Image

CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

L´INTELLIGENZA ARTIFICIALE FRA NORMATIVA EUROPEA E STRATEGIA NAZIONALE

Il presente contributo analizza i principi espressi dall´Ai Act in ambito europeo e la loro iniziale applicazione nel quadro normativo nazionale sotto il profilo strategico

di **Angelo Brofferio**
IUS/10 - DIRITTO AMMINISTRATIVO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Giovedì 7 Novembre 2024

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

This paper analyzes the principles expressed by the Ai Act in the european context and their initial application in the national regulatory frame work from a strategic point of view

Sommario: 1. L'Intelligenza Artificiale; 2. L'approvazione dell'AI ACT; 3. La struttura analitica del rischio; 4. La ratio dell'architettura normativa ed il rapporto con il GDPR; 5.La Strategia italiana per l'Intelligenza Artificiale 2024-2026; 6. La valutazione proattiva del rischio; 7. Conclusioni

1. L'Intelligenza Artificiale

L'Intelligenza Artificiale è una disciplina scientifica, che afferisce alla più ampia categoria dell'informatica, che studia, tanto sotto il profilo teorico che tecnico, il fenomeno dei sistemi informatici capaci di imitare le potenzialità ed il comportamento dell'intelligenza umana. Ne deriva che la similitudine rispetto al comportamento umano, considerato sotto l'aspetto razionale, diventa non solo pietra di paragone dell'intelligenza artificiale, ma anche l'unità di misura della sua efficienza.

Il pensiero considerato deve essere declinato come pensiero razionale, derivante dalle capacità cognitive e logiche dell'essere umano e tale da raggiungere il miglior esito razionale nella risoluzione dei problemi sulla base delle informazioni e strumenti disponibili. Il termine "intelligenza artificiale" fu formulato per la prima volta dallo scienziato John Mc Charty nel corso di un convegno tenutosi nel New Hempshire, presso il Dartmouth College, nel 1956, con un team di altri 9 importanti esperti della materia, quali Marvin Misky (che già aveva elaborato la prima rete neurale artificiale denominata SNARC) , che avrebbe dovuto dare vita, in tempi ragionevolmente brevi, ad un sistema informatico capace di riprodurre le capacità della mente umana anche in merito alla possibilità di apprendimento.

Un progetto del genere si scontrò inevitabilmente con una serie di difficoltà, in fase di applicazione pratica, che hanno richiesto diversi decenni di studio per avvicinarsi a degli esiti più aderenti alle ambizioni iniziali, tramite una serie di approcci concreti e progressivi in specifici settori di applicazione.

Una svolta decisa si è realizzata tramite l'adozione e la successiva evoluzione del linguaggio Python, molto più efficace nel realizzare algoritmi complessi, ed oggi la stessa

CamminoDiritto.it
ISSN 2421-7123

ChatGPT di OpenAI, sistema più innovativo fra quelli in essere, prende spunto da Python come modello linguistico di apprendimento automatico[1]. In particolare il modello GPT ha avuto un successo notevole, specializzandosi nell'utilizzo delle reti neurali per la generazione di testi, in un processo informatico che parte da un input testuale per realizzare un risultato testuale diverso e complesso, con una potenzialità di applicazione tendenzialmente illimitata.

L'esempio più evidente è, probabilmente, quello dato dal giornale canadese Globe and Mail che è diretto dalla intelligenza artificiale, ma nella vita di tutti i giorni abbiamo sempre più news elaborate dall'intelligenza artificiale ed un impiego sempre più pervasivo in svariati campi fra cui probabilmente spicca, come potenzialità, quello delle scienze mediche e della ricerca scientifica[2].

Pertanto, si è passati progressivamente da una intelligenza artificiale debole, in grado di riprodurre alcune funzionalità soltanto della mente umana (calcolo, statistica, previsioni) ad una intelligenza artificiale forte, in grado di raggiungere esiti molto più complessi tramite algoritmi progressivamente più elaborati e soprattutto in grado di implementare la performance ad ogni tentativo successivo, attraverso l'autoapprendimento e l'esperienza, tanto da iniziare a porre un vero proprio problema etico rispetto alla prospettiva per cui si potrebbe raggiungere un punto di non ritorno, nel caso in cui la stessa intelligenza artificiale possa sfuggire alle mani dell'uomo minacciando, addirittura, in un futuro, la sopravvivenza stessa della specie, come paventato dallo scienziato Stephen Hawking nel 2014.

Anche sulla base di queste considerazioni, si è tenuta nel 2017 la Conferenza di Asilomar sulla Intelligenza Artificiale, che ha coinvolto circa 800 fra i massimi esperti in materia, per affrontarne le problematiche etiche, sociali, culturali e militari, stabilendo, in un vademecum di circa 23 punti, alcuni principi fondamentali come quello di avere presenti, durante la ricerca scientifica, le finalità benefiche a cui deve tendere la nuova tecnologia, la valutazione delle implicazioni potenzialmente negative, la tutela della privacy, la programmazione, valutazione dei rischi e, soprattutto, una precisa applicazione del controllo umano a tutto il procedimento ed alle conseguenze che possono derivarne[3].

La profondità di queste riflessioni ha determinato la nascita del concetto di algoretica, intesa come valutazione etica della applicazione degli algoritmi e la necessità di un intervento normativo nazionale e sovranazionale che sovraintendesse al sistema complesso di applicazione delle nuove tecnologie. In ambito sovranazionale, la UE, nel 2019, ha avvertito la esigenza di dare vita ad un Codice Etico, elaborato da 52 esperti di varie discipline, che delinea delle linee guida in materia, ricercandone i fondamenti di ispirazione giuridica nelle leggi internazionali, nei trattati Ue e nei principi generali dei

CamminoDiritto.it
ISSN 2421-7123

diritti dell'uomo, avendo come stella polare del sistema il bene comune, inteso come obiettivo finale dell'utilizzo della tecnologia per implementare la libertà ed il benessere degli individui.

Nello specifico, si chiarisce che l'uomo deve, in primis, essere in grado di controllare e governare il sistema che, in ogni caso, è tenuto a garantire la responsabilità, sicurezza dei dati e delle persone e, più in generale, una governance trasparente ed efficiente minimizzandone i rischi. Il codice etico si concentra sia sugli aspetti tecnici che quelli normativi/sostanziali in ragione di uno sviluppo sostenibile della tecnologia che sia effettivamente compatibile con un principio condiviso di responsabilità, che dovrebbe costituire la cifra morale di un intervento così strutturale in una materia così invasiva rispetto alla vita dei cittadini europei. In sostanza vengono sviluppate delle linee guida finalizzate che sollecitano a favorire la non discriminazione, riservatezza e supervisione dell'uomo rispetto al fenomeno della intelligenza artificiale, che deve risultare servente rispetto alle esigenze ed alle autonomie dell'uomo e mai limitante rispetto agli stessi valori[4].

I sistemi di protezione possono riassumersi in una tensione generale di tutela della dignità umana che non può assolutamente prescindere dalla accessibilità, trasparenza e reversibilità della dipendenza dai dispositivi tecnici coinvolti nei processi neurali, in misura da tutelare la cifra etica di ogni fase del processo oltre che della sua intera completezza.

Nell'ambito di questa cornice normativa l'Italia ha elaborato, in prima battuta, il Piano Strategico per l'Intelligenza Artificiale per gli anni 2022/2024, che individua ventiquattro politiche atte a sostenere la competitività tecnologica della Stato come volano, anche a livello internazionale, di sostenibilità delle sfide tecnologiche e di sviluppo del paese a cui ha contribuito un gruppo di lavoro di esperti del Ministero dell'Università e della Ricerca, del Ministero dello Sviluppo Economico e Ministero della Innovazione tecnologica e transizione digitale.

2. L'approvazione dell'AI ACT

Il 09/12/2023 rappresenta una delle date storiche dell'Unione Europea, infatti, all'esito di un difficile e complesso negoziato informale che ha coinvolto i rappresentanti del Parlamento Europeo, del Consiglio e della Commissione (c.d. Trilogo), si è raggiunto un composito ed articolato accordo interistituzionale che è confluito in un testo finale che ha definito la normativa UE sull' Intelligenza artificiale, con impegno ad essere interamente completato entro la fine della legislatura, per poi entrare definitivamente in vigore entro i due anni successivi[5]. Il testo è composto di 85 articoli e 9 allegati ed entrerà pienamente

CamminoDiritto.it
ISSN 2421-7123

in vigore il 01.01.2026, mentre i produttori di sistemi di intelligenza artificiale avranno tempo fino a tre anni dopo (01.01.2029) per conformarsi alla nuova normativa.

Nel frattempo l'iter procedimentale ha previsto che, dopo il voto dei Rappresentanti Permanenti (COREPER) il 02.02.2024, la Commissione avrebbe avuto nove mesi di tempo per elaborare i Codici di Condotta. E' anche previsto che i sistemi di Ai open source per uso generale possano beneficiare di una esenzione rispetto alla applicazione del regolamento, pur rispettando la normativa sul copyright, a meno che non rientrino in una delle pratiche vietate previste dal regolamento stesso, in maniera da rappresentare un rischio sistemico o siano finalizzati alla commercializzazione, ovvero facciano uso di deepfake.

Si tratta chiaramente di una svolta epocale nel rapporto fra istituzioni e cittadini, in quanto la UE, per prima, potrà vantarsi di avere la disciplina più organica e dettagliata in materia e, soprattutto, attenta alla tutela dei diritti fondamentali e delle garanzie degli individui, sia come singoli che in un più complesso quadro collettivo ed istituzionale[6]. E' pur vero che questa disciplina giunge in ritardo rispetto a quella di altri stati come Brasile o Cina, ma non può non considerarsi che questa circostanza non sia dovuta a intoppi burocratici o conflittualità politiche, quanto piuttosto ad una complessa negoziazione derivante dall' attenzione che le istituzioni europee hanno ritenuto opportuno dedicare ad una materia così composita, pervasiva e ricca di sviluppi potenzialmente imprevedibili.

Anche per questo essa nasce come una legislazione in fieri, che già prevede degli aggiustamenti e momenti di successiva programmata ponderazione in fase di prima applicazione ed anche nei successivi archi temporali di medio e lungo periodo. Si delinea pertanto una dinamica normativa di bilanciamento fra rivoluzione tecnologica, innovazione e tutela della persona, nella consapevolezza che la natura stessa della materia implica delle incognite che necessariamente dovranno essere riconsiderate[7].

3. La struttura analitica del rischio

Le considerazioni sopra rappresentate hanno convinto il legislatore europeo ad assumere un atteggiamento assolutamente prudente, non perdendo mai di vista, considerata la innovatività del quadro normativo e sostanziale delineato, gli eventuali effetti indesiderati che uno scenario siffatto comporta, oltre che una finalità dichiaratamente proattiva, in grado regolamentare il settore, nell'ottica di migliorare la performance dei servizi. Tutto ciò ha delineato un approccio di studio basato sulla analisi del rischio che generalmente viene graficamente rappresentato in una forma di tipo triangolare/piramidale, divisa in sezioni, a cui corrispondono quattro categorie di gravità dello stesso.

CamminoDiritto.it
ISSN 2421-7123

Al vertice della piramide viene rappresentata la categoria del rischio inaccettabile, che corrisponde a quello che si qualifica come evidente minaccia per la sicurezza, per i diritti dei cittadini e comunque tale da realizzare o causare comportamenti pericolosi. E' chiaro che una siffatta categoria non può trovare un riconoscimento normativo e che, anzi, deve essere oggetto di un attento monitoraggio delle istituzioni preposte, al fine di non cagionare danni irreparabili al tessuto di diritto e sociale dei cittadini europei.

La seconda categoria considerata è invece quella del rischio elevato, che sinteticamente afferisce a dei settori sociali che implicano una attenta attività di vigilanza e di monitoraggio, in concreto, del rapporto costi/benefici. I settori sensibili sono anzitutto quello della giustizia per le ricadute che può avere sulla libertà delle persone ed i diritti dell'individuo, i diritti fondamentali della persona, i servizi pubblici essenziali, la gestione del rapporto di lavoro, la istruzione e la formazione[8].

E' di tutta chiarezza che trattasi di materie, di per sé stesse, qualificate come sensibili, in ragione della delicatezza dei dati trattati e delle ricadute che un erroneo trattamento e gestione di dati e processi potrebbe recare agli individui ed alla collettività. Va da sé che la relativa ricaduta, sotto il profilo dei limiti e delle cautele, passa attraverso sistemi di registrazione e tracciabilità e, sotto il profilo del potenziale danneggiato, attraverso l'obbligo di una preventiva informazione, con previsione di margini di sicurezza anche qualora vengano previsti meccanismi di automazione procedurale più o meno vincolanti.

E' emblematico il caso dei sistemi di identificazione biometrica, il cui utilizzo in spazi pubblici è tendenzialmente vietato per gli ovvi rischi che comporta e che, comunque, può essere ammesso, solo in casi tassativamente normati e codificati, in ragione di una esigenza di ordine superiore, che comunque deve essere volta per volta valutata, quale, ad esempio, la minaccia per la sicurezza in caso di pericolo terroristico o il perseguimento di un reato particolarmente grave, previa previsione normativa antecedente e successiva valutazione della Autorità Giudiziaria.

Si parla invece di rischio limitato nella misura in cui, secondo i canoni di ordinaria diligenza, l'utente è consapevole che una determinata attività implica l'interazione con un sistema automatizzato e quindi è altrettanto conscio del rischio che comporta lo svolgimento e/o il proseguimento dell'attività in corso, per cui ogni sua valutazione deve ritenersi, di per sé, adeguatamente informata.

Si ha infine il rischio minimo o nullo quando l'utente viene liberamente a contatto con applicazioni, inerenti la presenza dell'intelligenza artificiale, che derivano da una opportuna predisposizione su un mercato pienamente regolamentato, anche e soprattutto sotto il profilo qualitativo, così come avviene nella quasi totalità dei casi generalmente

CamminoDiritto.it
ISSN 2421-7123

affrontati nell'ambito operativo UE a livello commerciale, con un margine di rischio che per l'utente si concreta come più che minimale.

Lo sforzo dell' Ai Act è quello di mantenere un taglio pratico ed orientato ad una autoregolamentazione del sistema sulla base delle difficoltà affrontate. In questa specifica ottica, si sottolinea la centralità dell' apprendimento automatico per qualificare i sistemi di intelligenza artificiale rispetto a quelli informatici ordinari. L'autoapprendimento rappresenta il tratto distintivo di espressione delle potenzialità del processo telematico, ma, nello stesso tempo, il suo possibile limite potenziale di rischio, nella misura in cui sfugga al dominio dell'uomo e diventi, piuttosto che uno strumento, il fine stesso del sistema[9].

Queste dinamiche normative appaiono di tutta evidenza nel caso probabilmente più emblematico che è quello del social scoring (sistema che valuta il comportamento dei cittadini attribuendo loro un punteggio - qualificato come rischio inaccettabile), che viene sviluppato indipendentemente dalla dimensione sociale e/o economica dell'utente, rappresentando un limite invalicabile anche per le piccole o medie imprese (PMI), spesso più esposte in ragione di minori disponibilità di capitali e risorse da dedicare ai servizi di prevenzione, monitoraggio e tutela del rischio[10].

La valutazione dell'impatto del fenomeno, sotto il profilo sostanziale e normativo, è esponenzialmente più stringente a seconda della sensibilità del settore di riferimento. E' intuitivo che settori supersensibili quali quello della difesa, sicurezza interna e internazionale debbano essere esclusi dal campo di applicazione dei nuovi sistemi, in quanto il rischio, già insito nei processi automatici considerati, viene elevato a potenza, laddove ricerca e sviluppo debbano soccombere di fronte a interessi superiori ed esiziali per l'interesse dello Stato.

Deve essere delineato un delicato gioco di pesi e contrappesi (check end balances) che riesca a ponderare le esigenze di trasparenza con un profilo implementato di rischio a seconda della natura commerciale, strutturale o pubblicistica degli organi e degli interessi coinvolti. Tutto ciò implica una piena conoscibilità, per le istituzioni comunitarie, delle aziende che interagiscono nella ricerca ed applicazione dell'intelligenza digitale ed, in secondo luogo, la previsione, per periodi predeterminati, in un contesto protetto e monitorato, di ambiti di sperimentazione con test applicativi della norma (c.d. sandboxes).

Costituisce naturale corollario di quanto sopra descritto la previsione di un correlativo sistema sanzionatorio la cui incidenza, secondo le intenzione del Legislatore comunitario, si riduce a seconda della rilevanza organizzativa e strutturale del soggetto coinvolto, cercando tendenzialmente di escludere il più possibile PMI e start-up, per non causare un

CamminoDiritto.it
ISSN 2421-7123

laccio troppo rigoroso allo sforzo di innovazione digitale e, comunque, garantendo un sistema di reclami che possa comunque tutelare le ragioni degli operatori economici operanti sul mercato europeo.

A tale proposito viene prevista la istituzione di una autorità indipendente sia a livello europeo, con sede a Bruxelles, che nazionale, con previsione di sanzioni fino ad una massimale di 35 milioni di euro o il 7% del fatturato nei casi più gravi, oltre che la facoltà, per le legislazioni dei singoli stati membri, di prevedere regimi sanzionatori, anche più incisivi, fermo restando l'obbligo a livello UE di proibire entro 6 mesi (e quindi prima dei 24 mesi in cui il sistema dovrebbe entrare a regime) gli usi più pericolosi, già in una fase di prima applicazione. Non a caso c'è stata una unanimità di intenti e generale approvazione a livello europeo per il bando generale che ha riguardato, oltre che il social scoring, anche i sistemi in grado di elaborare emozioni o, comunque, tendenziali rispetto alla manipolazione dei comportamenti umani, oltre la previsione di una tutela rafforzata ed opportuni sistemi di tracciamento per evitare il fenomeno del c.d. deep fake[11].

4. La ratio dell'architettura normativa ed il rapporto con il GDPR

Sinteticamente, il precipitato normativo derivante dalla struttura analitica del rischio, come sopra descritta e declinata in una struttura piramidale, proporzionalmente collegata alla gravità delle sue relative categorie, ha delineato una impalcatura legislativa fondata su dei divieti assoluti e delle attività e processi, progressivamente consentiti, quanto minore risulti il rischio connesso alla stessa o, volta per volta, valutato.

A ben vedere, si tratta della stessa architettura normativa prevista per le ipotesi di legge di limitazione della libertà personale, con una batteria di garanzie piuttosto similari, che evidenziano le potenzialità lesive che il Legislatore riconosce a questi tipi di processi, con la relativa esigenza di tipizzarne l'utilizzo ed i limiti. Infatti, l'elenco dei reati che prevedono una identificazione biometrica da remoto ed in tempo reale sono piuttosto limitati ed afferiscono a materie come prevenzione di minacce terroristiche, traffico di esseri umani, gravi reati contro la persona, allo scopo di identificare il colpevole o prevenire la attuazione di un programma criminoso da parte del soggetto sospettato. Analogamente si qualificano dei dati che devono essere inseriti nella categoria dei dati sensibili, quali quelli che afferiscono a sesso, razza, religione, orientamento politico e condizioni personali o sociali, la cui rilevazione risulta assolutamente vietata, costituendo una sorta di nocciolo duro, che non può essere sfiorato dai processi di elaborazione ed analisi dei dati[12].

A questo stesso principio deve ricollegarsi il divieto di ricerca delle emozioni dell'individuo, soprattutto nel contesto lavorativo ed educativo, estendendo il concetto di

CamminoDiritto.it
ISSN 2421-7123

sensibilità non soltanto al dato in sé, quanto alla cornice sociale che consente di qualificarlo in categorie di rischio di volta in volta implementali. Analogamente, la sensibilità dei dati può essere connotata da particolari condizioni personali o sociali quali la minore età, la disabilità, il disagio economico personale, che qualificano il soggetto potenzialmente controllato come fragile e /o vulnerabile, innescando una serie di tutele e divieti aggiuntivi e non derogabili. In questo senso, appare pienamente aderente alla preventiva ponderazione degli interessi effettuata dal Legislatore europeo, il descritto divieto delle attività di social scoring, funzionali ad analizzare il comportamento umano allo scopo di manipolarlo, qualificandole come illecite.

La ponderazione fra i principi di trasparenza e privacy sembra apparire, analogamente, decisamente valutata a favore di quest'ultima, nell'ambito del divieto di scraping di immagini, che si sostanzia nella impossibilità di acquisire immagini dalla rete o sistemi analoghi, anche a circuito chiuso, utilizzando le cautele necessarie ad evitare potenziali abusi, quali quelli connessi alla profilazione individuale, piuttosto che su dati massivi e generali[13].

Il controllo biometrico, nei casi consentiti, potrà essere in tempo reale/ contemporaneo o post remoto, su dati già acquisiti, rigorosamente secondo i limiti di legge. Sotto il profilo dei poteri e limiti a cui sono soggette le forze dell'ordine, vale il principio generale di contemperamento degli interessi in atto, nella misura in cui, al fine di evitare abusi e consentire anche un monitoraggio in costanza di utilizzo dei processi di intelligenza artificiale, esse dovranno notificarne l'utilizzo alle autorità indipendenti preposte, che presiederanno alla trasparenza e correttezza del sistema.

Gli operatori e le aziende coinvolte nei sistemi di intelligenza artificiale, d'altro canto, dovranno garantire standard tecnici di sicurezza adeguati e soddisfacenti e, comunque, tali da minimizzare il rischio, garantendo, in ogni caso, un controllo ed una supervisione umana, tanto più severa, quanto più profilata di alto rischio, quali sono per esempio le attività che, potenzialmente, possano condizionare le libere elezioni o comunque possano incidere nello sviluppo e coerenza del sistema democratico. Gli stessi modelli utilizzati dagli operatori del settore dell'intelligenza digitale, utilizzano diversi strumenti che possono essere qualificati tecnicamente di alto, medio o basso impatto. Tali strumenti dovranno essere sottoposti a degli idonei controlli di sicurezza informatica e trasparenza della documentazione tecnica sulle caratteristiche degli algoritmi utilizzati prima di avere una approvazione all'immissione ed utilizzo sul mercato europeo.

E' opportuno rilevare come, ad un primo esame della normativa, sembri evidenziarsi un disallineamento dei fini fra la normativa posta dall' Ai Act ed il Regolamento Ue sul trattamento dei dati personali (GDPR). Difatti il GDPR, tendenzialmente, si riferisce ad

CamminoDiritto.it
ISSN 2421-7123

un utilizzo minimo di dati, fino a restringerne la cerchia a quelli strettamente necessari per il raggiungimento dello scopo istituzionale ed una conservazione per il più breve tempo possibile come garanzia della loro tutela[14]. Ciò appare tecnologicamente, prima che normativamente, incompatibile con l'intelligenza artificiale che, per essere performante, necessita del principio opposto della disamina e trattamento di più dati possibili, al fine di rendere l'algoritmo efficiente e competitivo fino al limite estremo dell'autoapprendimento.

Ma, a ben vedere, non si tratta di posizioni inconciliabili, ma solo di una diversa maturazione dell'approccio che passa, progressivamente, dal profilo quantitativo dell'insieme dei dati trattati, sia pure con distinguo della loro natura, a quello qualitativo della loro stessa natura, considerando il contesto, le finalità e le caratteristiche degli individui coinvolti. Si consente, in questi termini, un ottimale contemperamento degli interessi e costante attività di monitoraggio, che è oggi imprescindibile, vista la velocità e lo sviluppo esponenziale dei processi coinvolti, tenendo sempre presente il valore della dignità ed i diritti fondamentali della persona sanciti a livello europeo e costituzionale, che ne costituiscono il limite estremo di utilizzo e di legittimità[15].

5. La Strategia italiana per l'Intelligenza Artificiale 2024-2026

Nel corso del mese di Luglio 2024 è stata pubblicata la Strategia italiana per l'Intelligenza Artificiale 2024-2026, che è intervenuta sostituendo il precedente documento strategico, con un analogo orizzonte triennale, che era stato licenziato dal Governo Draghi nel 2021. Il piano decritto dal Governo Italiano fa seguito ad analoghi documenti di altri importanti Stati europei come la Germania e la Francia, testimoniando la necessità di una normazione che concreti ed armonizzi i principi dell'AI Act nel tessuto sociale e di diritto degli Stati membri, anche in considerazione del valore strategico che il settore della Intelligenza Artificiale ha acquisito negli ultimi anni. Infatti è assolutamente evidente che, in questo campo, il dato tecnologico e quello normativo sono eziologicamente legati fra loro.

I primi anni di questo decennio sono stati infatti testimoni di una presenza sempre più esponenziale degli algoritmi in tutti i processi sociali, sino ad arrivare a considerare l'impatto tecnologico degli algoritmi generativi che hanno iniziato a porre delle problematiche di uno sviluppo etico e sostenibile del fenomeno, che ha richiesto la genesi di un intervento organico prima a livello europeo e, successivamente, nazionale. in maniera sempre più dettagliata.[16]

Il modello italiano si è sforzato di regolamentare il fenomeno individuando tre fondamentali macro-obiettivi generali, quali sono quelli di uno sviluppo controllato e

CamminoDiritto.it
ISSN 2421-7123

sostenibile del sistema, l'incentivazione della ricerca e della formazione e l'efficientamento del settore pubblico, che si sviluppano in quattro macro-aree di intervento: Pubblica Amministrazione, Impresa, Ricerca e Formazione, che sono da considerarsi interconnesse ed interoperabili fra di loro, nonchè prevedendo, per ogni macro-area, apposti target e strumenti di monitoraggio del processo di sviluppo.

Quello che appare importante nella strategia nazionale è che, mentre l'Ai Act si fonda dichiaratamente su un risk based approach , quest'ultima, invece, considera il fenomeno della IA, ed in particolare quella generativa, come una opportunità, partendo dalla considerazione che la stessa avrebbe le potenzialità stimata di accrescere il PIL italiano del 18,2% annuo. Siamo pertanto presenti ad una rivoluzione di portata epocale, rispetto alla quale, rimanere meri spettatori o utilizzatori vuol dire segnare il passo a livello economico e sociale in una prospettiva strategica per il sistema nazione. Al contrario si è evidenziata l'esigenza di investire in infrastrutture ed applicazioni che rendano il tessuto sociale competitivo, se non addirittura attrattivo, per i talenti e le risorse umane impegnate nel settore.

Questi propositi si sviluppano nella PA attraverso l'utilizzo di infrastrutture e piattaforme, che consentano di implementare i servizi, garantendo, nel contempo, privacy e trasparenza. Nel settore della ricerca si ambisce ad un processo di innovazione tecnologica, attraverso la creazione di dataset ed addestramento su modelli open source. Nell'ambito della formazione sono previsti dei modelli di crescita, anche attraverso delle forme di partenariato pubblico-privato, avendo cura di uno sviluppo omogeneo delle conoscenze in materia che non crei uno squilibrio sociale ed anzi, possa accrescere il tessuto produttivo ed il mondo del lavoro attraverso dei ciclici percorsi di reskilling ed upskilling dei lavoratori, che rendano il mondo imprenditoriale sempre più performante e pronto ad affrontare le sfide che la IA inevitabilmente creerà sul mercato.[17]

6. La valutazione proattiva del rischio

Non può assolutamente passare inosservato che lo stesso profilo del rischio, che è architrave dell'Ai Act, viene rivisto nella Strategia nazionale sotto una diversa lente proattiva. Sotto l'aspetto appena considerato viene scolpito il rischio di una mancato sviluppo del settore del lavoro, sotto il profilo infrastrutturale e di idonea formazione del personale, che finisce per confluire nel rischio del c.d. digital devide, che realizza una disomogeneità del contesto sociale e lavorativo, pretendendo, in tal senso, che i progetti in materia di sviluppo della competenze di IA non siano mai frammentari o di natura estemporanea, per non avere un effetto divisivo. La effettività degli interventi dovrà essere garantita attraverso la previsione di dettagliati target e sistemi di monitoraggio (c.d. Rischio di inefficacia). Analogamente, un effettivo raggiungimento degli obiettivi

CamminoDiritto.it
ISSN 2421-7123

strategici potrebbe essere compromesso da un eccessivo intervento del Legislatore in materie fra di loro affini, anche attraverso le varie Autorità indipendenti dedicate per Legge (Garante per la protezione dei dati personali- AGCOM- ACN etc.).

E' evidente quindi il cambio di prospettiva, dall'impianto difensivo del rischio previsto dall'Ai Act, che ritiene prioritari i diritti dell'individuo nelle sue varie espressioni, rispetto a quello della strategia italiana, che valuta i profili di pericolo della over regulation sulla tenuta dell'impianto normativo, ma soprattutto, qualifica come il rischio fondamentale, il c.d. Rischio del non fare, che delinea un esito inevitabile di sconfitta strategica del sistema su tutta la linea, rispetto ad una sfida inevitabile, ma altrettanto stimolante, che si è tutti tenuti ad affrontare[18].

Lo sforzo di garantire una effettività di applicazione della strategia nazionale non può prescindere dalla predisposizione di idonee infrastrutture ed azioni di controllo e monitoraggio. Sotto il primo aspetto, si è ritenuto di dover garantire appositi registri di dataset e modelli che favoriscano la selezione di soluzioni efficienti e standardizzate, anche attraverso una virtuoso processo di bottom-up, che possa svilupparsi dall'ecosistema locale sino a quello nazionale.

Sotto il secondo aspetto si è ritenuto di istituire una Fondazione per l'Intelligenza Artificiale, sotto la diretta dipendenza del CdM, con il fine istituzionale di garantire l'attuazione, il coordinamento ed il monitoraggio della materia ed, ancora più nel dettaglio, gestire e mantenere un registro delle soluzioni e valutare lo stato di avanzamento e raggiungimento dei target. La strategia italiana per la IA inoltre tende ad evidenziare diversi obiettivi e strumenti per ognuna della quattro macro-aree individuate in ragione delle rispettive peculiarità.

L'Area della Ricerca prevede una collaborazione interna ed internazionale, finalizzata ad affrontare le nuove sfide ed insidie che derivano dall' utilizzo del deep-fake, della disinformation on line, da un lato, e, dall'altro, dalla considerazione che la ricerca è il volano dell'innovazione ed, oggi più che mai, strumento strategico di sviluppo della società. Pertanto non si può prescindere da una sinergia stabile fra mondo universitario, scientifico ed imprese che operano nel settore ICT, con particolare attenzione allo studio dei modelli LLM[19].

Il settore della PA è altrettanto indirizzato al duplice obiettivo di ottimizzare le procedure e garantire l'efficienza del servizio reso al cittadino. Il raggiungimento di questi obiettivi non può prescindere dall'utilizzo di idonee piattaforme che garantiscono la interoperabilità delle amministrazioni e che tutelino adeguatamente la sicurezza dei dati, garantendo, nel contempo, possibili feedback degli utenti ed assessment sulla affidabilità

CamminoDiritto.it
ISSN 2421-7123

del sistema. La necessità di prassi metodologiche per settori omogenei crea un legame verso le soluzioni che vengono proposte dal mondo della ricerca e dello sviluppo scientifico, anche attraverso appositi percorsi di partenariato pubblico-privato.

Nel settore economico e di impresa si pone massima attenzione ad intercettare le esigenze tecnologiche e sostenere le imprese del settore ICT, anche attraverso la nuova figura dei Facilitatori. Si tratta di un vero e proprio ecosistema di professionalità, sotto il controllo della Fondazione per l'Intelligenza Artificiale, con il fine di favorire occasioni di incontro istituzionale fra imprese del settore ICT, PMI in genere e start-up, creando un circolo virtuoso di cooperazione e sviluppo sinergico. Il concetto di formazione deve inoltre intendersi nel senso più ampio possibile.

La strategia italiana inoltre prevede percorsi che partono dai livelli più bassi di istruzione, con l'introduzione dello studio dell' intelligenza artificiale nel contesto generale dell'educazione civica ed i corsi professionalizzanti degli studi tecnici, passando per una generale divulgazione da parte dei mass-media, sino ad arrivare ai livelli più alti di formazione. L'obiettivo è quello dichiarato di creare una cultura diffusa, in materia, ad ogni livello. Sono già attivi percorsi di Laurea e Dottorato di Ricerca presso le università italiane ed altri strumenti, più o meno professionalizzanti, come Tirocini, Internship ed Apprendistato. La formazione dovrà avere una valenza trasversale e coinvolgere i lavoratori del settore privato e pubblico con i percorsi di reskilling ed upskilling[20].

Un' ultima prospettiva che merita di essere brevemente approfondita è quella del monitoraggio, che si è tentato di rendere quanto più efficace possibile, ritenendolo cruciale per il conseguimento effettivo degli obiettivi. In merito sono previsti due fondamentali strumenti derivanti dalla esperienza delle scienze manageriali, quali il Key Performance Indicator (KPI), che monitora l'avanzamento delle azioni strategiche rispetto agli obiettivi, e i Flagship Projects, ossia alcuni progetti selezionati che possono considerarsi indicativi dello sviluppo dell'intero comparto. La Fondazione per l'Intelligenza Artificiale potrà avvalersi di questi strumenti nell'ambito del report annuale sulle diverse macro-aree di intervento.

Un ruolo istituzionale diverso verrà invece svolto dalla Autorità Nazionale, prevista dall'Ai Act per ogni Stato membro. Quest'ultima svolgerà una attività di vigilanza su tutto il sistema e, nel dettaglio, dovrà effettuare una delicata verifica sulla conformità delle certificazioni rilasciate da soggetti terzi sulle attività qualificate come ad alto rischio. E' di tutta evidenza che si tratta di una mission istituzionale che si interseca con quella di competenza della Autorità Nazionale per la Cybersicurezza (ACN), delineando settori di intervento diversi e indipendenti ma che, inevitabilmente, dovranno operare, in maniera sinergica, per potere affrontare le sfide strategiche del prossimo futuro.

CamminoDiritto.it
ISSN 2421-7123

7. Conclusioni

Il confronto con strumenti informatici sempre più performanti ha manifestato, con assoluta evidenza, la necessità di un complesso ed articolato intervento del Legislatore europeo e nazionale che, sia pure con approcci parzialmente diversi, si sono prodigati di supplire ai vuoti normativi che hanno finora caratterizzato alcuni aspetti peculiari del processo di digitalizzazione della pubblica amministrazione e della società in genere[21].

Il dato che emerge chiaramente dalla disamina normativa è che l'utilizzo dei nuovi strumenti di Intelligenza Artificiale ha oggi posto, sia le amministrazioni che il cittadino, di fronte ad una sfida epocale. Sotto il profilo dell'impegno degli operatori del diritto, tutto ciò viene ulteriormente complicato dal fatto che il percorso normativo che gradualmente ha portato lo strumento informatico a diventare, sempre più spesso, fonte automatica di scelte amministrative, costringe a riconsiderare tutte le categorie del processo decisionale sotto una nuova chiave di lettura al fine di fare convergere, in maniera equilibrata, innovazione digitale e innovazione normativa, fino a fonderle in un unico contesto indissolubile. L' approvazione dell'Ai Act, in questo quadro generale, non deve essere considerato un punto definitivo di svolta, ma semplicemente un primo passo rispetto al confronto con le nuove tecnologie, a cui nessun campo del sapere umano può oggi sottrarsi.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

1 Python è il linguaggio più usato, in quanto il più veloce a realizzare algoritmi complessi, ed, attualmente, è cresciuto al punto di diventare standard come linguaggio di programmazione

2 Si tratta del secondo quotidiano più diffuso in Canada dopo il Toronto Star , con un bacino di lettori settimanali di circa 935.000 unità

3 La Conferenza di Asilomar sulla IA Benefica è stata organizzata dal Future of Life Institute, dal 5 all'8 Gennaio 2017, presso l' Asilomar Conference Grounds in California dove si sono confrontati "thought leaders" e ricercatori in diverse discipline

4 L.TREMOLADA, L'europa pubblica un codice etico sull'intelligenza artificiale, su www.ilsole24ore.com

5 Il Regolamento UE n. 1689/2024, dopo il voto del Parlamento Europeo del 13/03/2024, è stato definitivamente pubblicato in Gazzetta Ufficiale il 12/07/2024, con tempi di attuazione dai 6 ai 36 mesi, a secondo dei settori di rischio considerati

6 Vedasi Ai Act: a step closer to the first rules on Articial Intelligence, su europarl.europa.eu

7 M.VEALE, Demystifing the Draft EU Artificial Intelligence act in Computer Law Review International, vol.22, n. 4, 2021

8 L.MANCONI e F. RESTA, Le regole dell' Intelligenza artificiale, La Stampa, 16/06/2023

9 GOSMAR, Machine learning. Il sesto chackra dell'intelligenza artificiale, 2020

10 In merito alle implicazioni di potenziale lesione della privacy dai sistemi di AI, vedasi, M. BARTOLONI, Cure ed intelligenza artificiale:la privacy e il rischio dell' algoritmo che discrimina, su www.ilsole24ore.com, 11/10/2023

11 J.G. GANASCIA, L'intelligenza artificiale, Milano, Il Saggiatore, 1997

12 Interessanti le riflessioni di A.TARTARO, Regulating by standards: current progress and main challenges in the standardisation of Artificial Intelligence in support of the Ai Act, in European Journal of Privacy Law and Tecnologies, vol.1, n.1, 2023

13 Vedasi in materia L. VIOLA, Giustizia predittiva ed interpretazione della Legge con modelli matematici, 2019

14 M. ALMADA e N. PETIT, The EU Ai Act: Between Product Safety and Fundamental Rights, 20/12/2022

15 Lo stesso GDPR nasce come testo di compromesso fra diversi orientamenti generali che, in sede di Consiglio, hanno consentito una convergenza di vedute, sfociata nel testo oggi in vigore; Consiglio dell'Unione Europea, Testo di Compromesso, in data.consilium.europa.eu

16 Si può ritenere, a buon titolo, che un punto di svolta possa essere rappresentato dal nascere ed il diffondersi di ChatGPT di OpenAI nel 2022

17 Sotto il profilo della politica industriale, il Legislatore italiano è intervenuto attraverso il DL PNRR che reca il "Piano Transizione 5.0" , che mira alla piena transizione digitale delle imprese italiane, attraverso un sistema di credito di imposta automatico sugli investimenti in materia e sulla formazione dei lavoratori

18 E' paradigmatico di questo differente approccio alla materia il fatto che, mentre nell' Ai Act si prevede la marcatura CE per i sistemi di IA ad alto rischio, nel documento strategico nazionale siano previste delle misure di sostegno per ridurre gli oneri della compliance normativa ed incentivi alle PMI e start-up per accedere alle sandboxes

19 Large Language Model (LLM) è una tecnologia di IA molto avanzata che si concentra sulla analisi e comprensione del testo.

CamminoDiritto.it
ISSN 2421-7123

20 E' previsto presso la SNA un apposito Dipartimento per l'Intelligenza Artificiale

21 Il 23/04/2024 è stato approvato, in sede di CdM, il DDL sull'Intelligenza Artificiale, con l'obiettivo di recepire ed integrare, in ambito nazionale, quanto disposto dall'Ai Act.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=10705