il 24 Febbraio è iniziato il primo conflitto simmetrico della era digitale, nel senso che noi abbiamo vissuto gli ultimi vent'anni, e parlo di ufficiali della mia generazione e di quelle più recenti, abbiamo vissuto per vent'anni in combattimento in Iraq, Afghanistan, per parlare dei principali teatri, ma si è trattato sempre di conflitti asimmetrici, cioè fra unità che avevano capacità tecnologiche totalmente diverse.

Infatti io sono stato in Afghanistan e devo dire che la problematica cyber era veramente relativa. Era poco sentita rispetto a quello che è successo in Ucraina.

Questo è il primo fattore che ci deve far riflettere: da questo momento la parte cibernetica è entrata nella guerra in senso lato perché di guerra si parla e perché è un conflitto cibernetico.

Carioti: Scusi che intende per simmetrico?

Gen. C.A. Masiello: simmetrico, vuol dire che hanno le stesse capacità. Sono due avversari che si muovono allo stesso livello di capacità, noi e i Russi siamo e sarebbe un conflitto simmetrico. Noi e i talebani: è un conflitto asimmetrico, quindi per semplificare. E quindi stavo dicendo: nell'Afghanistan non si parlava di questo. E dicevo quindi: conflitto cibernetico, perché di vero e proprio conflitto si tratta, dobbiamo dare alle parole il loro senso di un conflitto quotidiano.

Ogni giorno nel mondo ci sono milioni di attacchi cyber e non è un segreto, tutti tenuti per la maggior parte sotto soglia, ovviamente per evitare che vi sia la risposta dell'aggressivo. Il cyber poi, come è già stato detto dal Presidente Urso, fa parte oramai dei domini a tutti gli effetti, quindi abbiamo visto nel conflitto del 24 Febbraio come il dominio cibernetico è stato integrato nelle operazioni militari, quindi gli attacchi cibernetici si muovevano parallelamente agli attacchi convenzionali.

Quindi mentre si muovono i carri armati e aerei bombardavano, c'erano attacchi cyber che venivano condotti contro l'Ucraina in particolare, e non solo. E parliamo chiaramente di centinaia di attacchi. E questo è stato sicuramente un grosso ammaestramento per noi, quindi sapevamo come poteva essere. Sapevamo in teoria quello che poteva succedere, poi l'abbiamo visto praticamente. Un'altra cosa molto interessante è la problematica dello spazio, perché lo spazio come nuovo dominio, è stato accennato, è strettamente legato alla cyber. Il non garantire la sicurezza cibernetica nel dominio spaziale, porta evidentemente a rendere lo spazio inutile, a questo noi pensiamo raramente, non ci facciamo molta attenzione perché siamo abituati, però se pensiamo a

vivere 10 minuti, mezz'ora, un'ora senza spazio, probabilmente non riusciremo più a vivere.

Oggi il posizionamento che abbiamo, i nostri cellulari quando ci spostiamo, è tutto dato dai GPS, dai satelliti - posizionamento che sono in quota. Le comunicazioni da un continente all'altro avvengono grazie ai satelliti. Le transazioni finanziarie avvengono grazie ai satelliti. Quindi le immagini satellitari, che un ruolo enorme hanno avuto e stanno avendo nel conflitto in Ucraina, anche quello si fermerebbe, se non vi fosse la sicurezza cybernetica.

Quindi sono due domini che si muovono parallelamente. È su questo va posta molta attenzione; ma è una cosa che non facciamo, non l'abbiamo fatto con Internet, non l'abbiamo fatto con la crescita del digitale, non abbiam saputo regolamentarlo, non ci abbiamo riflettuto, non abbiamo fatto una scada di cultura, la stessa cosa sta succedendo nello spazio dove ci stiamo approcciando con la stessa leggerezza. Così come pensavamo che internet all'inizio fosse solamente un campo da sfruttare, forse un nuovo dominio per l'economia.

In effetti si parla di space economy, è il termine più noto quando si parla di spazio, però nessuno si preoccupa della sicurezza. Io faccio sempre questo esempio, quando intervengo a parlare di questi domini, questo esempio è : Lo spazio e il cyber sono un po come il Mar Mediterraneo, cioè la dimensione del Mar Mediterraneo, dove il progresso dipende dalla sicurezza, cioè se il Mediterraneo è sicuro, se le navi si possono muovere, se si può commerciare con le diverse sponde in sicurezza, senza sottomarini che ci aggrediscono, questo ci garantisce il progresso.

Ecco lo spazio, così come il dominio cybernetico sono un po' così, bisogna garantirne la sicurezza affinché il progresso possa evolvere, perché di progresso stiamo parlando, stiamo parlando di crescita della nostra società. Il futuro (siamo già nel futuro, questo è stato detto) noi come difesa condividiamo gli stessi problemi che condivide l'Agenzia cibernetica, ovviamente.

Il problema principale è una carenza di risorse. Si è parlato di Israele, Israele è un bellissimo esempio, purtroppo non è calzante. Perché Israele? Come è noto a tutti, ha un esercito di leva, quindi tutti i cittadini israeliani passano

attraverso la leva, è chiaro il bacino enorme, ma soprattutto devi passare da lì per forza, poi se sei bravo ti prendono.

Noi questa possibilità ovviamente non l'abbiamo e quindi dobbiamo cercare di attrarre i giovani migliori per venire nelle nostre Istituzioni e questo non è difficile, non è particolarmente difficile. Il problema che io personalmente ritengo essenziale è che molte volte si riduca tutto a un problema salariale. Quanto guadagno qui, quanto guadagno nel privato, quando guadagno nel pubblico.

E forse invece bisognerebbe fare leva sui valori, cosa vuol dire lavorare per il tuo paese, lavorare per la tua bandiera, questo è molto importante. E non è una cosa solitamente italiana, perché in tutti gli altri paesi, quando si lavora nel pubblico si guadagna meno che nel privato.

Però altri paesi sanno far leva maggiormente sullo spirito di Patria, sull'amore per il proprio paese e questo li aiuta a reclutare queste persone. Quindi per noi è un grosso sforzo nel reclutamento e un grosso sforzo nella formazione, formazione non soltanto dei nuovi che arrivano o di quelli che ci sono, ma soprattutto formazione della nostra giovane leadership, quelli che si stanno affacciando alla carriera militare perché devono essere abituati sin da piccoli a pensare cyber e a pensare spazio, li metto sempre insieme, perché solamente dall'integrazione fra tutte queste capacità possono diventare dei comandanti del domani e possono garantire la difesa e il progresso del nostro paese. Grazie.

**LE SFIDE GLOBALI DEL CYBERCRIME, COME DIFENDERSI
E IL RUOLO DELLA GUARDIA DI FINANZA**
Col. Marco Menegazzo

*Comandante del Gruppo Privacy del Nucleo Speciale Tutela Privacy
e Frodi Tecnologiche della Guardia di Finanza*

1. PREMESSA

Desidero anzitutto porgere il mio personale ringraziamento per questa occasione offerta al Corpo della Guardia di Finanza di esporre la propria testimonianza e il proprio punto di vista in merito a tematiche di grande attualità e particolare interesse operativo, quali quelle riconducibili al mondo della sicurezza cibernetica e, più in generale, al mondo della sicurezza nazionale di fronte alle minacce portate dalle moderne tecnologie.

Sono il Colonnello Marco Menegazzo Comandante del Gruppo Privacy del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza, reparto con sede in Roma con competenza nazionale, orientato in via preminente alla collaborazione con l’Autorità Garante per la protezione dei dati personali, per i profili operativi in materia di tutela e protezione dei dati personali e al contrasto della criminalità in rete, per gli aspetti concernenti il cybercrime avente riflessi sugli interessi economico-finanziari del Paese.

Nel corso del mio intervento saranno delineati i principali elementi informativi concernenti lo scenario di contesto del cybercrime e la conseguente necessità di difesa dalle aggressioni portate ai dati e ai sistemi informativi, il rapporto tra sicurezza cibernetica e tutela della privacy e il ruolo del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche quale dispositivo di contrasto messo in campo dalla Guardia di Finanza.

2. ANALISI DI CONTESTO

Nel contesto attuale, caratterizzato dall’incremento esponenziale del ricorso all’utilizzo degli strumenti informatici e dal parallelo incremento degli attacchi alle reti e ai sistemi informativi, il dominio cibernetico rappresenta un “terreno di confronto” con riflessi sulla regolarità della prestazione dei servizi essenziali e sulla sicurezza nazionale e, non ultimi, sugli interessi economico-

finanziari del Paese, la cui tutela rappresenta la mission istituzionale della Guardia di Finanza.

Gli interventi del legislatore, attraverso la Direttiva NIS, l'istituzione del perimetro di sicurezza nazionale cibernetica e la creazione dell'Agenzia per la Cybersicurezza Nazionale, oltre che armonizzarsi con la normativa europea in materia e con le analoghe iniziative poste in essere dagli altri Paesi comunitari, mirano alla progressiva crescita della cultura della sicurezza informatica, i cui fattori cruciali restano il rafforzamento della collaborazione tra settore privato, Amministrazioni centrali ed Istituzioni locali, in un quadro di maggiore promozione e conoscenza della cultura digitale in funzione anche dello sviluppo industriale e tecnologico del Paese.

La strategia nazionale, come indicato in particolare dalla Direttiva, prevede che siano definiti i piani di valutazione dei rischi informatici, di sensibilizzazione e di formazione dei cittadini in materia di sicurezza informatica e soprattutto prevede che siano predisposte le contromisure agli incidenti informatici in termini di preparazione, risposta e recupero dei servizi eventualmente compromessi, in un quadro di spiccata resilienza dei sistemi informativi strategici per il Paese.

Conformemente a quanto previsto dalla Direttiva, appare evidente come i sistemi informativi che operano servizi essenziali per il vivere civile debbano essere necessariamente dotati di “adeguate” misure tecnico-organizzative per la gestione dei rischi e per la prevenzione degli incidenti informatici.

Comunque, devono poter essere in grado di ridurre l'impatto di eventuali incidenti occorsi dimostrando di essere adeguatamente resilienti attraverso il tempestivo rispristino dei servizi eventualmente compromessi.

Infatti, se un servizio è fondamentale per il mantenimento di attività sociali e/o economiche, se la fornitura di tale servizio dipende dalla rete e dai sistemi informativi e se un incidente informatico produce effetti negativi rilevanti sulla fornitura di tale servizio, le ricadute in termini di funzionalità, di frustrazione dei diritti e delle legittime aspettative dei cittadini, di danno economico e di immagine, possono essere di notevole portata.

Il “mondo cibernetico”, che potremmo definire come quell’insieme di infrastrutture tecnologiche interconnesse, rete internet compresa, che si estende a tutti gli apparati tecnologici (sistemi di telecomunicazione, computer e loro componenti, prodotti hi-tech, ecc.) in grado di collegarsi tra loro, rappresenta una nuova dimensione in cui le tecnologie vanno a caratterizzare e condizionare, ormai in modo determinante, la vita delle società moderne, ampliando il perimetro di quello che fino ad oggi abbiamo chiamato il mondo reale.

Il mondo cibernetico è fatto di strutture fisiche, processi matematici, software ed informazioni, che finiscono per rappresentare un sistema articolato e complesso, non sempre conosciuto in tutte le sue parti, si pensi alle reti del c.d. “dark web”, capace di generare ingenti profitti ma anche significative perdite per le economie ed i sistemi nazionali.

Gli aspetti connessi alla rete mondiale toccano sempre di più la vita quotidiana delle persone, riverberano innumerevoli implicazioni in ambito lavorativo e sociale, ma in molti casi si assiste ancora alla mancanza di coscienza e consapevolezza riguardo alle opportunità ma soprattutto ai rischi.

Il rapporto tra cittadini e tecnologie evidenzia talvolta aspetti preoccupanti sul piano dell’alfabetizzazione e del corretto uso dei dispositivi elettronici, facendo emergere, molto spesso, criticità e vulnerabilità comportamentali che offrono terreno fertile e profitto a numerose condotte illecite.

Parimenti, analoga situazione viene riscontrata dal lato delle imprese, ove una scarsa percezione del problema e una insufficiente sensibilità tecnologica, accompagnate sovente dall’assenza di competenze o ruoli organizzativi dedicati, finiscono per aprire la strada a minacce informatiche o azioni fraudolente, sempre più massive e sofisticate.

Come risulta dal Rapporto Censis-DeepCyber sulla cybersicurezza in Italia, presentato lo scorso 22 aprile al Senato della Repubblica, la situazione è in chiaro-scuro. Infatti, se il 61,6% degli italiani è preoccupato per la sicurezza informatica e adotta sui propri device precauzioni per difendersi, il restante 38,4, quindi quasi 4 italiani su 10, sono indifferenti o non si tutelano dagli attacchi informatici.

Di contro, l'81,7% degli italiani ha paura di essere vittima di furti e violazioni dei propri dati personali in rete, percependo il rischio principalmente nella navigazione web, nell'utilizzo di account social, negli acquisti di prodotti online e nelle operazioni di home banking, ma solo 1 su 4 ha un'idea chiara di cosa sia la cybersecurity.

Lo spazio telematico globale, di dimensioni virtualmente infinite, è estremamente complesso, soprattutto se lo si guarda dal lato del rischio sistematico. Costituisce anche un luogo di interesse per le reti criminali organizzate, il cui obiettivo è di sottrarre denaro, truffare o raggirare a scopo di lucro cittadini ed organizzazioni, falsando in questo modo la leale concorrenza, nuovo inedito campo di battaglia e di competizione anche geopolitica.

Tutto ciò determina enormi ricadute sul tessuto economico e produttivo nazionale tanto che la vulnerabilità dei sistemi e delle reti, anche sotto il profilo della sicurezza economico/finanziaria, è tra i fondamentali fattori di preoccupazione per la maggioranza delle istituzioni e per le categorie economiche e sociali.

Particolarmente insidiose sono poi le nuove criticità dovute alla crescita esponenziale di tutte quelle attività illecite che trovano particolare agio nella parte più profonda della rete, in quell'area nascosta del dark web, non indicizzata dai motori di ricerca, che offre ampia garanzia di anonimato grazie anche ai numerosi servizi nascosti ivi presenti e all'uso massivo di transazioni finanziarie operate attraverso cryptovalute dalle caratteristiche intrinsecamente anonime.

La situazione emergenziale creata dalla pandemia da Covid-19 ha comportato un massiccio ricorso al digitale e questo ha permesso a molte aziende di proseguire la propria attività, così come ha consentito alla Pubblica Amministrazione di continuare a erogare i servizi ai cittadini. Con lo smart working, la nuova modalità di lavoro imposta dall'emergenza Covid-19, si è ampliata la superficie di attacco informatico, dischiudendo nuove opportunità ai cyber criminali: i dipendenti sono risultati in molti casi vulnerabili alle campagne di phishing per carpire credenziali di accesso ai sistemi informativi, esponendo così dati aziendali o dati sensibili al rischio di perdita o furto.

Si tratta dunque di un quadro d'insieme particolarmente complesso e in continua trasformazione, ove l'incremento delle opportunità è accompagnato da un parallelo incremento delle vulnerabilità, tanto da richiedere una sempre maggiore consapevolezza ed attenzione da parte di tutte le istituzioni interessate.

La diffusione massiva della tecnologia rende la vita più semplice ma al tempo stesso anche più fragile e vulnerabile: i problemi legati alla digitalizzazione e alla diffusione della cultura della sicurezza e della resilienza cibernetica non sono nati con la pandemia, ma erano e restano centrali.

La cybersecurity, che non può più essere considerata un costo o un ambito per soli esperti, diventa sempre più un investimento sociale di interesse collettivo, indispensabile per una corretta evoluzione digitale.

La sfida riguarda la messa in sicurezza delle infrastrutture, l'affrancamento dalla dipendenza tecnologica, la consapevolezza e la formazione degli utenti all'interno della cornice data dai ruoli attribuiti all'Agenzia nazionale, alle investigazioni svolte dalle Forze di polizia, alla cyber intelligence e alla cyber defence.

Nondimeno, la necessità di intervenire nella cybersicurezza, con investimenti appropriati e in un quadro coerente di necessità e priorità adeguate a fronteggiare le minacce cibernetiche globali, rende ineludibile l'esigenza di dare attuazione al Piano nazionale di ripresa e resilienza (PNRR), che prevede apposite progettualità nell'ambito della cybersecurity, oltre alle specifiche iniziative per la digitalizzazione e l'innovazione quali strumenti per rilanciare la competitività e la produttività del sistema Paese.

Il ruolo della digitalizzazione e innovazione riguarda infatti, trasversalmente, tutte le Missioni previste dal Piano: la Digital Transformation è quindi un passaggio obbligato per consentire alla Pubblica Amministrazione, come alle aziende private, di affrontare le sfide che pone l'economia attuale.

Parallelamente alle sfide poste dalla criminalità informatica sul piano dell'aggressione ai sistemi informativi pubblici e privati, come ai danni dei cittadini, si pone il tema dell'utilizzo, nelle attività illegali cibernetiche delle valute virtuali, la cui connessione con la missione istituzionale della Guardia di Finanza emerge chiaramente sia sotto il profilo della polizia giudiziaria di

prevenzione e repressione dei reati che della polizia economico-finanziaria per gli aspetti relativi al riciclaggio dei proventi illeciti e della immissione nell'economia di capitali di origine illegale.

Le valute virtuali o criptovalute, la cui origine viene fatta risalire al 2009 con la creazione del Bitcoin, possono essere utilizzate in una grande varietà di modi, di cui alcuni legittimi ed eticamente corretti, altri illegali e pericolosi, sottoponendo gli operatori di polizia a sfide sempre nuove, che possono essere affrontate solo avendo chiari e definiti i criteri posti alla base della loro essenza e funzionamento.

Una delle caratteristiche che rende difficile l'azione di controllo e di vigilanza del mondo delle criptovalute è la decentralizzazione, ovvero l'assenza di un organo centrale che possa esercitare un qualsiasi tipo di potere sulle stesse e sulle attività effettuate dagli utenti, essendo le criptovalute, per definizione, prive del requisito della materialità.

Altro aspetto da tenere presente è che le criptovalute funzionano grazie alla rete Internet, risultando pertanto prive di qualsiasi nazionalità o riferimento territoriale. Queste caratteristiche, in linea di massima, possono essere riscontrate anche nelle altre centinaia di monete virtuali esistenti, create successivamente al Bitcoin, soprattutto in quelle caratterizzate da un elevato grado di anonimizzazione.

Dal punto di vista normativo, sussistono invece criticità in ordine alle tematiche del sequestro della valuta virtuale e della sua conversione in valuta corrente per la devoluzione al Fondo Unico di Giustizia.

Altre tematiche da tenere in considerazione sono quelle della disponibilità di fondi in criptovaluta per l'esecuzione di operazioni undercover e dell'auspicabile modifica normativa inerente l'estensione ai reati informatici dell'istituto delle "Operazioni sotto copertura" di cui all'art. 9 della Legge 146/2006.

3. CYBERCRIME E DIFESA DALL'AGGRESSIONE AI DATI

L'impianto normativo nazionale a tutela della sicurezza dei dati e la conoscenza delle dinamiche che agitano il mondo del cybercrime non possono

naturalmente, da soli, arginare le minacce e prevenire i danni derivanti dagli attacchi informatici, soprattutto da quelli portati da soggetti ed organizzazioni particolarmente preparati e determinati, e quindi insidiosi. Né la funzione repressiva esercitata dagli attori istituzionali, in primis dalle Forze di Polizia, può scongiurare l'insorgenza di nuovi attori malevoli e di nuove tecnologie di aggressione alla sicurezza informatica pubblica, aziendale e privata.

La principale barriera rimane la prevenzione e la protezione delle infrastrutture informatiche e dei dati attraverso politiche operative di sicurezza nazionale adottate dai Governi, dalle Istituzioni, dalle imprese e anche dai singoli cittadini, sia implementando misure di difesa attiva, sia diffondendo in maniera sempre più capillare la cultura della consapevolezza della sicurezza informatica a tutti i livelli.

In definitiva, sia che si tratti di una Pubblica Amministrazione, di un'impresa privata o di semplici cittadini, la definizione stessa di cybersicurezza fornita dalla Legge e in particolare dall'art. 1 del Decreto 82/2021 istitutivo dell'Agenzia per la Cybersicurezza Nazionale, stabilisce che l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, deve assicurare la disponibilità, la confidenzialità o riservatezza e l'integrità dei dati, garantendone la resilienza.

In definitiva è la concreta risposta a questi principi ispiratori che costituisce l'unica tipologia di efficace difesa dalle aggressioni portate ai dati.

In sostanza, le informazioni devono essere accessibili nel determinato momento in cui servono, esclusivamente ai soggetti che hanno diritto ad accedervi e non devono essere alterate o corrotte. Caratteristiche che peraltro devono essere garantite durante tutto il ciclo di vita dell'informazione, ossia da quando viene generata e/o raccolta a quando viene distrutta, passando ovviamente per ogni tipo di conservazione.

A questo si aggiunge la resilienza, ovverossia la capacità dei sistemi di resistere ad un attacco non solo in termini di "robustezza" delle strutture ma soprattutto come capacità di recuperare al più presto le funzionalità previste attraverso il tempestivo ripristino della piena operatività.

Da sottolineare che questi punti di riferimento programmatico

possono essere compromessi non solo da azioni ostili via malware, terreno di battaglia tipico del cybercrime, ma anche alla possibilità di attacco fisico ai sistemi informativi in chiave simbolica, propagandistica e politica. Mi riferisco ad eventuali atti terroristici mirati alle infrastrutture dove sono residenti i sistemi elaborativi e alla conseguente indisponibilità di dati e servizi di importanza rilevante o strategica per il Paese. La difesa da queste minacce è possibile con adeguate misure di sicurezza e vigilanza fisica delle infrastrutture ma soprattutto adottando soluzioni di disaster recovery in grado di scongiurare la perdita dei dati e il ripristino delle funzionalità in tempi rapidi e comunque non impattanti sulla produttività dei sistemi eventualmente coinvolti.

Stesso discorso di ottimizzazione delle soluzioni di disaster recovery in termini di operatività vale per tutte le minacce di tipo fisico, vale a dire quegli eventi naturali o fortuiti, quali terremoti, alluvioni, incendi, azioni umane sconsiderate, che possono compromettere l'integrità fisica dei sistemi e dei dati.

Più complesso ma non meno critico da punto di vista della risposta all'aggressione ai patrimoni informativi pubblici o privati è il mondo del cybercrime prettamente inteso. Come noto, il crimine informatico è il fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica. Il crimine informatico può essere generalmente definito come un'attività criminale che coinvolge la struttura della tecnologia di informazione, compreso l'accesso illegale, l'intercettazione, le interferenze sui dati, l'uso improprio di dispositivi, il furto di identità e le frodi elettroniche.

Attesa la dimensione transnazionale dei crimini informatici che dispiegano la propria azione nella extraterritorialità della rete Internet, l'esigenza collaborativa internazionale si è concretizzata con l'approvazione, da parte del Consiglio d'Europa, in data 23 novembre 2001, della cosiddetta Convenzione di Budapest. Essa rappresenta il primo accordo internazionale sui reati commessi tramite Internet o reti elettroniche. Con tale Convenzione gli Stati aderenti hanno adottato misure legislative rivolte alla repressione penale dei crimini informatici, armonizzando, in questo modo, i diversi ordinamenti giuridici interni e coordinando forme di collaborazione ai fini dell'acquisizione delle prove.

La ratifica della convenzione ha modificato il codice penale, con

l'introduzione di nuove specifiche fattispecie di reato e la modifica di alcune fattispecie già previste, il codice di procedura penale, con riferimento ad articoli fondamentali per le indagini di polizia giudiziaria, la competenza del Procuratore Distrettuale sui reati informatici, e la responsabilità amministrativa dell'impresa di cui al D.Lgs. 231/2001 per taluni reati informatici.

Anche le indagini di polizia giudiziaria rappresentano quindi una risposta all'aggressione ai dati, quantomeno in chiave repressiva mirata a colpire gli autori di eventi dannosi penalmente rilevanti e in chiave preventiva di deterrenza e di eventuale scoperta di nuove minacce da fronteggiare con adeguate contromisure.

Ma catalogare gli attacchi tecnici possibili è un esercizio difficile, dal momento che la loro quantità e la loro qualità sono connotate dalla creatività e dall'ingegnosità degli attaccanti e spesso, negli attacchi reali, tecniche diverse possono essere usate in modo combinato, rendendo più sfumata una possibile classificazione. Generalmente, con il termine “malware” si indica la particolare categoria di programmi informatici il cui scopo è quello di danneggiare l'utente o i sistemi sui quali tali programmi vengono involontariamente caricati, mediante l'esecuzione di processi inattesi e non autorizzati. Esistono diversi tipi di malware ma la loro composizione e la loro continua evoluzione rendono difficile una classificazione coerente.

Il compito del malware è quello di infettare i sistemi informatici target allo scopo di danneggiarli o per carpire informazioni di vario genere, soprattutto quelle riservate o sensibili, soprattutto dal punto di vista economico.

Altre forme di cyber-attacco prevedono lo sfruttamento di vulnerabilità delle reti, dei software di base, delle configurazioni hardware e software dei sistemi o di fallo nell'organizzazione IT per guadagnare un accesso, non controllato, ai sistemi stessi. In molti casi tale accesso viene facilitato dagli stessi utenti, indotti a rivelare le informazioni necessarie, come account, password, iban, mediante tecniche che si basano, essenzialmente, sulla vulnerabilità del “fattore umano”. In questo caso i cyber attacchi sfruttano qualunque forma di debolezza o vulnerabilità umana delle vittime facendo leva su tecniche sempre più sofisticate di “social engineering” .

Pertanto, la risposta alla domanda “come difendersi dagli attacchi informatici” passa anche e forse soprattutto dalla serie di accorgimenti e buone pratiche generali che dovrebbero essere patrimonio di tutti i cittadini, sia nella veste di appartenenti ad organizzazioni più o meno complesse pubbliche o aziendali, sia nella sfera privata.

I comportamenti virtuosi sono in definitiva basilari ma non per questo meno efficaci se praticati con costanza e vigile attenzione. Ci si riferisce, alle seguenti regole:

- eseguire backup periodici con la regola 3-2-1, dove 3 sta per tre versioni dei dati, una originale e due copie, 2 sta per due tipi di supporto diverso per le copie e 1 sta per una copia custodita in luogo diverso;
- utilizzare password complesse e possibilmente multifattoriali;
- utilizzare sistemi firewall di protezione perimetrale della rete;
- utilizzare mail istituzionali con crittografia abilitata;
- evitare click compulsivi e verificare i mittenti dei messaggi di posta;
- proteggere le postazioni di lavoro e i device mobili con antivirus;
- aggiornare i software di base quando richiesto;
- adeguare i piani di protezione e sviluppare i sistemi nuovi con la filosofia della “security by design”;
- aggiornarsi periodicamente sulle soluzioni di sicurezza, anche consultando canali tematici.

4. CYBERSECURITY E PRIVACY

Diverse quindi sono le minacce a cui è esposta costantemente la sicurezza della dimensione cibernetica in cui anche i conflitti si spostano sempre più su un terreno sostanzialmente privo di un'adeguata cornice di diritto internazionale.

In tale contesto, l'equilibrio tra protezione dei dati e tutela della sicurezza cibernetica è complesso ma anche foriero di nuove sfide e sinergie. In sintesi, occorre riuscire a contemperare le esigenze di tutela della sicurezza cibernetica, quale dimensione rilevante anche della sicurezza nazionale, con le esigenze di tutela della privacy dei cittadini, attraverso il rispetto del principio

di proporzionalità, unico punto di riferimento per controbilanciare esigenze di prevenzione generali e diritti individuali.

Ma si può osservare anche come il rapporto tra protezione dati e cybersecurity presenti punti di contatto e reciproche funzionalità. Infatti, mentre la cybersecurity implica innanzitutto la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale fino, in ultima analisi, alla sicurezza nazionale, le eventuali compromissioni di basi dati personali appartenenti a soggetti pubblici o privati, i cd. "data breach" previsti dalla normativa in materia di tutela dei dati personali, oltre ad assumere importanza per i singoli cittadini interessati, possono essere di rilievo anche per la sicurezza nazionale in funzione della tipologia dei dati acceduti in maniera illegale.

Soprattutto nel campo economico-finanziario, settore di intervento della Guardia di Finanza, il rapporto tra protezione dati e sicurezza significa tutelare contemporaneamente i singoli e la collettività.

Per fronteggiare le minacce globali alla sicurezza cibernetica, l'obiettivo deve essere traguardato in chiave sovranazionale, quantomeno europea. Notevole, dal punto di vista giuridico, economico e simbolico l'applicabilità del GDPR a soggetti esterni alla Comunità ma che trattano dati all'interno del continente europeo. In tal modo, i cosiddetti "giganti del web" sono stati attratti nell'orbita del diritto comunitario a prescindere dalla sede dell'attività aziendale.

D'altronde, in uno spazio privo di dimensione "fisica" come la rete, la sovranità deve ispirarsi a forme nuove, non necessariamente legate al tradizionale criterio della territorialità, capaci di garantire ai cittadini di rendere effettiva la tutela dei propri diritti.

La manipolazione dei dati personali e la profilazione degli utenti finalizzata ad orientare tendenziosamente le volontà dei cittadini, rendono evidenti i connessi profili di sicurezza nazionale in quanto possibile alterazione dell'ordinata competizione democratica. In definitiva, la disinformazione online, sfruttando le caratteristiche del domino cibernetico, può condizionare o influenzare i processi sociali, economici e politici del Paese.

Parallelamente, vanno considerati i rischi, per la sicurezza nazionale,

derivanti dall'adozione di tecnologie ad alto valore aggiunto da parte di Paesi in cui il sistema politico è fortemente incidente sulle aziende produttrici di tecnologie, soprattutto nel campo delle telecomunicazioni. Qualunque accordo commerciale non può prescindere dal rispetto delle basilari condizioni di tutela del diritto alla protezione dei dati dei cittadini europei, tutela che in questo caso dispiega i propri effetti anche sul terreno della sicurezza cibernetica.

5. IL RUOLO DELLA GUARDIA DI FINANZA

Nel documento di Strategia Nazionale di Cybersicurezza, presentato dall'Agenzia Nazionale alla fine dello scorso mese di maggio, tra i pilastri tecnico-operativi della complessiva architettura nazionale di cybersicurezza, viene indicata la funzione di prevenzione e contrasto della criminalità informatica che viene attuata dalle componenti specialistiche delle Forze di Polizia, venendo quindi menzionato anche il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza.

Infatti, la presa di coscienza delle gravi minacce al sistema Paese derivanti dall'utilizzo illecito delle nuove tecnologie ha portato la Guardia di Finanza a rafforzare il dispositivo di contrasto alle condotte criminali che impattano sul tessuto economico e finanziario, peraltro in continua evoluzione.

In tale contesto, l'attività svolta dal Corpo si declina, in ragione dei poteri ad essa attribuiti, in attività di polizia economica e finanziaria, nonché giudiziaria, estesa ad ambiti sempre più diversificati sul piano tecnologico e territoriale, coprendo, nello specifico, la rete internet e più in generale le tecnologie, e superando, sempre più spesso, la soglia dei confini nazionali in cooperazione con i paesi aderenti alle diverse organizzazioni internazionali previste da singoli trattati o convenzioni.

La Guardia di Finanza, in ogni sua espressione operativa, si muove trasversalmente nell'ambito della missione istituzionale di polizia economico-finanziaria che le è affidata, attraverso un approccio per sua natura multidisciplinare.

I moduli di azione, anche nelle investigazioni che impattano con il mondo digitale, sono, quindi, contestualmente orientati:

- al controllo economico del territorio virtuale, attraverso il

monitoraggio della rete telematica, anche nascosta, per verificare l'esistenza di sacche d'illegalità e per intercettare flussi finanziari "sospetti";

- a verificare la posizione fiscale dei soggetti investigati per l'eventuale tassazione dei proventi illeciti;

- ad intervenire, trasversalmente, sui diversi profili, quali, ad esempio, quelli in materia valutaria, della privativa intellettuale e sicurezza prodotti, della concorrenza e mercato, oltre che della privacy.

Nel contrasto agli illeciti di carattere economico-finanziario realizzati in internet, ovvero per mezzo di dispositivi tecnologici, il Corpo interviene attraverso due direttive che sono in continuo contatto funzionale tra loro:

- la rete dei reparti territoriali, capillarmente distribuiti sul territorio nazionale, con il compito di assicurare, nei rispettivi ambiti, l'esecuzione dei compiti istituzionali. Tra i reparti, i Nuclei di polizia economico-finanziaria, ulteriormente rafforzati da specifiche professionalità, si pongono come unità investigative di punta;

- i reparti speciali che si affiancano ai primi e che, istituiti per l'approfondimento di specifiche materie, sono incaricati di realizzare direttamente, ovvero con azioni di supporto alle unità operative, moduli investigativi connotati da elevati standard qualitativi.

Questi ultimi, proprio in ragione della sempre maggiore complessità dei fenomeni criminali, assumono un ruolo fondamentale nella strategia di contrasto a tale tipologia di illeciti, soprattutto in tema di "supporto di conoscenze", acquisendo ed aggiornando costantemente il patrimonio conoscitivo e tecnico specialistico utile all'azione di tutti i reparti.

Allo scopo di meglio delineare il quadro delle competenze e delle attribuzioni delle Forze di Polizia a carattere generale, con Decreto del Ministro dell'Interno in data 15 agosto 2017, sono stati fissati i principi ispiratori dell'azione delle strutture dedicate al mondo virtuale e tecnologico della Polizia di Stato, dell'Arma dei Carabinieri e della Guardia di Finanza.

L'azione di prevenzione e contrasto, che vede coinvolte tutte le Forze di Polizia, deve dispiegarsi sul "terreno virtuale" in cui sempre più trovano una propria proiezione pervasiva le organizzazioni criminali che hanno solide radici

nel mondo reale. Nondimeno, è stata ritenuta necessaria l'adozione di criteri di ripartizione di specialità, ferme restando le specifiche attribuzioni delle singole Forze di Polizia e le relative competenze trasversali sulle attività criminali di più spiccato allarme sociale quali, ad esempio, il traffico di sostanze stupefacenti.

Il Corpo della Guardia di Finanza, tenuto conto delle attribuzioni di polizia economico-finanziaria, valutaria e amministrativa conferite dall'art. 2 del decreto legislativo 19 marzo 2001, n. 68 e dalle normative specifiche di settore, attraverso il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, ha competenza preminente per la ricerca, la prevenzione e il contrasto degli illeciti perpetrati sfruttando la rete nei settori delle entrate tributarie, della spesa pubblica, della tutela della concorrenza e del mercato, della normativa valutaria e dei mercati finanziari.

Peraltro, il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, in ossequio al principio che ha assimilato l'ambiente virtuale al territorio fisico, opera costantemente gli approfondimenti in rete, sia attraverso metodologie di Open Source Intelligence, sia mediante sofisticate tecniche di reperimento, analisi e filtraggio delle informazioni rinvenute, al fine di isolare potenziali risorse web dedite ad attività illegali.

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, che dipende dal Comando delle Unità Speciali, è il reparto della Guardia di Finanza che garantisce il costante presidio di polizia economico-finanziaria in rete. Il Comando Generale del Corpo, sin dal 2001, aveva avvertito l'esigenza di istituire un reparto che quotidianamente fosse impegnato in prima fila in un contesto operativo in esponenziale sviluppo tecnologico, dove gli interessi delle organizzazioni criminali avevano individuato un florido ambiente per perseguire i propri obiettivi in danno del settore economico-finanziario. Nel tempo, la consapevolezza di un maggiore impegno nel settore degli illeciti di natura economico-finanziaria perpetrati in rete ha portato, nel corso del 2004 all'elevazione dell'allora Gruppo Anticrimine Tecnologico (GAT) a Nucleo Speciale Frodi Telematiche, poi Tecnologiche. Nel corso del 2012 ne veniva, contestualmente, potenziata la struttura ordinativa, prevedendo la creazione al suo interno di quattro Gruppi operativi che sviluppano attività di polizia

giudiziaria nel cybercrime, effettuando un monitoraggio costante della rete finalizzato all'individuazione di fenomeni illegali, ivi incluso il riciclaggio e il finanziamento al terrorismo internazionale. Viene, altresì, attenzionato il settore delle criptovalute, che, atteso l'elevato grado di anonimità garantito dal loro utilizzo, sono sempre più impiegate per effettuare transazioni illecite. Nel 2018, con l'avvento del GDPR ed una conseguente riforma ordinativa, il Nucleo ha integrato la propria struttura operativa con l'azione a tutela della privacy, passando da 4 a 5 Gruppi investigativi.

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche garantisce altresì un'attività di ausilio agli altri reparti del Corpo in tutti quei settori d'interesse istituzionale nei quali le violazioni sono commesse ricorrendo ad Internet ovvero alle cosiddette "nuove tecnologie". In tale ambito, il Nucleo è Polo Tecnologico per tutta la Guardia di Finanza ed è incaricato di assumere un ruolo di centralità nella gestione delle tecnologie e nello sviluppo di sistemi informatici di ausilio alle indagini di polizia, nel supporto specifico alle unità territoriali nel settore della "Computer Forensics & Data Analysis", nonché nell'interscambio di esperienze con Enti istituzionali esterni, al fine di avviare specifiche iniziative di collaborazione che consentano di migliorare le professionalità e l'aggiornamento del personale impiegato in tali specifici ambiti di servizio.

Tutto questo richiede, ovviamente, un costante aggiornamento professionale, anche attraverso il continuo confronto con omologhe strutture di "law enforcement" nazionali ed estere, centri ricerche, mondo accademico, associazioni di categoria, principali operatori economici nel campo delle tecnologie e della sicurezza delle comunicazioni.

Vale la pena di accennare anche al fatto che il Nucleo Speciale svolge, con propri rappresentanti, attività di docenza all'interno di master universitari organizzati da diverse Università, oltre che presso le strutture di formazione del Corpo e partecipa a convegni tematici proposti da Istituzioni, Enti, Associazioni e Forze di Polizia nazionali e internazionali.

Numerose sono poi le partecipazioni a tavoli di lavoro interforze a livello nazionale e internazionale.

Impegnativo e significativo ai fini della tutela della legalità e della

sicurezza, infine, è il monitoraggio svolto sulla parte oscura della rete, il cd. dark web, in cui proliferano numerose attività illecite particolarmente insidiose se si pensa a fenomeni gravi come quelli del traffico d'armi, di droga, di documenti falsi, dati personali ecc. La caratteristica peculiare che rende il Dark Web appetibile per la perpetrazione di pratiche illegali è l'alto grado di anonimato che offre. Si tratta, infatti, di un particolare protocollo di comunicazione elettronica che fornisce servizi di vario genere, quali quelli web, di chat e di posta elettronica, non indicizzabili dai comuni motori di ricerca utilizzati per la navigazione Internet.

6. CONCLUSIONE

L'articolata dimensione che chiamiamo spazio cibernetico non può essere definita nella sua interezza da parametri tecnologici quali la velocità di connessione, la numerosità di interazioni tra utenti e l'accessibilità di dati e informazioni online ma bensì occorre avere riguardo agli innumerevoli servizi, interconnessi e comunicanti, concepiti per il soddisfacimento delle quotidiane esigenze delle nostre comunità e per lo svolgimento delle relative attività economiche: mi riferisco fondamentalmente alle infrastrutture energetiche, ai mercati finanziari, alle forniture di acqua potabile, ai trasporti di massa, e, non ultime, alle funzioni essenziali dello Stato, incluse la sua difesa e integrità.

La dualità tra mondo digitale e mondo reale tende a sfumare all'interno della complessità e interdipendenza dei sistemi, rendendo spesso problematica l'identificazione dei rispettivi confini e caratteristiche.

Da una parte, la “migrazione” verso il digitale è resa più conveniente dall'incessante evoluzione delle moderne tecnologie, dall'altra, la sicurezza della società e, in prospettiva, lo sviluppo economico e il benessere del Paese possono essere garantite solo dalla resilienza e dalla sicurezza delle reti e dei sistemi su cui tali servizi si basano.

L'eliminazione delle minacce che provengono dallo spazio cibernetico non può essere completamente raggiunta da parte di nessuna organizzazione, pur tecnologicamente equipaggiata e proceduralmente preparata, siano le minacce stesse volte ad ottenere profitti illeciti, come nel caso del cyber-crime, che a generare vantaggi informativi o a diffondere narrative divisive e

polarizzanti in aderenza a specifiche ideologie nella competizione geopolitica, come nel caso del cyber-espionage.

Le sfide che vengono portate, quindi, richiedono l'innalzamento della resilienza delle infrastrutture digitali, secondo un approccio che includa l'adozione di misure di prevenzione e mitigazione del rischio nelle reti e nei sistemi di dati e, soprattutto, l'aumento della consapevolezza degli attori istituzionali, delle imprese private e dei cittadini attraverso una diffusa cultura della cybersicurezza.

È in tale contesto infatti che emerge il disallineamento della percezione della propria sicurezza in quanto alle azioni volte a tutelare la dimensione della sfera fisica o patrimoniale non corrisponde, troppo spesso, la pari tutela della dimensione digitale. Inoltre, i bassi costi e l'elevata disponibilità degli strumenti offensivi uniti all'accresciuto livello di complessità degli attacchi, alla difficoltà tecnica di individuarne gli autori e alle vulnerabilità di software e hardware diffusi, comporta l'attuale aumento del trend delle azioni ostili.

La diffusione e il progressivo impiego delle nuove tecnologie, il cui impatto presenta caratteristiche sempre più dirompenti, rischia di generare potenziali molteplici ricadute negli ambiti economico, sociale e politico, sia in termini di dipendenza tecnologica e perdita di autonomia strategica dello Stato, sia dal punto di vista dell'errore umano provocato da attori malevoli caratterizzati da diverso grado di sofisticazione e mossi da differenti, ma ugualmente dannosi, intenti.

È su queste premesse quindi che il “sistema Paese” deve proseguire ed incrementare le iniziative in materia di cybersicurezza. Lo impongono le nuove forme di competizione strategica che caratterizzano lo scenario geopolitico, la tutela degli interessi nazionali e dei cittadini. L'obbiettivo deve pertanto essere la sapiente costruzione di un ecosistema di cybersicurezza, fondato sulla collaborazione tra i settori pubblico e privato in cui la strategia nazionale per la cybersicurezza unisca sicurezza e sviluppo nel rispetto dei valori della nostra Costituzione, degli impegni assunti nell'ambito delle organizzazioni internazionali a cui l'Italia partecipa, in particolare per quanto previsto dalle strategie dell'Unione europea e della NATO.

Le Istituzioni e gli operatori economici, in particolare i gestori delle infrastrutture da cui dipende l'erogazione dei servizi essenziali dello Stato, il mondo dell'università e della ricerca, la società civile devono farsi parte attiva nel proteggere i propri assetti informatici e divenire realmente resilienti alle minacce, soprattutto nei settori della banda ultralarga, del 5G e del cloud su cui principalmente si concentra l'attenzione e la fiducia dei cittadini.

Rinnovo il mio personale ringraziamento alle Autorità intervenute e all'Autorità Garante per questa preziosa occasione di confronto su tematiche che attraversano trasversalmente le fasce generazionali della nostra società, dal punto di vista privato e lavorativo, suscitando timori e aspettative diverse, ma che tanto impattano sulla vita di tutti.

QUINTA SESSIONE



L'INFORMAZIONE NELL'ERA DIGITALE: VERO, FALSO O VIRTUALE?



- MODERA: **Baldo Meo**
- **Martina Pennisi**
- **David Puente**
- **Raffaele Barberio**
- **Massimiliano Panarari**
- **Federico Ferrazza**

QUINTA SESSIONE

L'INFORMAZIONE NELL'ERA DIGITALE: VERO, FALSO O VIRTUALE

AGOSTINO GHIGLIA

Passiamo ora all'ultima sessione dei nostri lavori, ringrazio ancora il sottocapo di Stato Maggiore, tutti gli ufficiali che ci hanno raggiunti, grazie per la disponibilità, grazie.

E grazie ovviamente al Presidente del Copasir, al Vice Direttore dell'Agenzia per la Cybersicurezza nazionale dottoressa Ciardi, al Colonnello Menegazzo, a tutti i Relatori del precedente panel e al dottor Carioti che ha sapientemente gestito questa difficile tavola rotonda.

Passiamo all'ultima sessione, **L'informazione nell'era digitale: vero, falso o virtuale?** Tema di grandissima attualità e di enorme interesse.

Avremo come moderatore il dottor Baldo Meo, nostro capo ufficio stampa da un po' di anni, nonché memoria storica importante della nostra Autorità; il dottor Federico Ferrazza, Direttore di Wired Italia, che prego di accomodarsi; il dottor Raffaele Barberio, Direttore di Key4Biz; il dottor David Puente, Vice Direttore di Open, autore televisivo e fact-checker; e il professor Massimiliano Panarari, sociologo della comunicazione presso l'Università Mercatorum ed editorialista.

Grazie, a voi la parola.

BALDO MEO

Allora buonasera, ringrazio di cuore tutti i presenti che sono rimasti stoicamente fino alla fine a seguire tutte le sessioni. Noi li ricompenseremo, cercheremo di tenere desta la loro attenzione con i temi che tratteremo in questa sessione e che riguardano appunto l'informazione nell'era digitale. Doveva essere presente Gianni Riotta, che si trova purtroppo bloccato a Leopoli.

E ringraziamo dunque Martina Pennisi, giornalista del "Corriere della Sera", di cui possiamo avvalerci anche in questo panel, nel ruolo che, a mio avviso, più le si addice: quello di grande conoscitrice del mondo della

scienza, della tecnologia e degli impatti che scienze e tecnologie hanno su vita sociale e vita economica.

Passo quindi a presentare tutti i relatori e poi dirò qualcosa anch'io, senza indulgere troppo e rubare tempo.

David Puente è un conoscitore delle tecnologie multimediali, ma soprattutto è un esperto che svolge un ruolo benemerito nel mondo dell'informazione digitale, perché è - dobbiamo usare i termini inglesi - un debunker, un fact-checker, un esperto che smaschera "bufale", che contrasta la disinformazione e le frodi online. Dal 2018 David Puente è vicedirettore di Open dove ricopre anche il ruolo responsabile del progetto di fact checking.

E' poi la volta di Raffaele Barberio, fondatore e direttore responsabile di una rivista conosciutissima nell'ambito delle tecnologie dell'informazione elettronica come Key4Biz, e negli ultimi tempi ha anche fondatore di "Privacy Italia", un'associazione molto attiva nella promozione della protezione dei dati.

E' con noi anche Massimiliano Panarari, sociologo della comunicazione, professore associato all'Università Mercatorum di Roma, ma che è anche docente di comunicazione politica alla Luiss e di storia del giornalismo alla Bocconi, nonché editorialista di importanti testate come "La Stampa" e "L'Espresso". E' autore di numerosi saggi, tra i quali vorrei ricordare "Poteri e informazione" del 2017, testo che è legato ai temi che qui oggi tratteremo.

Abbiamo con noi Federico Ferrazza, direttore di Wired, anche lui grande conoscitore di materie tech, che lavora anche come consulente strategico della comunicazione. "Wired", non occorre ricordarlo, è una prestigiosissima rivista che si occupa di tecnologia e di nuovi media.

Con i nostri relatori ragioneremo insieme su un tema che si può a buon diritto considerare cruciale e decisivo nell'epoca in cui ci troviamo a vivere. E cioè, detto in sintesi, l'effettiva capacità del mondo dell'informazione di costruire e formare un'opinione pubblica in coerenza con i fatti.

E, aggiungo, di farlo senza manipolare le coscienze: questa è una formula che può apparire un po' antiquata, ma che risulta ancora utile per

capire il processo di trasformazione e di costruzione del consenso che spuò realizzarsi attraverso i nuovi media.

Noi ci troviamo in un'epoca che è stata definita della "Platform Society", la società delle piattaforme. Bene, la società delle piattaforme, governate dai grandi oligopolisti, dai Big Tech, è una dimensione in cui si sono indeboliti, se non sono stati addirittura cancellati, i confini tra vero, falso, virtuale. Dove per virtuale noi dovremmo cominciare a intendere una pseudo verità, una elaborazione fatta di un mix di contenuti e di fonti, costruita su misura per alcune categorie di utenti o per più vaste platee, con diversi gradi di intenzionalità. E, quindi, anche a fini manipolativi.

I sistemi di questo tipo ci sono noti: dalla profilazione, a fini elettorali del caso "Cambridge Analytica" fino alle fake news e al deep fake, ricordate da Fausto Carioti e dalla dottoressa Ciardi.

Per descrivere il deep fake il caso più eclatante, forse perché è uno dei primi, riguarda la speaker della Camera Usa, Nancy Pelosi, artatamente resa ubriaca. Oppure del video di Zelensky che invita gli Ucraini ad arrendersi.

In questa sessione ci occuperemo anche della protezione dei dati personali in una società dell'archiviazione generalizzata, dove il diritto all'oblio è qualcosa di molto importante, ma anche di molto difficile da realizzare. Una società - secondo la lettura del filosofo Maurizio Ferraris - della mobilitazione totale.

Un mondo in cui, cioè, noi tutti lavoriamo gratis per i grandi monopolisti di dati che li usano a fini di guadagno, ma anche a fini cognitivi, fini di orientamento e influenza: ogni volta - e questo ormai ci dovrebbe essere chiaro - che twittiamo, commentiamo, postiamo una nostra opinione forniamo dati, riveliamo i nostri gusti, le nostre abitudini, le nostre scelte, le nostre emozioni: tutte informazioni che saranno usate per profilarci o a fini predittivi. Lavoriamo gratis per l'industria dei dati, siamo una sorta di sottoproletariato di nuova specie, diciamo così, perché anche depauperato di sé stesso.

Con i nostri relatori cercheremo dunque di parlare anche di come i nostri dati di utenti - e questo accade soprattutto nei social media -

vengono usati per creare massa informativa, anzi meglio, massa di pressione informativa, costruita per rafforzare o contrastare un’idea, una notizia o uno pseudo fatto, per amplificarlo e per costruire consenso. Da strumenti identificativi, i nostri dati stanno diventando strumenti per creare consenso. Parleremo anche, inevitabilmente, di come i governi hanno strutturato la loro comunicazione in tempi di pandemia e di guerra, e come i siti e le fonti si sono organizzati a questi fini.

Tenendo dunque il filo rosso della precedente sessione dedicata alla cyberwar, vorrei iniziare col chiedere a David Puente che effetti hanno avuto la pandemia e la guerra sull’informazione in generale e sull’informazione digitale in particolare.

DAVID PUENTE

Buonasera.

È un argomento molto carino.

Dalla mia esperienza ho notato che c’è stata questa sorta di parallelismo o fusione fra due temi, quello della pandemia e quello dell’invasione russa in Ucraina.

Molto spesso ho sentito parlare di queste fabbriche delle fake news provenienti dalla Russia, da San Pietroburgo, che “fanno cose”, ma alla fine vedo molte piccole realtà in Italia o in generale in Europa, di piccoli nuclei che fanno disinformazione a livello locale. Qualcuno lo fa per denaro, altri per ideologia.

A cavallo fra queste due situazioni ho notato che c’è stata una sorta di alleanza basata su un concetto: “il nemico del mio nemico è mio amico”. Durante la pandemia le varie realtà della disinformazione hanno creato, diffuso e sfruttato notizie false sulla Covid-19, sui vaccini, contro le case farmaceutiche, contro gli Stati Uniti, la Nato, o contro Bill Gates accusato di voler sterminare o controllare il mondo, ma cosa è successo durante la guerra in Ucraina? I russi hanno sostanzialmente riutilizzato una macchina che già funzionava bene in questi due anni pandemici.

Hanno sfruttato questo ambiente per proporci all’interno le loro narrazioni per andare contro i “nemici comuni” come l’Europa, la NATO e via dicendo. C’è questo rapporto stretto fra le due realtà, e in merito a

questo argomento c'è una mole di dati impressionante.

Faccio un esempio: si parla molto di account fasulli, di furto d'identità, ma non ho riscontrato situazioni di domini registrati con le identità rubate, piuttosto situazioni dove i documenti personali sono stati modificati, parliamo di documenti trafugati che vengono utilizzati per diffondere falsità come è successo contro Zelensky.

Se a livello europeo, non solo quello italiano, c'è un leak riguardante dei documenti, questi possono essere modificati per attribuire a Zelensky la nazionalità russa anziché quella ucraina accusandolo di essere un Presidente illegittimo. Una delle fake diffuse contro di lui è stata proprio questa. Certe cose circolavano tranquillamente nel mondo degli ambienti No vax, o comunque complottisti della Covid-19, ecco perché sono luoghi fertili per la propaganda russa.

Facendo un passo indietro, il tema della privacy e della protezione dei dati personali l'ho riscontrata per di più durante il periodo pandemico. C'è stata una sorta di fiducia tra le persone e le varie piccole entità di cui vi accennavo prima. Per molti questa fiducia non c'era più nei confronti delle istituzioni, rivolta piuttosto a un personaggio che magari è anonimo, oppure che in qualche modo fa credere che li "difenderà contro i cattivi".

Ho riscontrato realtà formate da avvocati, medici, dentisti e infermieri che con la scusa di "curare la Covid con terapie alternative", basate magari su integratori o roba del genere, facevano in modo che i cittadini fornissero il loro consenso per diventare oggetto di studio.

Ho visionato dei leak di documenti, in formato Excel, dove all'interno c'erano nomi e cognomi di persone reali con indicato il loro status vaccinale, le informazioni sulla loro positività al Sars-CoV-2, quali sintomi hanno avuto durante la malattia, che medicinali sono stati forniti da quali medici. In alcuni casi, chi ha seguito questi malati non risultavano nemmeno abilitati a farlo.

Ho posto delle domande a chi ha condotto uno studio su questi pazienti, in particolare su come è stato presentato il consenso all'utilizzo dei dati sensibili, ottenendo questo risultato: non mi hanno voluto rispondere.

Come sono stati usati questi dati?

Quanto sono eventualmente ricattabili queste persone?

Oltre ad aver fornito i dati a questa entità, ho notato un eccesso di fiducia nei confronti di queste realtà, dove un gruppo di medici promette miracoli contro la malattia ma che per avere una precedenza rispetto agli altri pazienti devi iscriverti al loro comitato. Una volta iscritto, che fine fanno i dati personali? In questo modo un gruppo può vantarsi di avere 10.000 o 30.000 iscritti attribuendosi di fronte al pubblico forza e autorevolezza, utili per poi fondare eventualmente un partito.

C'è troppa leggerezza, spinta in questo caso dalla disperazione, nel fornire i dati a entità del genere.

In parallelo, però, le stesse persone dimostrano e denunciano il timore che i propri dati vengano forniti ad altre realtà che magari risultano più strutturate e più controllate, che siano privati o le stesse istituzioni. Tra queste persone c'è chi ha paura di usare la tessera sanitaria perché convinte che "traccino qualsiasi cosa". Trovo assurdo che attraverso le bugie e le manipolazioni alcune realtà riescano ad ottenere un controllo di dati delicati con i quali possono sfruttare ulteriormente a proprio vantaggio, non solo dal punto di vista medico ma anche dal punto di vista eventualmente anche ideologico.

BALDO MEO

Se ho capito bene, quindi, diciamo la "macchina ibrida" usata per la pandemia poi si è trasferita in altri ambiti...

DAVID PUENTE

Non è che si è trasferita, è stata riutilizzata.

C'è un qualcosa che funziona, che ha funzionato per due anni, che non ha diffuso bufale nei confronti della Russia o dei vaccini russi. Parliamo di ambienti dove associano problematiche nei vaccini come AstraZeneca o Pfizer, ma per Sputnik?

Ho potuto leggere e raccontare i contenuti di alcune cartelle cliniche che riportano eventi avversi associati al vaccino russo, realtà che

non sono state raccontate pubblicamente in Russia. Sono state raccontate attraverso la diffusione di documenti all'estero da parte di un Whistleblower che voleva raccontare cosa stava succedendo in Russia.

Gli ambienti No vax e complottisti, utilizzati per diffondere notizie sull'invasione russa in Ucraina, non ne parlano. Sono all'interno di questi gruppi social, per capire come funzionano, come comunicano, che cosa raccontano, ed è un po' come entrare nella tana del Bianconiglio, una cosa spaventosa, dove non si contesta la Russia quanto piuttosto l'America, Bill Gates, Soros e compagnia, sempre gli stessi. Quindi per i russi è stato, come dire, un tappeto rosso: "il nemico del mio nemico è mio amico".

BALDO MEO

Se da una parte il fact-checker ha un ruolo di grande importanza, un tale ruolo è piuttosto difficile da svolgere, perché questa sorta di polverizzazione delle fonti a cui facevi cenno è complicata da seguire e contrastare.... .

DAVID PUENTE

Ci sono tante realtà e non è un problema italiano.

Durante la pandemia con i miei colleghi stranieri, circa una settantina in giro per il mondo, ci siamo messi d'accordo, abbiamo comunicato, ci siamo scambiati informazioni su quello che accadeva, notando che una bufala diffusa da un piccolo gruppo a Parigi o in Francia poteva diventare virale anche negli Stati Uniti o in Sudamerica. Tante piccole realtà che fanno rumore e che poi improvvisamente esplodono.

Siamo tenuti a capire cosa sta succedendo e a dover in qualche modo monitorare tutte queste reti, dovreste vedere uno dei miei cellulari dove tengo tutte le chat Telegram che monitoro, una lista di canali molto lunga e faccio fatica a gestire le notifiche.

Effettuo ricerche attraverso parole chiave, soprattutto quando mi segnalano un post sui social e scopro da dove è stata condivisa e in che maniera, trovando eventualmente l'origine in un canale Telegram russo o in uno francese.

Si può ricostruire un percorso che è stato fatto dalla “notizia”, ed è difficile perché ci troviamo di fronte a un mosaico composto da piccoli tasselli, in un certo senso spaventoso perché non sai cosa potrebbero inventarsi tra le varie realtà. Ci sono tante menti, non ce n’è una.

BALDO MEO

In questo discorso si intravede in sottofondo un convitato di pietra: i social media. E chiedo a Raffaele Barberio: se il fact-checker decostruisce notizie false, chi è che le costruisce?

RAFFAELE BARBERIO

La realtà e quelle sue deformazioni che puntano a scardinare la tutela dei dati personali

I social non presentano i fatti oggettivi, offrono senza apparente controllo ciò che gli utenti ritagliano e pubblicano su questo o quel canale.

Possiamo dire che in questo non vi sia alcun intervento più o meno rilevante di quella sofisticata intelligenza artificiale che si riconosce ai canali social.

Ciò che appare invece è la dualità tra realtà e rappresentazione, ben più antica della breve vita di internet rispetto ai modi in cui nel corso del tempo abbiamo dovuto affrontare questo tema.

Quante volte ci sarà capitato di vedere una rosa appena recisa in giardino, talmente perfetta da farci esclamare: “Che bella, sembra finta”. E quante volte ci è capitato di osservare una rosa di plastica o di stoffa, come quelle che si vedono in alcuni uffici sofisticati, fatta talmente bene da farci commentare: “Che bella! Sembra vera”.

È una metafora per dire che le cose non sono mai come appaiono. E volendo rimanere sul terreno delle metafore, spesso ci viene rivelato con clamore magari un inedito corso di eventi o l'avverarsi di circostanze in aperta contrapposizione alle regole del senso comune.

Anche in questo caso si ha la sensazione della ricerca della novità ad ogni costo. Ma non è così. Il mondo gira da sempre allo stesso modo e, forse proprio per questo, la prima regola è non fidarsi di quello che si vede. Le cose non sono quasi mai come appaiono.

Ora proviamo ad applicare questo punto di vista all'argomento del periodo ovvero lo stato attuale della guerra in Ucraina e le modalità attraverso viene rappresentata la realtà dei fatti dall'una e dall'altra delle parti in guerra.

Difficile immaginare che da una parte siano tutti bugiardi e dall'altra siano tutti cultori della verità. La guerra altera tutto, non solo i territori martoriati o la vita ordinaria delle persone, che viene completamente sconvolta.

Come affrontare e gestire le informazioni durante una guerra? Vista dal di dentro, una delle regole fondamentali è quella di screditare il nemico. Anche qui, non c'è nulla di nuovo.

Eppure, in queste settimane si sente parlare ininterrottamente di misinformazione, di macchina russa della bugia. Si tratta di affermazioni che rischiano a loro volta, esse stesse, di contribuire ad alterare la realtà e nascondono il fatto che l'obiettivo di screditare il nemico agli occhi dell'opinione pubblica nazionale e, ancor di più, internazionale è sempre stato una delle prassi fondamentali dello stato di guerra. Da ambo le parti coinvolte nel conflitto non si fa altro che interpretare un copione vecchio come il mondo.

Chi non conosce, del resto, le modalità di informazione internazionale ai tempi della Guerra Fredda?

Chi non ricorda l'epopea di Radio Free Europe, la radio della CIA messa in Germania, o The Voice of America, anch'essa in Germania da una parte, e Radio Mosca, dall'altra, che trasmetteva in 74 lingue?

Allora come oggi, l'obiettivo era screditare il nemico, con un'attività di disinformazione reciproca che è parte integrante dello stato di guerra e dell'uso di tutte le armi che essa implica.

Ma torniamo alla guerra in Ucraina, si legge continuamente di forme nuove di cosiddetta "guerra ibrida", ma in effetti ogni guerra è sempre stata ibrida, perché combattuta con ogni tipo di armi, da fuoco e culturali, reali e virtuali.

Quindi quando leggo o sento da giornali e tv di questa grande novità della guerra ibrida, mi viene da sorridere.

Ciò che invece è reale è un'altra guerra ibrida, ma non dichiarata,

che si combatte ogni giorno sulla rete, con l'estrazione dei dati dei cittadini di questa o quella nazione e che è finalizzata alla acquisizione di dati su cui si potrà esercitare prima un dominio commerciale e magari in seguito politico o addirittura di sorveglianza di massa.

Si tratta di una raccolta di dati fatta in un contesto di apparente consenso, perché le montagne di dati che transitano in rete per essere consegnati alle cosiddette terze parti sono volontariamente forniti con non poca superficialità dagli stessi utenti. Una singolare sindrome di Stoccolma in cui la vittima non si rende conto di cosa dà in pasto al proprio carnefice, ignorando la natura stessa di quest'ultimo.

Da questo punto di vista, i social sono la più grande macchina da guerra per la raccolta dei dati personali. Non c'è mai stata una macchina così bellicosa nella storia dell'umanità e tutto questo è avvenuto in soli venti anni o poco più. Per cosa si raccolgono questi dati? Certo la risposta sembrerebbe abbastanza scontata, ma ancora una volta le cose non sono come appaiono. Ci dicono che la loro raccolta è utile per interpretare meglio i gusti personali e offrire una migliore qualità di servizio. Ma non è così, perché anche questo obiettivo non è un fine ma un mezzo per raggiungere qualcos'altro.

E allora si raccolgono per far commercio di dati? Qui cominciamo a centrare la risposta. Sappiamo che Facebook non è nato per far comunicare le persone, ma per raccogliere dati. Sappiamo che Google non è fatto per offrirci un motore di ricerca, ma è fatto per raccogliere dati.

Sappiamo che Microsoft ci consente di inviare e ricevere mail, ma non appare il fatto che faccia incetta di miliardi di dati contenuti nelle nostre mail e usati nei modi più disparati. La stessa considerazione vale per la cinese TikTok o per il commercio di Amazon. Poi ci sono i player puramente informatici, come Oracle, che hanno perfezionato le modalità di estrazione millimetrica dei dati con tecniche fino a poco tempo fa inconcepibili. Da notare che i software di Oracle sono alla base dei sistemi di sorveglianza di massa in Cina. Un fenomeno allarmante che non riguarda solo la Cina o i regimi cosiddetti non democratici, dal momento che la città, dopo Pechino, con il più penetrante sistema di sorveglianza di massa è Londra, patria del primo Parlamento democratico della storia.

Quindi il modello di business sostanziale di queste aziende è innanzitutto raccogliere dati. A questo punto viene da chiedersi: a cosa servono questi dati e perché si raccolgono in questo modo così intensivo? La prima risposta, sostenuta da motivazioni commerciali, è che la loro raccolta consente a molte aziende di sviluppare il proprio business in modo più sofisticato e mirato, in forme fortemente personalizzate.

Vi sono al mondo centinaia e centinaia di società che attraverso i social raccolgono dati secondo filtri che vengono concordati con i social stessi.

Questi dati, una volta raccolti, diventano merce grezza o già lavorata per centinaia di società che utilizzano i dati personali raccolti su centinaia di milioni di persone. Sono i cosiddetti broker dei dati personali, che raccolgono, comprano, elaborano e vendono all'ingrosso e al dettaglio dati personali che vengono raccolti usando tutti i sotterfugi che la rete consente.

Vediamone qualcuna. Axiom, per esempio, che ha un database di un miliardo di persone al mondo, di cui conosce tutte le operazioni immobiliari. Un'altra, Corlogic, molto più piccola, fa più o meno lo stesso lavoro.

Ce n'è un'altra ancora, Equifax, che forse tutti voi ricorderete perché è stata oggetto di un attacco hacker che le ha sottratto i dati di alcune centinaia di milioni di persone. Addirittura Equifax ha una storia antica di raccolta dati, essendo nata addirittura a fine Ottocento. Infine la Nielsen stessa che ha sempre raccolto dati e che ha anch'essa oltre cento anni.

Si noti come, anche in questi casi, non c'è niente di nuovo, ciò che cambia è la modalità con cui vengono rese efficienti le modalità di raccolta dei dati. E qui emergono le straordinarie capacità del digitale.

Ma vorrei ritornare al mio invito iniziale a considerare che le cose non sono mai come appaiono. L'iniziale moto propulsivo dell'innovazione di massa, a partire dagli anni Ottanta, ha potuto contare su una narrativa convincente quanto affascinante, riportando le storie affascinanti di giovani fissati con la tecnologia, spesso privi di alcun titolo di studio, chiusi in garage di villette americane e capaci di costruire visioni e inventare soluzioni tecnologiche inedite.

Ma questa è la narrazione. Certo quei ragazzi erano in carne e ossa e avevano talento da vendere, ma le origini del miracolo tecnologico non stava nelle loro teste.

La tecnologia, tutta o quasi la tecnologia digitale di cui oggi facciamo uso, è figlia diretta dell'immenso sforzo di ricerca e sviluppo militare degli anni Cinquanta, generato a sua volta dalla Guerra Fredda tra USA e Unione Sovietica.

Lo scontro tra le due superpotenze era alimentato da una competizione sulla disponibilità di nuove armi e all'interno di questo processo possono essere collegate tutte le espressioni tecnologiche dell'epoca, dalla corsa verso lo spazio (sempre motivata da ragioni militari) alla produzione di chip capaci di assicurare capacità di calcolo sempre maggiori. La stessa Silicon Valley, nata all'inizio degli anni Settanta, non può che essere considerata come l'espressione industriale di quel moto e il successivo scudo spaziale di Reagan, che rappresentò l'inizio del tracollo militare dell'allora Unione Sovietica, confermò come il potere di una superpotenza potesse essere esercitato innanzitutto grazie alla tecnologia militare disponibile.

Naturalmente, lo sforzo di ricerca e sviluppo militare deve essere poi convertito ad usi civili. È un meccanismo inevitabile che consente di dare nuovo impulso alla struttura industriale, alla crescita economica, allo sviluppo di ogni nazione.

Il caso degli USA, letto attraverso i processi di crescita dell'economia americana in relazione all'impegno tecnologico degli apparati militari, è emblematico. Ad esempio, se guardiamo al Mediterraneo di oggi, il Paese con maggior capacità tecnologica e con un esercito (è il caso di dire) di startup capaci di trovare soluzioni applicative in ogni settore del vivere quotidiano, è lo Stato di Israele che, non a caso, è in una guerra ininterrotta dalla nascita della nazione a fine anni Quaranta.

Ma torniamo agli USA per vedere cosa è avvenuto più precisamente. È avvenuto che per decenni il cosiddetto Military Industrial Complex (MIC) ha esercitato un peso determinante nell'economia americana, orientando economia e relazioni internazionali, in un più ampio quadro di geopolitica.

Per il MIC fare ricerca e sviluppo militare era un must. E le acquisizioni tecnologiche provenienti dal settore militare hanno alimentato

un parco di conoscenze che ha iniziato a generare quelle innovazioni direttamente orientate all'uso civile che sono sotto gli occhi di tutti. Poi, a un certo punto, la tecnologia civile americana, cioè la Silicon Valley, ha cominciato a correre più velocemente, ma molto più velocemente del passo di marcia degli apparati di ricerca e sviluppo del MIC, al punto che coloro che stavano in Silicon Valley cominciarono a dire ai militari: "...Quel vostro progetto richiede venti mesi di lavorazione, ma se lo date a noi, riusciremo a completarlo in un quarto del tempo di lavorazione...", e si sono invertite le parti. Quindi la ricerca e sviluppo militare ha alimentato una tecnologia che ha iniziato a riprodursi e crescere autonomamente al punto da diventare supporto di quella militare, fino a prendere il controllo delle operazioni.

Oggi non è così facile distinguere i due segmenti, la tecnologia è unica e si distingue solo per famiglie di applicazioni nell'uno o nell'altro ambito. E, come è noto, vi sono cruscotti decisionali composti da rappresentanti dell'esercito e da rappresentanti dei Big Tech. Uno di questi cruscotti vede seduti allo stesso tavolo generali americani assieme a personaggi come Eric Schmidt o Jeff Bezos.

Alla luce di tali considerazioni, la guerra in Ucraina si colloca in un contesto che è meno piatto e meno scontato di quanto non appaia.

I dati, in questo scontro bellico, rientrano tra i proiettili più usati. Lo scontro nel dominio cyber è importante come gli attacchi della fanteria o lo sfondamento con mezzi blindati.

Nel contempo il fronte di guerra è ben lungi dall'essere limitato alla linea di confine tra Ucraina e Russia. In ballo vi sono equilibri ben più complessi: la composizione della Nato, i rapporti tra UE e USA, le dinamiche tra i Paesi in seno alla UE, l'autonomia di quest'ultima rispetto alle aspirazioni unipolari degli USA.

Il 18 aprile 2022, è stata fatta circolare negli USA, all'interno dei circuiti istituzionali anche se poi fatta trapelare verso l'esterno, una lettera firmata da Leon Panetta (ex direttore generale della CIA), Michael Rogers (ex direttore della National Security Agency), Frances Townsend (ex assistente al presidente dell'antiterrorismo della Homeland Security),

Michael Morell (ex vicedirettore generale della CIA), James Clapper (ex direttore della National Intelligence), James R. Clapper (ex direttore della National Intelligence), Jane Harman (ex membro della House Intelligence Committe), infine Jeh C. Johnson (ex segretario della Homeland Security). Sette firme eccellenti e tutte persone in pensione.

Ma nella cultura americana, quando hai prestato servizio in certi uffici, anche se sei pensionato rimani sempre un patriota e sei sempre un soldato.

Perché questa lettera?

Questi signori dicevano una cosa molto semplice: vi è il timore condiviso dalla maggior parte dei membri del Congresso e dal mondo delle istituzioni americane che il Digital Market Act europeo possa avvantaggiare solo potenti imprese statali o compagnie sussidiarie russe e cinesi, e chiedono pertanto che l'Europa modifichi il Digital Market Act. E nel corpo della lettera si facevano esplicativi riferimenti allo sforzo che le piattaforme americane stanno facendo per contrastare il nemico che minaccia i confini, l'economia, la cultura, stessa.

Ora, sette pensionati che dicono queste cose, si dirà, non fanno male a nessuno, ma il principio è che loro parlano al gotha della politica americana, e quello che loro esprimono è una pressione di forte intensità nei confronti dell'Europa perché modificasse un atto che in quel periodo era in fase di approvazione.

In questo modo, mettendo assieme armi convenzionali e piattaforme di rete usate per intrattenimento non si fa altro che “weaponizzare” la tecnologia. Tutta. E le stesse piattaforme si stanno “weaponizzando”, di fatto, per essere usate come un ingranaggio del meccanismo bellico.

In sostanza il significato di quella lettera aperta all'Europa è stato: europei, non rallentate lo sviluppo e l'azione delle nostre piattaforme, perché le nostre piattaforme sono necessarie per neutralizzare la disinformazione russa.

Il punto è che tutti fanno disinformazione e, pertanto, non si capisce perché usare l'occasione pur drammatica di questa guerra, in cui

l'Europa non è direttamente coinvolta, per legittimare operazioni di scardinamento del sistema normativo europeo.

Questa guerra ha in qualche modo ridimensionato l'autonomia europea, l'autonomia di un continente che è fatto di 500 milioni di cittadini che hanno i loro dati personali. Se l'Europa perde la propria autonomia o deve assoggettare le proprie prerogative alle esigenze di altre nazioni, cosa succede dei dati di questi 500 milioni di cittadini? Questo è il problema politico che noi tutti dobbiamo porre a noi stessi.

Per nostra fortuna, l'impianto normativo europeo sta reggendo, ma rimane sempre aperto uno scontro che è ben lungi dall'esser sopito. Abbiamo davanti a noi un mondo che è forse destinato al frazionamento regionale a causa delle spinte verso la deglobalizzazione. Continueranno, forse ancora per lunghi mesi a soffiare venti di guerra, ma indipendentemente da tale stato di conflitto, va salvaguardata la difesa della integrità dei dati personali dei cittadini europei, perché la loro protezione è alla base di alcuni principi fondamentali della nostra democrazia.

BALDO MEO

Grazie Raffaele Barberio: ha messo tanta carne al fuoco. Colgo la suggestione della “weaponizzazione” della tecnologia che mi pare una questione su cui occorre riflettere, questo finire nell'ingranaggio bellico da parte della tecnologia. Personalmente non sono così convinto che la storia si ripeta sempre uguale perché una macchina da guerra ibrida potentissima come sono i social non credo ci sia mai stata nella storia.

Do la parola ora a Massimiliano Panarari e gli domando qual è la sua visione, da sociologo della comunicazione e dell'informazione, dell'attuale situazione. Oggi l'informazione tradizionale, anzi meglio, professionale, è veramente così devastata dai social o ha una sua validità indipendente da certi strumenti?

MASSIMILIANO PANARARI

Per parafrasare il generale de Gaulle, si potrebbe dire che è una “vasta domanda”.

Buonasera a tutte e a tutti, e molte grazie per l'invito al Garante.

Credo che vi siano una serie di piani da affrontare in relazione a quanto evocato da Baldo Meo, e anche rispetto agli interventi precedenti che sono stati molto ricchi di spunti, tra loro molto differenti naturalmente.

Credo che vi sia un livello direttamente industriale che riguarda l'informazione, ovvero un piano - come si sarebbe detto in un'altra epoca, e come avrebbe detto un anziano signore con la barba - strutturale, dal quale naturalmente non si può prescindere, perché l'informazione è - come è noto - merce, quindi deve essere venduta esattamente come qualunque altro tipo di prodotto, e dall'altro è una componente fondamentale dei processi di costruzione della sfera pubblica. Merce, con riferimento alla prima dimensione, che viene (ed è stata) venduta in vari modi; ed è per questo che la Yellow Press e la stampa sensazionalistica della New York di fine Ottocento sosteneva, per fare un esempio, che a Coney Island erano stati trovati i fossili di un drago oppure di un unicorno, naturalmente per aumentare il numero di copie vendute.

Al tempo stesso, giustappunto, nell'affaticata società occidentale, l'informazione presenta anche e ancor più quella componente che si potrebbe definire per certi versi valoriale, che è stata evocata questa mattina dal Presidente e dagli altri componenti del collegio del Garante: ovvero, sostanzialmente a partire dalla diffusione delle idde dell'Illuminismo identifica un pilastro sul quale si è costruita la sfera pubblica.

Il nodo - come noto - è che oggi l'informazione di per sé stessa non risulta sufficiente per strutturare, dare forza e autorevolezza alla sfera pubblica. E, per giunta, risulta costantemente aggredita e sotto attacco da parte di molteplici soggetti, a partire dalle potenze ostili che ricorrono agli strumenti della guerra ibrida e della cyberwar.

Ma, più in generale, anche da parte di altri attori, come le potenze economiche che oggi ritornano con grande frequenza all'interno dei ragionamenti svolti in questa giornata, e determinano una spinta alla privatizzazione dello spazio pubblico e all'orientamento del discorso pubblico, da cui deriva un indebolimento della sfera pubblica.

Un ulteriore elemento riguarda il lato degli utenti, nel senso che consapevolmente o inconsapevolmente la trasformazione dell'informazione va nella direzione di un'orizzontalizzazione e di una partecipazione totale di ciascuno di noi a quella che non è giustappunto più la sfera pubblica nell'accezione classica della modernità, ma coincide, nella migliore delle ipotesi, con una "sfera pubblica interrelata", alla quale partecipano soggetti straordinariamente diversi rispetto a quelli della sua genesi illuministica e che arriva "intatta" in tale forma sino alla Prima guerra mondiale.

È proprio il conflitto del 1914-'18 a proiettare le popolazioni coinvolte in seno a una dimensione di tecnicizzazione e scientificizzazione della propaganda inaudita e inedita rispetto al passato, che porterà in seguito soggetti tra loro diversi, e non più esclusivamente poteri statali e pubblici, a competere per la conquista di un consenso che è non più condiviso e va frammentandosi, e questa costituisce l'ulteriore, profonda differenza.

Se si osserva quanto si è tradizionalmente chiamato il discorso pubblico, che era sostanzialmente governato, strutturato e reso omogeneo dagli operatori dell'informazione (a partire dalle gazzette della rivoluzione francese, della rivoluzione americana e delle grandi rivoluzioni liberali), si trova che quel piano condiviso in maniera naturale è saltato e il linguaggio del discorso pubblico non risulta più omogeneo, mentre tutti quanti competono all'interno di quello che dovrebbe essere un luogo di condivisione, di formazione dialogica, la celebre sfera pubblica nella definizione habermasiana.

Si tratta, potremmo dire in senso letterale, di una condizione di competizione, in primis nell'ambito dell'economia dell'attenzione, uno dei grandi nodi di fondo che hanno minato la forza condivisa e la capacità di costruire un discorso pubblico condiviso da parte dei soggetti informativi. Un'economia dell'attenzione nell'ambito della cui competizione troviamo la grande stampa cartacea, ma anche e soprattutto oggi una fortissima spinta da parte di Tik Tok, per fare un esempio.

E allora se leggiamo una notizia su un giornale cartaceo o anche sull'homepage di quello che viene chiamato un giornale mainstream per

esempio a proposito della siccità, possiamo paragonarlo ai - qui sto un po' banalizzando per cercare di essere esplicativo naturalmente - possiamo paragonarlo al balletto di un gatto ammaestrato su Tik Tok? In tutta evidenza, la risposta è negativa. Ma, giustappunto, tutti questi soggetti e attori mediali competono in modo equivalente ("orizzontalizzato") sul mercato dell'economia dell'attenzione. Perché - e questo è un altro piano significativo di cui si deve tenere conto - quella che si è disgregata è, chiaramente, la dimensione dell'autorevolezza.

Non è un problema nuovo. Per trovare una data simbolica - molto discutibile naturalmente come tutte quelle adottate per evocare i turning point - si può ricorrere alla messa in crisi dell'autorità del postSessantotto, effetto dei processi di ipersoggettivizzazione e iperindividualizzazione che giungono, naturalmente rilanciati con ancora maggiore forza, sino ai nostri tempi.

Questo processo ha reso sempre maggiormente difficile trovare uno spazio culturale e simbolico condiviso al quale tutti quanti attribuiscono la stessa valenza di autorevolezza. Ecco, se possiamo dire che all'interno di questo magnifico salone torinese dove si sta svolgendo il convegno è verosimile che le persone presenti individuino come autorevoli fonti tra loro molto simili (se non direttamente tutte le stesse).

Il problema, invece, è che "là fuori" questa condivisione dell'idea dell'autorevolezza non esiste più, ma senza di essa si rivela estremamente difficile, se non decisamente impossibile, abitare collettivamente uno spazio pubblico. E, difatti, lo si può malauguratamente misurare a ogni livello delle infrastrutture immateriali della nostra società.

Si pensi alla scuola pubblica e alla disgregazione che essa sta subendo da tempo, un processo alimentato da questioni di ordine sociale come ben noto, con un'esasperazione delle disuguaglianze che produce un analfabetismo di ritorno.

Esiste oramai una palese difficoltà nel disporre di strumenti culturali davvero condivisi, perché a essere entrata in crisi è stata proprio l'idea di una sfera pubblica e del riconoscimento dell'autorevolezza insieme alla modalità tradizionale di trasmissione del sapere.

E, dunque, servirebbe una chiara consapevolezza del fatto che

quella innegabile e significativa opera di democratizzazione collegata al processo di orizzontalizzazione dei media evidenzia, altresì, naturalmente anche una dimensione assai problematica (e, anzi, “avvelenata”). Se tutti quanti partecipiamo allo spazio pubblico non sulla base di una condivisione di percorsi formativi, non sulla base dell'accettazione delle medesime “regole d'ingaggio”, non sulla base del riconoscimento dei sistemi esperti, la sfera pubblica già frammentata va verso la decomposizione e una sorta di deriva totale.

Certo, a integrazione di questi ragionamenti, non ci possiamo nascondere il fatto che anche alcuni degli specialisti portano una loro parte di responsabilità, e lo si è visto a proposito nel discorso pubblico sui media digitali in occasione della pandemia in cui ci siamo illusi per una fase iniziale significativa che, nel contesto tragico, si trattasse anche di una finestra di opportunità di riattribuzione di credibilità da parte dell'opinione pubblica ai virologi, agli infettivologi, agli immunologi e, più in generale, agli esponenti del sapere scientifico.

Ma si è dovuto anche assistere a un loro rapido assoggettamento nei confronti della logica mediale, anche per una serie di dinamiche psicologiche individuali molto accentuate (la ricerca della pubblicità e della visibilità personale), che ha condotto gli esperti a “orizzontalizzarsi” e prestare il fianco a una serie di critiche.

Qui si banalizza un po' naturalmente, ma se un autorevole infettivologo si presta a farsi intervistare sulla sua visione dell'amore e della fedeltà coniugale, e svariati di loro ci raccontano su un settimanale patinato come passeranno le vacanze d'agosto nel momento in cui, ancora fino a non troppo tempo prima dicevano che in vacanza sostanzialmente non ci si sarebbe dovuti andare per evitare il ritorno del contagio, ecco che assistiamo a un adagiarsi e assecondare i meccanismi della logica mediale, collocandosi appunto al livello di chiunque altro (una sorta di paradossale “uno vale l'altro”).

Tutto questo accade anche perché il trasferimento della spinta propulsiva dei media, che competono per l'economia dell'attenzione, su un piano di spettacolarizzazione, risulta fortissima.

È quello che un filosofo tedesco-coreano - qualche volta un po' sopravvalutato ma che va molto ed è spesso interessante - Byung-Chul Han, chiama la società dell'intrattenimento. Nel senso che l'unico codice autenticamente universale (ovvero globale) oggi rimasto coincide di fatto con l'intrattenimento: attualmente è davvero questa la base della condivisione, sostitutiva dell'autorevolezza; e, chiaramente questo processo produce un contesto diverso, e, anzi, potremmo dire una sorta di temporale che si abbatte sulle nostre teste e sul nostro dibattito pubblico.

Qual è la funzione giocata dalle piattaforme rispetto a questa dinamica?

Un ruolo fortissimo, decisivo.

La nostra società piattaforma, la piattaformizzazione del dibattito pubblico, che tutto orizzontalizza e disintermedia, consegna lo scenario a una dimensione di equivalenza delle opinioni; è il famoso dibattito tra doxa ed episteme, con la prevalenza della doxa e una destrutturazione della fiducia e della credibilità.

Credibilità e fiducia sono due elementi che si pongono in una relazione dinamica, un rapporto che muta nel corso del tempo, e cambia con le infrastrutture materiali e immateriali del corpo sociale.

La nostra è una società - lo diceva David Puente - in cui decresce la fiducia, e quindi, per converso, anche la credibilità nei confronti delle istituzioni. Quelle istituzioni, come si è già avuto modo di dire nel corso di questa giornata di lavori, che sono associate fortissimamente col dibattito pubblico e con l'informazione e sono i pilastri della democrazia liberalrappresentativa.

A crescere, come contraltare, è in termini contestuali una forma non di credibilità generale e condivisa, ma di polarizzazione affettiva nei confronti di quelli che sempre David Puente chiamava piccoli gruppi amicali, piccole comunità, sfere di pari in cui entra in gioco la componente fondamentale della sfiducia nei confronti di chi è considerato altro da sé, perché collocato dal punto di vista della gerarchia sociale su un livello più elevato.

Ed ecco, allora, che tutto quello che risulta riconducibile a élite ed

establishment viene separato dall'essere portatore di sapere esperto e considerato alla stregua del portatore di una forma di privilegio sociale odioso e incomprensibile.

La sfera pubblica ha bisogno di una dimensione razionale, come evidente, e specie nel momento in cui la componente sentimentale e affettiva e, soprattutto, quella delle passioni tristi, come le chiamava Spinoza e, più recentemente, Miguel Benasayag, diventa l'unico vero propellente sociale, col rischio di potenziali implosioni.

Noi oggi, nella migliore delle ipotesi, viviamo in un contesto di "sfera pubblica interrelata", a cui partecipano soggetti qualitativamente differenti, e che va pertanto difesa come diga e come argine - e la protezione dei dati personali rappresenta appunto uno tra i più fondamentali di tali argini.

Ma andiamo anche, sempre di più, nella direzione di una moltiplicazione delle sfere pubbliche, che ci riporta per certi versi a uno stadio tipico della premodernità. Prima dell'illuminismo non c'era una sfera pubblica unitaria, c'erano molte sfere pubbliche, piccole, estremamente limitate, non dialoganti tra loro, caratterizzate anche da profonde disuguaglianze sociali.

Se la postmodernità in cui siamo precipitati da molto tempo a questa parte rappresenta anche, sotto vari profili, il ripresentarsi e il riproporsi di una serie di dinamiche caratteristiche del pre-moderno, l'odierna è precisamente una di quelle. Con la fondamentale differenza che allora non c'erano le piattaforme, mentre con esse oggi dobbiamo massicciamente fare i conti.

BALDO MEO

Grazie. Crisi di credibilità, crisi di fiducia, mancanza più un discorso pubblico...

Vorrei, a questo punto, ragionare con Federico Ferrazza su un preciso tema: vero, falso e virtuale. Esistono notizie fatte solo di percezione?

In altri termini, possiamo intendere il concetto di "virtuale" come pura percezione?

FEDERICO FERRAZZA

Ci stiamo concentrando molto sui social network, sugli algoritmi, su come veniamo manipolati e sul tentativo di manipolazione da parte degli algoritmi stessi o di forze straniere. Ma invito a una riflessione che forse fa il paio con quello che diceva Barberio poco fa (e cioè sul fatto che non c'è niente di nuovo): avete visto la televisione che cosa ha mandato in onda durante la guerra?

Mi riferisco all'informazione sulla guerra in tv o sui giornali. Quanto di più anti-deontologico possibile.

E la stessa cosa vale per il Covid. Io non penso il problema sia solo Facebook, Instagram, Tik Tok, Telegram.

Le fandonie che sono uscite rispetto all'efficacia del vaccino, al fatto che ci vogliono schedare, al fatto che siamo in guerra per conto di qualcuno o che l'Ucraina è nazione di nazisti al soldo dell'Europa o degli Stati Uniti per sconfiggere Putin sono uscite sui giornali, su testate registrate ai tribunali italiani. Non è che sono uscite sui social network.

Quindi prima di cominciare a trovare le colpe e le responsabilità nei social network o negli algoritmi forse mi guarderei prima in casa. E vedo che c'è molta disinformazione fatta su organi di stampa tradizionali che niente hanno a che fare con i social network. Poi penso che la disinformazione (non mi piace tanto parlare di fake news perché dire cosa è vero o meno è sempre abbastanza difficile), sia paragonabile a una pandemia.

E come si sconfigge una pandemia? Si sconfigge vaccinando le persone. Quindi secondo me l'unico modo per capire qual è l'efficacia di una campagna di disinformazione è capire poi su quali soggetti va ad agire, e purtroppo in Italia agisce su una cittadinanza abbastanza ignorante.

Si parlava di percezioni: c'è un bellissimo studio di Ipsos che ormai porta avanti da diversi anni, che si chiama "Perils of perception", quindi i rischi e i pericoli della percezione.

Nello studio si vede come l'Italia sia uno dei Paesi, se non il Paese, i cui cittadini hanno la maggiore distanza tra la percezione e la realtà, oltre al fatto che, secondo l'Istat, in Italia, tra i 30 e i 34 anni i diplomatici sono il 75%, la media UE è dell'84%; e nella stessa fascia d'età il 27,6% sono

laureati, siamo gli ultimi in Europa con la Bulgaria, la media UE è più del 40%.

Allora, quando si parla di disinformazione c'è anche chi ci crede alla false notizie, e meno cultura c'è nel Paese, e più la gente è portata a crederci.

Vi dicevo la ricerca di Ipsos: allora dal 2000 a oggi numero di omicidi nel nostro Paese è calato del 40% ogni anno.

Il 49% degli italiani pensa che sia aumentato; il 35% pensa che sia lo stesso; solamente l'8% risponde in maniera corretta. Gli italiani pensano che il 30% di chi abita in Italia sia immigrato.

La verità è che è solamente il 7%.

E rispetto ai musulmani, la domanda che ha fatto Ipsos è: ogni cento abitanti quanti musulmani ci sono in Italia? La risposta media era 20, la risposta vera è 4. E poi: quanti over 65 ci sono ogni cento abitanti? La risposta degli italiani è quarantotto, la risposta corretta è 21.

Il prossimo è un dato un po' più vecchio ma serve a proseguire nel ragionamento: quanti disoccupati ci sono oggi in Italia in cerca di lavoro? Secondo gli italiani il 49%, la verità è il 12%. Tutto questo dà un po' la misura di quanto noi siamo poco alfabetizzati e non solamente dal punto di vista digitale, e quindi quanto gli italiani siano un terreno fertilissimo per ciò che chiamiamo fake news o disinformazione.

È del tutto evidente che l'unico modo per contrastare tutto questo è cercare di aumentare la conoscenza, investire sulla scuola e, dall'altra parte - parlo del mondo dell'informazione - si dovrebbe lavorare molto di più sulla coscienza e sulla deontologia; mi ritrovo molto in quello che diceva Panarari quando parlava di intrattenimento, oggi l'offerta informativa dei giornali e delle trasmissioni televisive che fanno informazione è per lo più fatta e costruita con la logica dell'intrattenimento.

Perché quando si chiamano in tv le solite persone a parlare di guerra, di Covid, di Draghi, di Mattarella o di qualsiasi altro argomento, allora vuol dire che si sta costruendo un palinsesto informativo che è fatto come una puntata di Uomini e Donne o di qualsiasi programma di intrattenimento o varietà, e chiedo scusa agli autori di Uomini e Donne.

Quindi è intrattenimento puro.

Poi ci sono le responsabilità dei social. Io più che responsabilità ne osservo diciamo la struttura che sicuramente non è fatta per aiutare a combattere la disinformazione.

Tutte le piattaforme sono fatte per polarizzare le discussioni. Ogni video, foto, post, opinione, idea o qualsiasi tipo di contenuto, è infatti sempre messo al voto da un cuoricino, un retweet, un pollice in su o un commento. Ma la realtà è fatta di sfumature e complessità e una eccessiva polarizzazione non aiuta a un corretto svolgimento dell'informazione.

E poi c'è un'interessante questione anche biologica a supporto di tutto questo, che è la questione della dopamina. La dopamina è un neurotrasmettore che ci dà piacere ogni volta che riceviamo un attestato di stima o un'altra forma di consenso.

Sono stati fatti diversi studi per cui la gente poi passa del tempo a guardare se ha avuto un like, se ha avuto un cuoricino, se ha avuto un commento positivo sulla foto su Instagram perché tutto questo dà delle scariche di dopamina. Tutto questo per capire quali siano i meccanismi strutturali dei social network e come viene costruito poi tutto il sistema di ingaggio, di engagement, per dirlo all'inglese, che avviene in quei luoghi digitali.

BALDO MEO

Grazie a Federico Ferrazza, che ci ha fatto fare un salutare bagno di realtà: ci ha rimesso coi piedi per terra, dove c'è attrito, ci ha invitato a non dare tutta la colpa ai social e, magari, neanche troppo al "contagio emotivo", di cui sono portatori. Chiederei a Martina Pennisi, per concludere, una parola di conforto sul fatto che in fondo si può fare ancora informazione seria ed autorevole.

MARTINA PENNISI

Anch'io pensavo che poteva essere un buon modo per chiudere. Lo faccio in realtà rialacciandomi a quello quanto detto questa mattina nella sessione che ho moderato.

Nel panel era presente un rappresentante di Meta, l'ex Facebook, il

gruppo di social network più importante del mondo, che ha più di 3 miliardi di utenti, che era qui a parlare di come stanno cercando di innovare di sperimentare altri modelli di business. immaginando e costruendo il Metaverso.

Noi, giustamente, siamo qua ancora a interrogarci sull'effetto che le piattaforme di social networking hanno avuto e hanno tuttora sull'informazione.

E in questo senso l'informazione, il lavoro dei giornali e dei giornalisti non è molto diverso da quello dei regolatori, dei legislatori di fronte all'innovazione e la tecnologia.

Faccio un rapidissimo esempio: chi fa desk, quindi chi è dentro le redazioni e non è fuori a seguire gli eventi come questo, ha tutta una serie di tool di programmi in cui vede dei dati in tempo reale, quindi vede come le persone reagiscono ai contenuti in rete, perché l'engagement è ovviamente un dato sulla reazione degli utenti, su come stanno funzionando i contenuti delle testate concorrenti. Ebbene, a questa macchina del gioco delle slot, sono esposti anche i professionisti dell'informazione.

E tuttavia, per le piattaforme i giornali sono stati una spina nel fianco, lo sono tuttora per questioni legate al copyright, e tutta un'altra serie di ragioni legate alla verifica dei fatti.

Questi sono aspetti di cui tener conto, di cui stiamo analizzando l'evoluzione tenendo conto che il futuro è una continua rincorsa e noi dobbiamo fare filtro - noi professionisti del settore - senza lasciarci troppo trascinare da questa disponibilità continua di dati e informazioni, i cui effetti sono stati benissimo spiegati anche in questo panel e risultano abbastanza chiari.

BALDO MEO

Grazie Martina, ci volevano queste tue parole dopo tanta problematicità.

Chiudiamo con un'ultima riflessione di David Puente e poi lasciamo la parola al dottor Ghiglia per i saluti.

DAVID PUENTE

Facendo un po' una riflessione finale. Con Open mi occupo della verifica dei fatti all'interno del social network Facebook, quindi quando qualcuno di voi condivide qualcosa di falso potrebbe trovarsi la notifica "Questa è una notizia falsa" o "parzialmente falsa" o al quale "manca il contesto", una notizia verificata da un fact-checker indipendente che fornisce un articolo dove vengono spiegate tutte le problematiche.

Questa pratica la vedo come una sorta di azione propedeutica, dove non c'è censura, ma un avviso e l'intenzione di spiegare che cosa sta succedendo e che cosa è stato diffuso in maniera errata. Ce l'abbiamo tanto coi social network per vari motivi, nessuno è perfetto, però rendiamoci conto che sono dei mezzi. La bugia c'è sempre stata, le bufale ci sono sempre state, la propaganda c'è sempre stata, cambiano i mezzi, cambiano i metodi, cambiano anche gli studi di quello che facciamo, di queste nuove realtà, però non vorrei demonizzarle del tutto.

Attività come quelle che faccio possono dare una mano, ma non sono sufficienti: il fact-checking non è la soluzione, è uno strumento in più per combattere questo sistema malato. Dico malato per dire proprio un'esagerazione. Però vorrei uscire da questa discussione dicendo che è un po' responsabilità di tutti noi, ognuno di noi è responsabile di quello che condivide, ognuno di noi è responsabile di quello che racconta agli altri, perché tutti quanti voi in questa sala avete una credibilità nei confronti delle persone che vi seguono, come quello che possono essere anche i famosi influencer o i virologi che parlano in televisione, però ognuno di noi nel nostro piccolo è responsabile.

Possiamo anche "arrabbiarci" contro le piattaforme e contro certe realtà, però se ognuno di noi fa la propria piccola parte nella lotta contro la disinformazione, come lo facciamo noi fact-checkers, non sarebbe male.

BALDO MEO

Grazie David. Questo è anche quanto da sempre raccomanda il Garante: bisogna che anche noi utenti ci responsabilizziamo, per usare in maniera consapevole i nuovi strumenti che la tecnologia ci offre.

Chiudiamo qui questa sessione ringraziandovi per l'attenzione e lascio la parola al dottor Ghiglia.

AGOSTINO GHIGLIA

Grazie, grazie a tutti.

Nel ringraziare la Società Eventum e la dottoressa Giani per la splendida organizzazione vorrei rubarvi ancora due minuti con un contributo, un nostro spot, è stato il primo spot di questo nuovo Garante, non per festeggiare i venticinque anni ma per ricordare un po' quello che è stata la nostra missione fin dall'inizio cioè, come dicevamo questa mattina, proteggere i dati delle persone, quindi proteggere la nostra libertà.

Grazie a tutti anche per la pazienza, per l'attenzione, per l'intelligenza con cui avete seguito questo nostro evento.

E non vi dico che ci rivedremo tra venticinque anni, spero di rivedere molti di voi molto prima ma sicuramente ci sarà ancora necessità, anche fra venticinque anni, di un Garante rinnovato, di un Garante presente, di un Garante un po' scudo delle nostre libertà personali.

