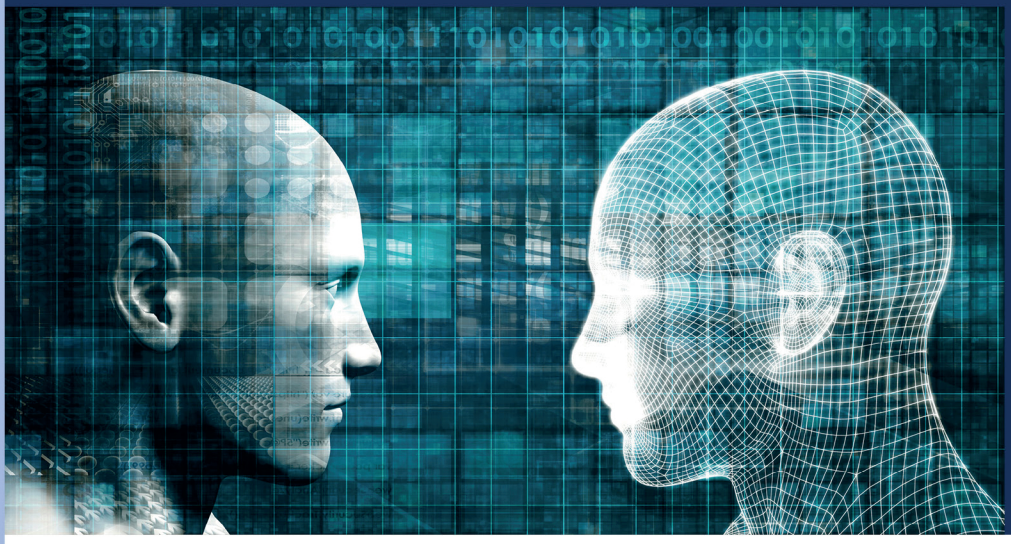
Fabio Lazzini

Etica digitale e Intelligenza Artificiale

I rischi per la protezione dei dati

Prefazione di Ginevra Cerrina Feroni



Giappichelli

Prefazione

Il Garante per la protezione dei dati personali come Garante dell'Intelligenza Artificiale

di *Ginevra Cerrina Feroni*

1. Premessa

Lo sviluppo dell'Intelligenza Artificiale è inquadrabile in una tendenza ormai consolidata da decenni: i dati in circolazione e le prestazioni dei sistemi che li trattano sono in aumento esponenziale, ma, al contempo, si assiste a una costante riduzione dei costi da sostenere per memorizzarli e analizzarli. Per averne un'idea, basti pensare che ogni due anni il volume dei dati trattati nel mondo raddoppia, mentre il costo per ottenere le stesse prestazioni da una macchina si dimezza. Questo processo è inarrestabile e l'effetto che oggi rileviamo di questa tendenza è la capacità delle macchine di funzionare attraverso algoritmi che non necessitano di una supervisione dell'uomo.

Non possiamo prescindere da questo elemento se vogliamo comprendere per quale motivo, rispetto al passato, l'Intelligenza Artificiale, e in particolare il *machine learning*, rappresenti oggi una rottura di paradigma: qualcosa che cambia le nostre consuetudini e le cambierà per sempre. Grazie alla crescente disponibilità di informazioni e allo sviluppo tecnologico, infatti, la macchina non ci consentirà soltanto di ottenere dei risultati attraverso l'elaborazione dei dati con cui viene alimentata e sulla base di una teoria sviluppata dall'uomo, cosa che facciamo già da decenni, ma renderà anche possibile estrarre il significato di questi dati e, questa la vera novità, lo farà in completa autonomia.

Dunque, la persona non si troverà più di fronte ad una macchina che si limita a svolgere compiti e analizzare dati sulla base di istruzioni assegnate, ma a una che decide, determina ed estrae senso dai dati

autonomamente. È proprio l'autonomia decisionale della macchina che, rispetto al passato, rappresenta l'elemento distintivo dell'Intelligenza Artificiale e su questo cambio di paradigma si sono concentrati principali interventi del legislatore europeo.

2. Intelligenza Artificiale e profili giuridici: il fondamentale ruolo del GDPR

L'Unione Europea ha invero iniziato il suo dibattito sull'Intelligenza Artificiale nel 2017 in modo piuttosto distopico, con la risoluzione del Parlamento europeo sulla robotica, che prevedeva la nascita di robot intelligenti autonomi ed evocava la necessità di attribuire diritti e doveri a queste nuove entità giuridiche. La stessa risoluzione invitava anche la Commissione Europea a considerare la creazione di un'agenzia per l'Intelligenza Artificiale e a stabilire un quadro politico globale per mitigare i rischi di questa potente tecnologia. Nonostante l'attenzione del Legislatore, parzialmente sbilanciata sui rischi dell'Intelligenza Artificiale piuttosto che sulle opportunità da essa derivanti, la posizione del Parlamento europeo, pur suscitando alcune reazioni critiche da parte della comunità scientifica, ha posto nuovamente (in seguito alla Convenzione 108, adottata in seno al Consiglio d'Europa nel 1981) l'Intelligenza Artificiale nell'agenda della politica europea.

Da quel momento, l'IA è stata oggetto di attenzione da parte di numerosi organismi e istituzioni. Ne sono testimonianza i vari documenti elaborati negli ultimi anni: testi normativi, ma soprattutto atti di *soft law* diversamente denominati. Tra i più importanti, è opportuno ricordare le "Linee guida relative ai principi sull'intelligenza artificiale" dell'*OCSE* (Organizzazione per la cooperazione e lo sviluppo economico) approvate il 22 maggio 2019, la Raccomandazione del Consiglio d'Europa adottata il 14 maggio 2019 e rubricata "*Unboxing artificial intelligence: 10 steps to protect Human Rights*" che, partendo dall'assunto per cui l'Intelligenza Artificiale può mettere a rischio i diritti umani, prevede in capo agli Stati l'obbligo di adottare determinate misure per ridurne l'impatto lesivo sui diritti delle persone. È invece del 2021 la Risoluzione del Parlamento europeo sull'Intelligenza Artificiale che affronta questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è coinvolta in impegni civili e militari, fino al passaggio epocale della presentazione del Rego-

lamento sull'Intelligenza Artificiale avvenuta il 21 aprile 2021 da parte della Commissione europea. Regolamento che, al momento in cui si scrive, è ancora in attesa di approvazione definitiva.

Quello appena delineato è uno scenario che negli ultimi anni è stato caratterizzato da una pluralità di fonti, variamente cogenti peraltro, che hanno disciplinano in modo frammentato singoli ambiti e tra le quali chi applica tecnologie IA doveva sapersi districare. Scenario che il Regolamento sull'IA, prima fonte a livello internazionale a disciplinare la materia in modo sistematico, muterà radicalmente.

In questo contesto disorganico, tuttavia, è opportuno ricordare come il Regolamento europeo n. 2016/679 (GDPR) si sia imposto, negli ultimi anni, quale principale riferimento normativo in materia di trattamenti automatizzati di dati personali, compresi quelli che hanno riguardato l'Intelligenza Artificiale. Una guida, dunque, per gli interessati e per le imprese che dovevano individuare dei principi cardine da seguire. Peraltro, anche la proposta di Regolamento sull'IA conferma che il cuore del sistema è da individuarsi negli strumenti già posti in essere dal GDPR e dalle migliori prassi della sua applicazione in tutta Europa: non esclusività, conoscibilità, sindacabilità e non discriminatorietà della decisione algoritmica e, non ultimo, il principio della *data protection by design*. Non è un caso, infatti, come il comitato europeo per l'Intelligenza Artificiale, che ha compiti di consulenza e assistenza alla Commissione Europea, sia composto dalle autorità nazionali di controllo nominate dai singoli Stati e proprio da quel Garante europeo della protezione dei dati, presieduto fino al 2019 dal compianto Giovanni Buttarelli, che ha il compito di monitorare e garantire il rispetto del diritto alla protezione dei dati personali da parte delle istituzioni e degli organismi europei.

3. L'esperienza ed il ruolo del Garante per la protezione dei dati personali

Che i principi del GDPR, come visto recepiti anche dal Regolamento sull'IA, abbiano svolto e possano continuare a svolgere un ruolo essenziale per la creazione di tale fiducia in una *disruptive technology*, qual è l'Intelligenza Artificiale, rispettosa dei diritti fondamentali, lo dimostra la costante attività degli ultimi anni del Garante per la protezione dei dati personali in tema di IA.

La competenza specifica acquisita dal Garante in questo ambito, quale vero e proprio regolatore, sulla base dell'interpretazione della disciplina in materia di protezione dati ed in particolare dell'art. 22 del GDPR, è comprovata dalla casistica, riguardante titolari sia pubblici che privati che si proverà a ripercorrere di seguito, attraverso l'illustrazione dei provvedimenti più significativi. Attraverso tale ricognizione si potrà saggiare come l'Autorità ha già indicato la strada da seguire per l'implementazione di una IA antropocentrica attraverso la normativa vigente.

3.1. Fisco e banche

A) Uno dei primi casi affrontati dal Garante, già nel 2013, ha riguardato il c.d. "*Redditometro*". Tale strumento di controllo si fondava sul trattamento automatizzato, tramite apposito algoritmo, di dati personali presenti nell'anagrafe tributaria, o comunque già conosciuti dall'Agenzia, al fine di selezionare i contribuenti da sottoporre ad accertamento e rideterminarne il reddito reale. In tale occasione, l'Autorità ha espresso parere favorevole sulla richiesta dell'Agenzia delle Entrate, definendo però le garanzie necessarie per il rispetto dei diritti degli interessati al fine di permettere che il trattamento di dati personali fosse effettuato dall'Agenzia delle entrate in conformità alla normativa privacy nazionale ed europea.

B) Sempre in ambito fiscale, sono poi da segnalare, in tema di *sperimentazione di procedure per l'individuazione di profili di evasione rilevanti* attraverso l'analisi dei dati finalizzata a riconoscere incongruenze tra le somme a disposizione del contribuente e i redditi e le spese desumibili dalle informazioni contenute nell'Anagrafe tributaria, i provvedimenti n. 320/2017 e n. 58/2019 nei quali, grazie alla interlocuzione avvenuta con l'Agenzia delle Entrate, sono state individuate, anche in questo frangente, le misure di sicurezza e organizzative idonee per fare in modo che il controllo tramite algoritmo fosse conforme alla protezione dei dati personali e, al contempo, efficace.

C) Nel 2016 è stata la volta della verifica preliminare richiesta al Garante da parte di un istituto di credito che intendeva utilizzare un *sistema di rilevazione di dati personali e biometrici basato sull'analisi comportamentale dei clienti durante la loro "navigazione" nell'area privata del proprio sito web*. Attraverso un sofisticato software in grado di registrare le attività dell'utente e la sua interazione con i dispositivi utilizzati, la banca intendeva offrire ai propri clienti un ser-

vizio ad elevato contenuto tecnologico in grado di innalzare i livelli di tutela e sicurezza rispetto a quelli originariamente previsti per l'utilizzo dei servizi di *internet banking* (*login* e *password* per l'accesso per intenderci), sempre più esposti al rischio di attacchi del tipo "*identity theft*" (furto di identità). Il Garante ha valutato positivamente la verifica preliminare, ritenendo lecite le finalità perseguite, le modalità di trattamento prospettate e indicando alcuni accorgimenti relativi all'adeguamento del sistema affinché fosse coerente col principio di proporzionalità e raccogliesse esclusivamente i dati necessari a garantire un livello di sicurezza maggiore all'utente. Le misure individuate dal Garante sono dunque servite a rendere il sistema ancora più funzionale rispetto allo scopo per cui era stato progettato.

3.2. Sanità e ricerca

D) Il Parere del 5 marzo 2020 al Consiglio di Stato in merito a un quesito sottoposto allo stesso Consiglio di Stato dal Ministero della salute e relativo ai nuovi criteri di ripartizione del Fondo Sanitario Nazionale (Fsn), che prevedono il trattamento di dati personali, anche sulla salute, di tutti i cittadini assistiti dal Servizio sanitario nazionale. Il Ministero della salute intendeva rimodulare il sistema di distribuzione delle risorse economiche dello Stato tra le Regioni. Tale rimodulazione presupponeva la profilazione dello stato di salute di ogni singolo assistito.

Il Garante ha rilevato che il progetto ministeriale risultava privo di una base normativa, necessaria invece per raggiungere gli obiettivi prefissati dal Ministero ovvero la creazione di un profilo individuale di ogni assistito, basato sulle patologie croniche e sulla situazione reddituale individuale, che, attraverso l'uso di algoritmi, avrebbe suddiviso tutta la popolazione in gruppi per omogeneità patologiche e reddituali. Il Consiglio di Stato ha poi accolto i rilievi del Garante, esprimendosi in senso conforme agli stessi.

E) Il Parere dell'8 maggio 2020 alla provincia autonoma di Trento sul disegno di legge provinciale concernente l'utilizzo dell'Intelligenza Artificiale sempre per una ingente attività di profilazione degli utenti nell'ambito della *medicina di prevenzione*. L'Autorità ha evidenziato gli specifici vincoli, in termini di protezione dei dati e trasparenza, che dovrebbero essere rispettati nel caso in cui tale attività di profilazione fosse stata realizzata attraverso l'uso di un algoritmo. Inoltre, richiamando il parere reso al Consiglio di Stato, sopra citato,

ha ricordato le necessità di effettuare una preventiva valutazione d'impatto sulla protezione dei dati.

F) Come dimenticare poi la costante e incessante attività con la quale, negli ultimi anni, il Garante ha presidiato l'attuazione delle *misure di contenimento della pandemia che prevedevano l'utilizzo di strumenti tecnologici e, in particolare, dell'IA*. Per citare solo un esempio, si pensi all'algoritmo messo a disposizione dal Framework A/G e utilizzato dall'app Immuni per il tracciamento dei contagi.

Nei suoi numerosi provvedimenti che hanno affiancato le misure adottate dai Governi in carica, il Garante è, in diverse occasioni, dovuto intervenire correggendo alcune "storture" che avrebbero potuto mettere a rischio la privacy dei cittadini senza, peraltro, che si configurasse un reale beneficio in termini di contenimento della stessa pandemia

3.3. Privati: Clearview e Delivery

Meritano inoltre di essere ricordati alcuni degli interventi più incisivi dell'Autorità relativi ai privati. Interventi che hanno tempestivamente permesso di scongiurare conseguenze ben più gravose per le persone interessate.

G) A marzo di quest'anno, il Garante ha imposto una sanzione di 20 milioni di euro alla società americana Clearview AI, per aver messo in atto un vero e proprio monitoraggio biometrico, tra le altre, di persone che si trovano nel territorio italiano.

La Società possedeva un *database* di oltre 10 miliardi di immagini di persone e di dati di geolocalizzazione estratti da fonti web pubbliche e offriva un servizio di ricerca altamente qualificata che, grazie a sistemi di Intelligenza Artificiale, consentiva la creazione di profili basati sui dati biometrici estratti dalle immagini, eventualmente arricchiti da altre informazioni ad esse correlate. Dall'istruttoria del Garante, attivata anche a seguito di reclami e segnalazioni, è emerso che Clearview, diversamente da quanto affermato dalla società, consentiva, appunto, anche il tracciamento di cittadini italiani e di persone collocate in Italia. Le risultanze hanno rivelato che i dati personali detenuti dalla società erano trattati illecitamente e che tali trattamenti ponevano ad alto rischio i diritti e le libertà fondamentali degli individui coinvolti.

H) A luglio del 2021, il Garante si è poi occupato di uno dei primi casi di evidente discriminazione per gli utenti derivante da determinazioni assunte da un algoritmo. L'Autorità ha infatti ingiunto

a *Deliveroo* Italia il pagamento di una sanzione di 2 milioni e 500 mila euro per aver trattato in modo illecito i dati personali di circa 8000 *rider* nell'ambito dell'utilizzo dell'Intelligenza Artificiale per l'assegnazione dei turni.

Dagli accertamenti effettuati era infatti emerso che Deliveroo analizzava la posizione dei propri fattorini attraverso la geolocalizzazione del dispositivo che utilizzava, acquisendo informazioni ben oltre il necessario per l'assegnazione di un ordine, come la posizione del rider ogni 12 secondi e la conservazione per sei mesi di tutti i percorsi fatti. La piattaforma segnalava inoltre ogni momento in cui il gps registrava uno scostamento di pochi minuti dei tempi stimati per il ritiro del cibo dal ristorante, lo spostamento del *rider* e la consegna al cliente. Il provvedimento è scattato a causa della riscontrata "mancanza di trasparenza degli algoritmi" che si alimentavano anche attraverso tali dati e che erano utilizzati per la gestione dei *rider*, l'assegnazione degli ordini e la prenotazione dei turni di lavoro effettuati, i quali comportavano il rischio di effetti distorti e discriminatori nei confronti dei rider stessi.

3.4. Istruzione

I) Il recente provvedimento relativo all'utilizzo del c.d. Sistema di *proctoring*, per la supervisione delle prove d'esame a distanza e l'identificazione degli studenti da parte di una nota Università. Il sistema prevedeva infatti il trattamento di dati biometrici (attraverso riconoscimento facciale) degli studenti al fine di poterne verificare l'identità (sia all'inizio della prova sia nel corso di svolgimento della stessa) ed evitare comportamenti scorretti, quali la sostituzione di persona.

Il video degli studenti che sostenevano la prova veniva analizzato con algoritmi di Intelligenza Artificiale che segnalavano comportamenti sospetti e valutavano la sessione d'esame complessiva in termini di probabilità che si fossero verificate violazioni degli esami. Il tutto avveniva tuttavia in violazione di diverse norme in materia di protezione dei dati personali a causa di evidenti vizi di trasparenza nella spiegazione delle logiche dell'algoritmo e nelle altre fondamentali informazioni da dare agli interessati (ad esempio, la possibilità che i dati venissero trasferiti negli Stati Uniti), nonché per la mancanza del consenso degli studenti al trattamento dei propri dati biometrici.

J) Infine, proprio pochi giorni fa, sono state richieste informazioni all'Associazione Crop News Onlus, in merito al progetto di *rating reputazionale degli studenti* delle scuole secondarie che la stessa sta ponendo in essere e che si basa interamente su algoritmi. Considerata la delicatezza del progetto che si rivolge a soggetti particolarmente vulnerabili (studenti e minori), il Garante ha chiesto all'Associazione di far pervenire entro 30 giorni chiarimenti utili a valutare se il trattamento dei dati sia o meno conforme ai principi previsti dalla normativa europea e nazionale.

4. Conclusione

Come dimostrato, gli interventi del Garante di questi anni sono stati caratterizzati da un approccio proattivo nei confronti dell'Intelligenza Artificiale. Un approccio volto ad estrarre da questa tecnologia gli effetti positivi per i cittadini e le imprese e mitigarne quelli dannosi. Le tecnologie non sono, infatti, intrinsecamente buone o cattive e non hanno lo scopo di migliorare la vita dell'essere umano o, al contrario, di coartarne la libertà. La tecnologia è neutra ed è l'uso che ne viene fatto che la connota.

È proprio l'uso che faremo dell'Intelligenza Artificiale che ne determinerà la sua connotazione in senso positivo o negativo ed è per questo motivo che una sua efficace regolamentazione assume un'importanza fondamentale. Sarà dunque da verificare quale sarà il testo definitivo del Regolamento IA e come verrà declinato l'aspetto della *governance* con riferimento all'Autorità competente. Quel che è certo è che non si potrà prescindere né dai principi del GDPR – considerato che la stessa Intelligenza Artificiale si nutre di dati e, in particolare, proprio quelli di natura personale – né da un ruolo centrale delle Autorità Garanti per la protezione dei dati a livello nazionale nelle decisioni strategiche complessive e nelle regolazioni settoriali. Infatti, ci troviamo di fronte a una sfida epocale per il mercato e per i diritti delle persone: estrarre tutto il potenziale positivo da una *disruptive technology*, qual è l'Intelligenza Artificiale, salvaguardando i diritti e le libertà fondamentali degli individui.

L'Unione Europea dovrà dunque essere in grado di sfruttare la prossima ondata di dati per sviluppare significativamente il *Digital Single Market* e al contempo costruire un «ecosistema di fiducia», che renda cittadini e imprese protagonisti di questo sviluppo. La tu-

tela dei dati personali non potrà che costituire uno dei valori fondanti di questo ecosistema digitale europeo e la proposta di Regolamento sull'IA, grazie alla sua impronta "umano-centrica" sembra andare proprio in questa direzione.

Nessun'altra Autorità e neppure una istituita *ex novo* potrebbe così come il Garante disporre di un patrimonio di conoscenza pratica e teorica tanto ampio rispetto all'applicazione limitata e garantita della tecnologia che contraddistingue la nostra epoca. Il Garante è il destinatario naturale delle norme della bozza di Regolamento europeo che fanno riferimento ad un'autorità di controllo da individuarsi come competente per la sorveglianza sull'applicazione del Regolamento stesso. L'esperienza maturata ci consente di disporre di una visione approfondita e versatile sul fenomeno. Le discipline di protezione dati e di limitazione del rischio IA saranno distinte e cumulabili, ma il tema, quello complessivo del digitale, della *governance* su di un'intera dimensione, è quanto di più distintivo e caratteristico della nostra azione: la sola, fra tutte le Autorità indipendenti ad aver intessuto sin dal principio un discorso istituzionale sulle tracce sia del diritto che dell'etica.

Nota dell'Autore

Un giorno le macchine riusciranno
a risolvere tutti i problemi, ma mai
nessuna di esse potrà porne uno
Albert Einstein

Parlare di etica e d'Intelligenza Artificiale (IA) è arduo, ma affascinante in un momento in cui le parole di Erich Fromm appaiono ancor più attuali, la civiltà sta producendo macchine che si comportano come uomini e, uomini che si comportano come macchine. Come potrà l'uomo non essere disumanizzato dalla macchina per dominarla, e renderla moralmente arma di progresso? Il problema se lo poneva già Giuseppe Ungaretti, con la consapevolezza tragica della complessità del rapporto tra l'uomo e la macchina, ma l'aspirazione a un governo antropocentrico e filantropico.

L'etica e l'Intelligenza Artificiale sono elementi determinanti per il successo e l'evoluzione dei processi di trasformazione digitale e per il progresso sociale ed economico del Paese. L'etica vigila sull'applicazione dell'IA e sulle relative conseguenze toccando un ampio ambito di diritti sia individuali che collettivi. L'essere umano attraverso l'attuazione dell'IA riesce a comprendere il mondo nelle diverse sfaccettature dell'ecosistema digitale.

L'Intelligenza Artificiale offre grandi e inimmaginabili opportunità di sviluppo e di crescita, ma al contempo, se non opportunamente governata e gestita, presenta rischi proprio per la protezione dei dati, e per le libertà e i diritti fondamentali degli individui. Il successo dell'attuazione dell'Intelligenza Artificiale passa sicuramente dal rimuovere questi limiti e vincoli, che potrebbero ledere i diritti e le libertà costituzionali dell'individuo, creando discrasie e discriminazioni per la libertà e dignità dell'uomo.

I rischi sono insiti al funzionamento della nuova tecnologia, si tro-

vano negli algoritmi alla base del processo decisionale, fondato sulle analisi e sulle valutazioni che riguardano l'affidabilità degli individui.

Diventa rilevante ai fini giuridici fissare norme, definire criteri e principi per disciplinare il complesso funzionamento dei sistemi d'Intelligenza Artificiale.

Occorre porre attenzione all'effetto dell'Intelligenza Artificiale sul diritto costituzionale e a come il giurista si pone di fronte alla complessa natura dell'algoritmo, in termini di trasparenza e protezione dei dati.

Il governo degli algoritmi è profondamente radicato nelle dinamiche informative del capitalismo estrattivo delle grandi piattaforme digitali, che influisce in modo rilevante sulla costruzione dell'anima, dell'Io della persona e sulla formazione, manipolazione e profilazione del pensiero della collettività.

Il punto su cui porre l'attenzione è come la distorsione informativa influenza l'individuo, nei suoi effetti sociali. Cosa può fare l'uomo per la tecnica e soprattutto, cosa la tecnica può fare per l'uomo? È qui che entra prepotentemente in gioco l'Intelligenza Artificiale, e prende corpo l'idea simbolica dell'automa. Lo sviluppo dell'Intelligenza Artificiale non può prescindere da un governo antropocentrico dell'innovazione, ma il diritto deve però dare un contributo importante se vuole agire e non subire l'innovazione tecnologica.

La sfida è nel definire il confine di fronte al crescente utilizzo dell'Intelligenza Artificiale, tenere conto che l'innovazione digitale e l'automazione tecnologica portano sempre con sé dei rischi, i quali devono essere opportunamente gestiti, per non creare sperequazioni ed iniquità sociali.

Altro rischio è la non neutralità dell'algoritmo, la cui progettazione, se non opportunatamente controllata, rischia di amplificare i pregiudizi a cui è assoggettata la mente umana.

La primaria struttura normativa è offerta dal GDPR – *General Data Protection Regulation* o Regolamento europeo n. 679/2016, poiché la tecnologia influenza la normativa e le policy ad essa applicata.

La normativa sulla protezione dati e i suoi principi sostanziali, secondo una declinazione consolidata del principio di trasparenza sono atti a minimizzare il rischio dell'opacità delle decisioni automatizzate, consentendo l'intervento umano nel processo automatizzato, per correggere eventuali errori suscettibili di produrre effetti pregiudizievoli. Quegli effetti discriminatori che sono insiti negli algoritmi che s'intendono utilizzare.

L'Intelligenza Artificiale, come generale capacità dei sistemi di risolvere problemi, è una tecnologia che esiste da molto tempo. Mentre lo sviluppo di soluzioni applicative di questa tecnologia ed in particolare il *Machine Learning* (apprendimento automatico) e il *Deep Learning* (apprendimento profondo), conseguenza di un certo tipo di programmazione delle attività basata su algoritmi, si è avuto solo negli ultimi anni.

L'Intelligenza Artificiale, il *Machine Learning* e il *Deep Learning* hanno come finalità l'integrazione dell'attività umana, lasciando al centro l'uomo e le sue prerogative.

Ecco come l'Intelligenza Artificiale ci aiuta a superare alcune delle sfide quotidiane del nostro mondo. Può, ad esempio, consentire ai medici di fare diagnosi più precise e perseguire nuovi percorsi terapeutici.

Nel cogliere queste nuove opportunità, si deve però garantire che il diritto alla *privacy*, all'autodeterminazione informativa e agli altri diritti fondamentali non vengano violati dall'uso dell'IA.

Le Autorità Garanti per la protezione dei dati personali e le Istituzioni Europee e Nazionali devono svolgere un importante ruolo di guida nella *governance* dell'IA basata sui dati, attuando un quadro di protezione dei diritti umani, democrazia di uno Stato sovrano, bene comune, libertà individuali e diritti fondamentali. Esse devono influire concretamente per lo sviluppo di sistemi che creino un clima d'innovazione per il benessere sociale.

La dignità umana deve essere un punto essenziale nella progettazione dei sistemi artificiali, i quali devono essere trasparenti, comprensibili e spiegabili. All'IA devono potersi pertanto applicare i principi di protezione dei dati concernenti la limitazione delle finalità, la minimizzazione dei dati, e i principi di liceità del trattamento.

Per tale motivo, parlare di etica e d'Intelligenza Artificiale non è semplice, specialmente quando al centro di questa rivoluzione umana si trovano gli individui con le loro necessità e i loro diritti costituzionalmente riconosciti.

Il progresso tecnologico, la progettazione e lo sviluppo di applicazioni informatiche sull'Intelligenza Artificiale, attualmente, rivestono e ricopriranno in futuro un ruolo fondamentale, nel tracciare l'evoluzione della nostra vita. Novità così importanti da poter sostenere l'uomo in ogni attività quotidiana e professionale. Il loro sviluppo in tanti settori diversi dovrà avere come limite un'elaborazione umanizzata delle informazioni, così da non assoggettare l'uomo alle regole del software intelligente.

Si può così affermare che l'obiettivo cui tende, o a cui dovrebbe

tendere l'innovazione digitale, è quello di uno sviluppo antropocentrico, ossia uno sviluppo che tiene l'uomo in una posizione di supremazia sulla macchina.

La visione antropocentrica deve tener conto della sicurezza dei dati, della *privacy* degli individui e dei loro diritti fondamentali. Ogni sviluppo tecnologico, basato sui processi algoritmici, deve avere un'influenza positiva sulla società. L'individuo deve essere sempre al centro, e la scelta e l'attuazione delle nuove tecnologie, anche di quelle legate all'Intelligenza Artificiale, deve obbligatoriamente essere funzionale alle sue esigenze.

Pertanto, la tecnologia dovrà modularsi sull'esigenze umane e sociali, come ad esempio la semplificazione dei processi burocratici o il miglioramento e l'ottimizzazione dei servizi pubblici offerti. Altro aspetto, quando si parla d'Intelligenza Artificiale, è l'utilizzo dei *Big Data*, che permettono di fare scelte sempre più consapevoli e ponderate, perché basate sui dati.

Un approccio etico all'uso dei dati e alle tecnologie è fondamentale per indirizzare l'innovazione tenendo conto dei principi di trasparenza. Perciò, i criteri che sottostanno alle scelte fatte dagli algoritmi devono essere sempre chiari.

La tecnologia deve prendere in considerazione i bisogni di tutti gli esseri umani e offrire benefici disponibili in eguale misura per tutti, cioè essere di inclusione.

Coloro che progettano e sviluppano i sistemi d'Intelligenza Artificiale devono operare nel rispetto e al servizio dei valori della società, ed essere responsabili.

Gli algoritmi devono operare e fare le proprie scelte (da qui l'imparzialità) e l'operato dei sistemi d'Intelligenza Artificiale deve essere affidabile. La sicurezza e la *privacy*, devono essere sempre un diritto tutelato e garantito a tutti i cittadini.

L'obiettivo da perseguire è il bene necessario per il progresso di tutta l'umanità. Occorre superare qualsiasi tipo di pregiudizio, che porta a plurime distorsioni dovute alla non corretta applicazione di regole da parte degli operatori finali.

Di qui la necessità auspicata di una regolamentazione europea per evitare le possibili distorsioni e, garantire così la sicurezza, secondo le linee della nostra Carta Costituzionale, ripresa anche dalla Carta di Nizza. Questo è l'approccio del Garante per la protezione dei dati personali all'uso dell'IA.

Solo in questo modo l'uomo non sarà disumanizzato dall'Intelligenza Artificiale, non sarà dominato, ma potrà utilizzarla per render-

la moralmente un'arma di progresso e di sviluppo. Se desideriamo agire e non subire l'innovazione dobbiamo evitare che la tecnica legga il nostro pensiero e lo renda trasparente. È pertanto chiaro l'approccio da perseguire: un uso delle tecnologie innovative in difesa di neuro diritti, da creare *ad hoc*, o da desumere dalle norme vigenti, perché sono la barriera necessaria all'uso improprio delle neuro tecnologie. Quindi, come espresso più volte anche dal Garante per la protezione dei dati personali è essenziale armonizzare e unire al progresso tecnologico e allo sviluppo dell'Intelligenza Artificiale la tutela dei diritti e della dignità della persona. L'obiettivo principale è creare un'IA affidabile e antropocentrica, credibile sul piano etico, così da fortificare e rendere più potente la nostra intelligenza emozionale. La persona umana non può essere schiava della macchina, ma deve restare una persona libera ed indipendente nelle sue decisioni.

L'IA ha un campo di intervento smisurato e se da un lato senza di essa non potremmo analizzare la grande quantità di dati che la società digitale produce, dall'altro è fondamentale indirizzare e governare quanto la stessa IA produce. La tecnologia è tra noi e con le interazioni sul nostro comportamento si sta sempre più evolvendo. È proprio la costante evoluzione a generare preoccupazioni circa la produzione massiccia di *fake news*.

Tecnologie diverse si combinano mostrando la loro interdipendenza e potenziandosi a vicenda: l'Internet delle Cose (IoT) ha bisogno dell'Intelligenza Artificiale per massimizzare e moltiplicare le proprie funzionalità; a sua volta, l'IA ha bisogno dell'IoT per raccogliere un numero crescente di dati da processare, grazie ai quali può prendere decisioni sempre più complesse. Entrambe, in egual modo, hanno bisogno delle reti 5G, come infrastruttura per veicolare i dati.

Le macchine possono essere i veri sensori e gli effettivi dispositivi di controllo dell'IA. Infatti, l'IA richiede ancora molta ricerca fondamentale e ha bisogno, se sviluppata nella pratica, di opportunità concrete su cui auto apprendere (ad esempio nel campo medico o in quello climatico per supportare modelli interpretativi). È anche necessario far sì che l'IA parli ai nostri settori produttivi per un avanzamento di qualità, che renda competitive le imprese modificandone anche i modelli di business e di sviluppo, per una ripresa e un'innovazione del Paese.

È importante essere consci del fatto che non si può vivere in modo disgiunto dai dati, perché ne abbiamo bisogno per analizzare e predire. La sfida del XXI secolo è la digitalizzazione e in particolare utilizzare sensori per raccogliere dati. L'IA, sostanzialmente, è uno

strumento che riceve dati in ingresso e fornisce informazioni in uscita, per prendere ed indirizzare decisioni. L'obiettivo è veicolare il funzionamento cognitivo dei sistemi artificiali, che si presuppone sia etico, per supportare le decisioni umane e, non sostituirle.

Altro aspetto è favorire l'incontro tra l'IA e la robotica, perché i dati sono creati anche dai *robot* e gli stessi hanno bisogno di informazioni per prendere decisioni. È necessario portare la potenza elaborativa di calcolo dove vi è l'effettiva necessità il più vicino possibile alle macchine.

L'IA non è mai artificiale ma è frutto di uno studio e di una ricerca dove al centro ci sono le persone su cui dobbiamo investire. Dobbiamo recuperare nell'innovazione i diritti e le libertà delle persone.

Ognuno di noi, nel mondo digitale, lascia tracce disseminate, che raccontano della nostra vita. Queste tracce, raccolte ed elaborate, possono influenzare il nostro comportamento e indirizzare le nostre scelte future, come ad esempio, per gli acquisiti, o per un'informazione relativa ad un ristorante o ad un cinema. Per generare questo tipo di sorveglianza dei comportamenti, è necessario distribuire dei sensori in luoghi fisici, così da poter valutare in modo circostanziale il flusso fisico-comportamentale dell'uomo e in seguito analizzarlo per bilanciare dinamicamente l'offerta. Non sempre questo bilanciamento avviene in modo diligente. Esistono dei rischi e rispecchiando il *risk based approach* del GDPR dobbiamo eseguire una valutazione.

In altre parole, l'IA è in grado di capire e comprendere i comportamenti ed influenzarli sia in senso positivo che negativo. Possediamo moli di dati che, se non vengono trattate in modo diligente, possono creare pericoli alla salute delle persone. Ad esempio, una bilancia che utilizza l'IA mi evidenzia di fare una dieta, senza controllo del medico. I sistemi di IA non possono essere utilizzati per ledere o mettere in pericolo diritti o libertà.

Il rapporto tra uomo e macchina è molto complesso. L'IA presenta un'infinita serie di vantaggi, come il miglioramento del lavoro, delle diagnosi e patologie delle malattie e così diventa un bene comune, che deve essere tutelato e governato. È possibile stabilire un confine tra l'uso consentito e non di strumenti come l'IA, mettendo delle regole e dei vincoli. Equità, dignità sociale, sono questi i pilastri su cui muoverci. L'algoritmo non deve creare discriminazione. È per questo che è importante tenere presente i principi definiti dal GDPR.

Oggi si assiste ad una sorta di deriva anti umanista che va raddrizzata e meglio indirizzata; le macchine tengono conto dei principi etici? Il confine e il limite a cui bisogna tendere implicano necessa-

riamente l'inclusione della componente umana e dei suoi principi nell'automatismo informativo degli algoritmi.

La convivenza tra uomini e macchine richiede quindi un nuovo approccio basato più su una dimensione umana la cosiddetta: algoretica. Ci si aspetta in tal senso un'IA più umana. È necessario però avere un approccio interdisciplinare per fondere i meccanismi dell'automazione con principi etici di comportamento e condotta (ad esempio nel supporto alle decisioni) poiché i risultati hanno effetti sulle persone.

Le domande sono tantissime. Come vivere ed affrontare queste sfide?

Spesso rappresentiamo la macchina come una entità che è rivale dell'uomo. Il robot come reale antagonista del genere umano. Il modello è per forza competitivo? Il modello italiano, sintetizzato nelle linee di sviluppo per l'IA elaborato dagli esperti del MISE, guarda ad un nuovo rinascimento secondo cui l'IA deve essere implementata, come un partner dell'umano, che possa aumentare le capacità umane, senza mai sostituirsi all'uomo. Come vivere questa sfida? Tornando sicuramente ad essere collettività, *polis*, piazza, facendo riecheggiare le domande per poi trovare delle risposte comuni.

Una successiva questione su cui soffermarsi è rappresentata dalla rete e dalle sue implicazioni. La rete come attualmente appare è un grande spazio, ovvero un luogo universale e immateriale costituito da utenti, che sono immersi in una sorta di coagulo di flussi perpetui e mutevoli nonché di operatori privati che si contendono la primazia sul digitale per aggiudicarsi il predominio dei dati e non solo. Il nuovo paradigma ci porta a leggere il mondo attraverso l'interpretazione delle informazioni.

Molto interessante è anche l'esame di quanto la grande migrazione *online*, imposta dalla pandemia ha accelerato ed ingigantito un processo, già in corso da anni, concentrando ancora più potere, ricchezza e influenza in capo alle *Over The Top*, ossia le grandi aziende, che distribuiscono i servizi della società della conoscenza, accumulano dati e monopolizzano i mercati del capitalismo digitale.

Le grandi piattaforme digitali sono capaci di esercitare prerogative tradizionalmente proprie dei poteri pubblici e condizionano i comportamenti di una moltitudine di persone. Le *Over The Top* contrattano al pari dei governi nazionali.

La domanda è quale natura gli Stati sovrani devono riconoscere a questi soggetti privati, che agiscono come operatori diretti, senza intermediazione dei governi, e sono in grado di contenere, gestire ed

elaborare un patrimonio informativo straordinario messo a disposizione per necessità degli Stati. Le piattaforme digitali sono i nuovi soggetti di diritto internazionale. Gli Stati sovrani devono scendere a patti definendo convenzioni, perché di fatto non possono non utilizzare i loro indispensabili servizi. In questa situazione lo Stato sovrano si trova con le piattaforme a rivendicare la pretesa di vedere rispettate prerogative, quali le imposizioni fiscali, la repressione del crimine e la protezione dei dati in uno spazio, che sfugge ai confini fisici della giurisdizione e al principio stesso di titolarità. Assistiamo ad una nuova geopolitica.

I sovrani privati dettano regole di *iurisdictio* e di esclusione e mettono in difficoltà il diritto pubblico e privato. Pure la stessa libertà di espressione in rete è una questione di grande importanza, infatti il costituzionalismo europeo ascrive la libertà di espressione al nucleo duro dei diritti inviolabili dell'uomo. In via teorica deve essere fatta una riflessione per rivalutare il diritto costituzionale inerente ai vari nodi impattati che hanno implicazioni anche sulla tenuta di un sistema democratico.

Abbiamo a che fare con una sorta di potere irraggiungibile, da parte delle grandi piattaforme digitali, sottratto ad ogni forma di controllo democratico. Soggetti di natura privata, censori della libertà costituzionale di espressione, che definiscono i confini eticamente e giuridicamente rilevanti dell'azione degli uomini.

Senza entrare in questioni geopolitiche è comunque opportuno evidenziare come l'IA possa indirizzare strategie nazionali da mettere in atto. Infatti, il report pubblicato dal CNR è un documento sullo stato dell'IA, in Italia ed in altri Paesi, ed è molto interessante in quanto rappresenta le posizioni aggiornate sul terreno del grande gioco internazionale sull'IA. Le nazioni più avanzate nel campo dell'IA si trovano in Europa Occidentale e nel Nord America. Gli Stati Uniti la fanno da padrone in virtù soprattutto della Silicon Valley e delle grandi aziende tecnologiche come *Google*, *Amazon*, *Facebook* e *Ibm* fondamentali per guidare e commercializzare la ricerca sull'IA.

Anche la Cina sta facendo forti investimenti nel mondo dell'IA, attraverso scelte strategiche, con un piano di sviluppo sfidante atto a far sì che l'IA diventi un importante motore della crescita economica sia in termini di competitività che di innovazioni tecnologiche costruendo così un robusto ecosistema di dati e ampliando l'adozione dell'IA nelle industrie tradizionali.

L'IA crescente e travolgente della Cina pone però interrogativi e preoccupazioni, legati al fatto che in un Paese governato centralmen-

te anche soluzioni basate sull'IA ma prive di limiti nell'azione e perfino a prescindere dai diritti e le libertà delle persone.

Il rischio concreto è che diventi un Paese di IA priva di responsabilità e di regole.

Una sorta di totalitarismo digitale con uno Stato autoritario che, avvalendosi di una mole sconfinata di dati pubblici e privati, può tracciare e valutare i comportamenti degli individui assegnando, tramite algoritmi, compensi e sanzioni, per condizionare la vita sociale ed economica degli individui e di fatto portare ad avere condizioni di condotte auspicabili dallo stesso Stato.

La visione cinese tende, quindi, ad avere una acquisizione completa dei dati, creare *report* sugli individui e a far sì che l'algoritmo e quindi l'IA porti ad una classifica, ad una profilazione dell'individuo e all'associazione di un punteggio personale (quasi fosse un credito sociale), influenzando la vita degli individui e diventando causa di potenziali, probabili discriminazioni.

Una IA non responsabile, insomma, può portare a una sorta di "capitalismo della sorveglianza di massa" indirizzando cosa può o non può fare un individuo e perdendo così parte della propria libertà a favore di un incremento di conoscenza da parte dello Stato.

La *privacy* e protezione dei dati diventa perciò baluardo ed elemento centrale nell'utilizzo etico dell'IA. Infatti, nell'ambito della protezione dati, in Cina ci potrebbero essere rischi significativi relativi all'implementazione dell'IA proprio per aspetti legati al tema sociale della sorveglianza di massa e di un controllo pervasivo con ricadute autoritarie.

Difatti, per avere un punto di incontro a livello di comunità mondiale nel mezzo di una trasformazione digitale che ci sta coinvolgendo tutti, la Cina sta perseguendo una serie di considerazioni e linee guida sull'etica dell'intelligenza artificiale, sottolineando l'importanza della protezione dei diritti dei cittadini e della prevenzione dei rischi di sicurezza informatica.

Una sorta di assunzione ufficiale di impegni per scongiurare i sospetti di un utilizzo indiscriminato e privo di regole delle informazioni personali dei cittadini. Resta da conoscere, se possibile, la coerenza tra dichiarazioni pubbliche di garanzia e rispetto dei diritti e i processi concreti di applicazione ed estensione dell'IA in ogni ambito sociale, economico e culturale in Cina.

L'Europa Occidentale ha un'alta concentrazione di strategie nazionali di IA supportate dalla strategia dell'Unione Europea. Il 24 novembre 2021 il Consiglio dei ministri presieduto da Mario Dra-

ghi ha adottato per l'Italia il Programma strategico per l'IA 2021-2024.

La tecnologia si sviluppa ed avanza in maniera vertiginosa, viene tutto ormai digitalizzato e reso automatico, e quello che appartiene alla nostra vita privata annullato e reso trasparente alle potenti piattaforme tecnologiche dove ogni cosa è tracciata e monitorata. Ritorna sempre più predominante la dicotomia tra sicurezza e *privacy* e, soprattutto l'antinomia tra ciò che è eticamente accettabile e realmente realizzabile.

Da quanto evidenziato scaturiscono riflessioni anche sul ruolo che deve giocare il Garante per la protezione dei dati personali, circa l'adeguatezza degli strumenti giuridici volti ad impedire alle grandi piattaforme digitali di trarre vantaggio dalle violazioni e dissuadere gli altri dal commetterle. È sostanziale che ogni risposta normativa adottata dalle Autorità Garanti per la protezione dei dati personali abbia al centro delle loro considerazioni i soggetti vittime di queste attività. I rimedi giuridici dovrebbero includere il risarcimento per i consumatori e i cittadini interessati, la responsabilità per le organizzazioni, condizioni di parità per le imprese e, la deterrenza di future non conformità.

I prossimi tempi saranno decisivi per approfondire se l'IA ha una coscienza e una consapevolezza umana tale da relazionarsi con l'individuo ed esserne parte attiva della propria vita.

Il funzionamento celebrale, visto in estrema sintesi, come la capacità di noi stessi di generare pensieri, fini, valori soggettivi e sensazioni potrà, davvero, essere riprodotto in maniera meccanica e auto deterministica da una macchina? Sembra inimmaginabile pensare di creare un essere che pur mostrando atteggiamenti e espressioni indistinguibili da quelli umani, senta e provi qualcosa come sente un individuo.

I sentimenti umani, lo stato emozionale della gioia e del dolore, propri dell'individuo come potranno essere governati da una macchina che pur intelligente che sia non ha quella capacità intrinseca di saper produrre e sviluppare impulsi di natura ed entità antropologica. La macchina auto apprende ovvero impara dalle informazioni che le sono fornite, si allena ed è per questo che può non essere neutrale, ma porta con sé quelle deviazioni volontarie o meno che indirizzano il suo operato.

Scegliere quali dati prendere in esame ed escluderne altri porta ad una soggettività della macchina e ad un condizionamento delle conseguenti azioni. Tali conseguenze possono influenzare l'uomo e cam-