PRIME RIFLESSIONI SULLA TUTELA DELLA PERSONA E DEI DATI PERSONALI TRA GDPR E AI ACT

EMILIO TOSI
Professore associato
nell'Università di Milano-Bicocca

SOMMARIO: 1. Il ruolo europeo di regolatore globale dell'innovazione digitale. – 2. La complessa orditura normativa dell'AI Act. – 3. La classificazione del rischio delle AI: inaccettabile, alto, limitato e minimo. – 4. Finalità e principi dell'AI Act. – 5. Prime riflessioni tra iporegolazione e iperregolazione. – 6. Osservazioni conclusive tra luci e ombre.

1. – L'Unione Europea, non potendo competere per la sfida tecnologica, tenta di vincere le complesse sfide regolatorie dei nuovi fenomeni digitali globali nel solco tracciato dall'esperienza straordinaria del *General Data Protection Regulation* (GDPR), divenuto vero e proprio modello di riferimento — *legal benchmark* — globale nel settore dei dati personali.

Numerosi Stati nel mondo, dal Brasile, Giappone e India, passando per la California, hanno mutuato i principi del GDPR aggiornando le legislazioni nazionali: da ultimo, non certo per importanza, si segnala l'*American Privacy Rights Act* (APRA) il progetto di legge federale sulla privacy degli Stati Uniti d'America da tempo atteso.

Il tratto comune della politica europea della normazione digitale pare essere ispirato dall'encomiabile tentativo di riequilibrare il problematico rapporto tra persona e tecnologia, libertà e innovazione, diritti fondamentali e mercato.

Tale principio ispiratore si rinviene non solo nel *GDPR* ma anche nei più recenti interventi normativi della UE in materia di innovazione digitale: emblematici in tal senso il *Digital Services Act*, *Digital Markets Act*, *Data Governance Act*, *Data Act* e da ultimo l'*Artificial Intelligence Act*[1].

Si tratta, quest'ultimo intervento normativo, della recente legge europea sulle intelligenze artificiali - non esiste, invero, un'unica forma di "intelligenza" artificiale ma semmai molteplici declinazioni alquanto eterogenee tra loro per potenza di calcolo e finalità verticali o generali - entrata in vigore almeno in parte a decorrere dal 2 agosto 2025, del Regolamento UE 13 giugno 2024, n. 1689 noto come *AI Act*

L'AI Act si segnala all'attenzione dei giuristi — e non solo — quale epocale tentativo di disciplinare l'intelligenza artificiale, *rectius* le intelligenze artificiali, per

[1] Si veda sul tema dei complessi rapporti tra AI Act e GDPR la recente raccolta di studi nel venticinquesimo volume della *Collana internazionale di studi giuridici privatistici, Diritto delle nuove tecnologie*, diretta da Vincenzo Franceschelli ed Emilio Tosi: E. TOSI (a cura di), *Persona, dati personali, algoritmi tra GDPR e AI ACT*, Milano, 2025.

renderle strumenti responsabili, affidabili e sicuri nel tentativo di salvaguardare una prospettiva antropocentrica di un nuovo umanesimo digitale fondato sulla tutela della dignità e dei diritti fondamentali della persona.

Gli Stati sovrani non possono e non devono cedere alla facile scorciatoia di affidarsi esclusivamente all'autodisciplina, consegnando al mercato oligopolistico e al potere autoregolatorio privatistico dell'innovazione concentrato in poche *big tech* e *gatekeeper*, la definizione del perimetro, di rilevanza costituzionale, di diritti e libertà.

L'AI Act dialoga necessariamente con il GDPR: precisamente è sottoposto al GDPR che non intende derogare per nulla e che anzi si prefigge di osservare e applicare pur con tutte le difficoltà del caso.

Il nuovo regolamento europeo non intende, infatti, pregiudicare l'applicazione della disciplina relativa al trattamento dei dati personali posta dal GDPR, inclusi i compiti e i poteri delle Autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti[2].

Come ci ricorda proprio l'AI Act nei considerando preliminari, il Regolamento "lascia impregiudicati gli obblighi dei fornitori e dei *deployer* dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento derivanti dal diritto dell'Unione o nazionale in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali".

E ancora chiarisce che l'interessato dal trattamento dei propri dati continuerà a beneficiare del diritto stabilito dall'art. 22 del GDPR 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.

Le nuove norme armonizzate dell'AI Act per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA dovrebbero facilitare l'efficace attuazione e consentire l'esercizio dei diritti degli interessati in materia di protezione dei dati personali nonché degli altri diritti fondamentali.

Pare ormai evidente che non si ripeterà il successo irripetibile del GDPR: non ci sarà un *Bruxelles effect* analogo a quello straordinario dell'esperienza normativa europea in materia di protezione del diritto fondamentale alla protezione dei dati personali.

---

[2] Si vedano sul tema della regolazione delle intelligenze artificiali: G. ALPA (a cura di), *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020, *passim*; F. FIDANZA, *L'AI Act: ambito e proiezioni applicative*, in *Studium*, 2025, 444 ss.; G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Bologna, 2024; A. GENTILI, *Regole per l'intelligenza artificiale*, in *Contratto e Impresa*, 2024, 1043-1069; e da ultimo A. MANTELERO, G. RESTA, G. M. RICCIO (a cura di), *Intelligenza artificiale commentario. Regolamento (UE) 2024/1689*, Torino, 2025.

In primo luogo, il Libro bianco della Commissione sull'IA del 2020, che annunciava l'intenzione di legiferare sull'IA, ha dato il via altre giurisdizioni in tutto il mondo relativamente alla regolamentazione dell'IA.

In secondo luogo, l'approccio basato sul rischio dell'AI Act e alcuni dei suoi concetti chiave troveranno formulazioni personalizzate in altre leggi di altri Stati che non potranno tenere conto di standard e certificazioni di origine europea considerandole universali.

Questo si vede già chiaramente con il Colorado AI Act – CAIA – che è stato adottato il 17 maggio 2024, un paio di giorni prima dell'adozione finale dell'AI Act europeo.

L'AI Act dunque difficilmente diverrà, con la stessa facilità di diffusione del modello e ampiezza di altri referenti normativi europei, *legal benchmark* globale al pari del GDPR.

Ma soprattutto per la semplice ragione che l'AI Act non è centrato sulla tutela di un nuovo diritto fondamentale facilmente esportabile a livello globale come la protezione dei dati personali ma su regole europee per conformare un sistema in termini di sicurezza, affidabilità, certificazioni e standard di un prodotto industriale.

Non può sfuggire all'interprete che il contenuto dell'AI Act in termini di sicurezza dei prodotti, compresi gli obblighi di documentazione relativi alle valutazioni di conformità pensate per il mercato europeo difficilmente si radicheranno altrove come dimostrano le opposte politiche AI di Stati Uniti e Cina.

L'AI Act è basato su un approccio "*risk-based*" che ritroviamo anche in altre normative (prima tra tutte, il GDPR): maggiore è il rischio insito nell'utilizzo di un determinato sistema intelligenza artificiale, maggiori saranno, conseguentemente, le responsabilità di chi sviluppa e usa quel sistema, sino a giungere a un divieto di utilizzo delle applicazioni e delle tecnologie il cui rischio è considerato inaccettabile.

L'AI Act è certamente un punto di partenza importante per la disciplina del nuovo fenomeno nonostante significative criticità, fra cui la complessità e la carenza di chiarezza di diversi profili definitori e applicativi che lo rendono più simile a una Direttiva mascherata per la generalità nella formulazione di diversi precetti che richiederanno ampio apparato attuativo per l'effettiva applicazione: ben lungi, pertanto, dall'essere un approdo regolatorio definitivo.

Pensiamo alla definizione di AI per nulla semplice e non ancorata a parametri oggettivi quali parametri di addestramento, in attesa di standardizzazione in sede attuativa, utilizzati e velocità di calcolo solo per fare alcuni esempi senza pretesa di esaustività.

Solo determinati sistemi di intelligenza artificiale sono soggetti a obblighi normativi e supervisione ai sensi della legge europea sull'intelligenza artificiale. L'approccio basato sul rischio dell'AI Act implica che solo i sistemi che danno origine ai rischi più significativi per i diritti e le libertà fondamentali saranno soggetti ai divieti stabiliti nell'articolo 5 dell'AI Act, al regime normativo per i sistemi di intelligenza

artificiale ad alto rischio coperti dall'articolo 6 dell'AI Act e ai requisiti di trasparenza per un numero limitato di sistemi di intelligenza artificiale predefiniti stabiliti nell'articolo 50 dell'AI Act.

La stragrande maggioranza dei sistemi AI, anche se si qualificano come sistemi di intelligenza artificiale ai sensi dell'art. 3.1 dell'AI Act, non sarà soggetta ad alcun obbligo normativo ai sensi della legge europea sull'intelligenza artificiale, in quanto la normativa europea si focalizza sui sistemi di AI a rischio alto e limitato e sui modelli di AI per finalità generali mentre sostanzialmente non considera, forse sbrigativamente e con un errore di valutazione prospettica, i sistemi di AI a rischio minimo o nullo.

L'AI Act si applica, inoltre, anche ai modelli di intelligenza artificiale di uso generale, che sono regolamentati nel capitolo V della legge sull'intelligenza artificiale.

Centrale per la corretta applicazione della legge sull'intelligenza artificiale è, pertanto, la corretta qualificazione giuridica del sistema di intelligenza artificiale.

Più facile a dirsi che a farsi. La definizione di un sistema di IA comprende effettivamente un ampio spettro di sistemi non sempre agevolmente qualificabili — in assenza di parametri di legge oggettivi — quale sistema di IA.

La qualificazione di un qualunque software in termini di sistema di IA dovrà basarsi — come suggerito dalla Commissione UE nelle bozze di Linee Guida sulla definizione di sistema di AI del 6 febbraio 2025 — sull'architettura e sulla funzionalità specifiche di un dato sistema e dovrà prendere in considerazione i sette elementi principali della definizione stabilita nell'articolo 3.1 dell'AI Act, vale a dire:

(1) un sistema basato su una macchina;
(2) progettato per funzionare con diversi livelli di autonomia;
(3) che può mostrare adattabilità dopo l'implementazione;
(4) e che, per obiettivi espliciti o impliciti;
(5) deduce, dall'input che riceve, come generare output;
(6) come previsioni, contenuti, raccomandazioni o decisioni
(7) che possono influenzare ambienti fisici o virtuali.

Non sono, quindi, possibili determinazioni automatiche o elenchi esaustivi di sistemi che rientrano o esulano dalla definizione di un sistema di IA.

L'onere della qualificazione di un sistema di IA è una parte fondamentale dell'applicazione dell'AI Act, ma non è affatto semplice per l'interprete in assenza di parametri normativi oggettivi e andrà operata caso per caso in concreto.

In buona sostanza l'impianto dell'AI Act, – rispetto al GDPR –, è meno incisivo più disordinato, ridondante ed eccessivamente burocratico, e a tratti financo poco chiaro, per non dire confuso, in numerosi aspetti della governance dell'AI Act: si pensi, a titolo esemplificativo, al riparto di competenze tra Commissione, AI Board e AI Office, da un lato, e autorità nazionali di notifica e vigilanza, dall'altro.

2. – L'AI Act costituisce un testo normativo davvero poderoso e complesso, forse troppo, che richiederà del tempo per essere compiutamente assimilato dall'interprete e dagli operatori:

— 180 considerando (173 GDPR);
— 113 articoli (99 GDPR);
— 68 definizioni (26 GDPR);
— XIII Allegati.

Testo normativo forse, come si accennava *supra*, troppo complesso, dettato dall'urgente necessità di intervenire tempestivamente su un fenomeno nuovo e dirompente in forte accelerazione, che rischia, tuttavia, di esporre l'iniziativa legislativa europea alle crescenti critiche di *iper-regolazione e sovrapposizione* con altri importanti referenti normativi europei del complesso *corpus iuris digitali*s europeo (oltre al GDPR *ex multis* e senza pretese di esaustività si possono almeno menzionare il *Digital Service Act, Data Act)*.

Non c'è dubbio che i diritti fondamentali debbano essere tutelati ma troppi obblighi, sovrapposizioni e scarsa sistematicità, che – non sempre sono funzionali ad assicurare maggior protezione, anzi – rischiano, invero, di ostacolare lo sviluppo del settore ammesso che ancora vi siano margini per la cara vecchia Europa.

Al tempo stesso la formulazione dei precetti ampia, e non sempre univoca, risente di una formulazione più simile a quella di una cripto-direttiva in luogo di un vero e proprio regolamento.

Forse la fretta di raggiungere l'intesa su un testo normativo condiviso non ha giovato alla chiarezza e sistematicità dell'AI Act.

Fondamentale anche in questo caso, come per il GDPR, il ruolo interpretativo e chiarificatore della Corte di Giustizia della UE.

La complessità dell'AI Act risulta ancora più evidente se raffrontata alla sostanziale deregulation federale da parte degli Stati Uniti.

Un AI Act più snello e focalizzato sui principi fondamentali e le AI vietate sarebbe stato forse più efficiente dal punto di vista applicativo: ma questo è il testo con cui allo stato dobbiamo confrontarci anche se l'auspicio di un intervento di semplificazione e razionalizzazione, a breve termine, è da senz'altro condivisibile.

L'articolato, suddiviso in tredici capi e corredato da un apparato di tredici allegati, ruota attorno a sette blocchi principali:

(*i*) parte generale e definizioni (Capo I);

(*ii*) usi vietati dell'AI e gestione del rischio, inclusa quella successiva alla collocazione dei sistemi sul mercato (Capi II, III, VIII, IX);

(*iii*) norme specifiche per AI ad alto rischio e AI per finalità generali, principalmente incentrate sulla trasparenza (Capi IV e V);

(*iv*) misure in favore dell'innovazione, ad esempio *sandboxes* (Capo VI);

(*v*) modello di governance, inclusivo delle competenti autorità di supervisione (Capo VII);

(*vi*) codici di condotta (Capo X);

(*vii*) delegazione legislativa (Capo XI), sanzioni (Capo XII) e previsioni finali (Capo XIII).

Non si può comprendere la rilevanza socioeconomica prima ancora che giuridica dell'AI Act ed il tenore delle previsioni ivi contenute senza tenere a mente il dominio statunitense sui mercati AI, nel rendere disponibili sul mercato business e consumer tecnologie ancora imprecise, o l'uso sistemico da parte di stati totalitari di strumenti di controllo biometrico e sociale.

Per disciplinare il fenomeno non è, tuttavia, sufficiente ricorrere all'elencazione delle categorie di usi vietati dell'AI contenute nell'AI Act, peraltro caratterizzato da troppe eccezioni e deroghe applicative ad avviso dello scrivente, richiamare le norme sui modelli della cosiddetta *General Purpose AI* (GPAI), affrontare il tema della valutazione d'impatto: occorre contestualizzare la fenomenologia delle intelligenze artificiali sottraendosi alla tentazione, facile quanto inutile, di ragionare solo in termini di astratte categorie e sterili tassonomie peraltro di scarsa utilità in un contesto così in evoluzione come quello di cui trattasi.

La stessa definizione di AI a ben vedere, non è né semplice né univoca: occorre dunque ancorarsi a principi generali ed evitare la cristallizzazione definitoria angusta che rischia di ingessare l'applicazione dell'AI Act fornendo tuttavia non solo parametri qualitativi ma anche oggettivi per agevolare l'interprete.

Si definisce ai sensi dell'art. 3 dell'AI Act "sistema di IA": «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

E ancora si definisce "modello di IA per finalità generali": «un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'auto-supervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato».

Persino l'EDPS, a titolo esemplificativo, senza pretese di esaustività, segnala come meritevole di chiarificazione il concetto di *livelli di autonomia variabili* e precisa che[3]:

«In our view, all IT systems may be considered autonomous, as they do automate calculations and processes. For example: an IT system that includes a machine

[3] EDPS comment to the AI Office's consultation on the application of the definition of an AI System and the prohibited AI practices established in the AI Act - 19 December 2024.

learning model that shows to a bank clerk a prediction on a loan application is autonomous. But in which sense is that IT system more autonomous that a simple rule based algorithm that will judge some attributes of the application? ».

E ancora sul concetto di "adattabilità dopo la diffusione":

«The EDPS considers the notion of adaptiveness should be broadened to include a fundamental element, namely the adaptation and the learning procedure that occur before the deployment, which isa unique element to AI systems. The definition seems to obviate the fact that AI systems learn during their development. Al systems start their development with a set of unadjusted initial parameters. Then, they undergo a learning procedure in order to adjust/tune these parameters to improve their performance in a defined task. AI systems become 'intelligent' precisely because of their capability of learning and adapting».

Sul punto soccorrono, almeno in linea di principio essendo il profilo applicativo tutt'altro che semplice, le linee guida della Commissione UE del 6 febbraio 2025 sulla definizione di un sistema di intelligenza artificiale stabilito dall'AI Act: Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).

Si registra, dunque, uno iato significativo tra sviluppo delle AI e la disciplina applicabile elaborata dal legislatore europeo.

È preminente, dunque, la necessità di definizioni rigorose, precetti normativi chiari e vincolanti corroborati da sanzioni adeguate e dissuasive.

L'AI Act non sempre soddisfa tali aspettative essendo eccessivamente prolifico di stringenti definizioni e di precetti non di agevole applicazione multilivello e spesso sovrapposti ad altri referenti normativi: si tratta, come si avrà modo di rilevare ulteriormente nel corso del presente approfondimento, di un atto legislativo estremamente complesso e poco meditato dal legislatore europeo.

Meglio sarebbe stato fermarsi alla statuizione di pochi principi generali rinviando ad altro atto la regolamentazione di dettaglio dei sistemi di AI ad alto rischio e per finalità generali. Quest'ultima parte, non presente nel testo originariamente presentato dalla Commissione UE, pare slegata dal resto del testo normativo e risente vistosamente del difetto di coordinamento, rispetto al resto dell'AI Act, ascrivibile verosimilmente all'introduzione tardiva ad opera del Parlamento Europeo.

Il Regolamento in parola pare orientato, si rileva da subito, in discontinuità rispetto al GDPR, principalmente alla sicurezza industriale e alla certificazione di prodotto piuttosto che alla tutela dei diritti fondamentali della persona, con una significativa attenzione alla gestione del rischio in termini di valutazione di conformità e con l'attribuzione di un peso significativo agli standard industriali.

Ne emerge un testo normativo, si ribadisce, che pare meno incisivo rispetto al GDPR: l'AI Act cerca una difficile equilibrio tra diritti fondamentali e innovazione tecnologica ma non sempre con la chiarezza d'intenti del GDPR. Anzi pare troppo timido l'intervento regolatorio come evidenziato dalle troppe deroghe ed eccezioni:

valga per tutti la formulazione dell'ambito applicativo fortemente limitato (art. 2 AI Act) e l'enunciazione delle pratiche vietate (art. 5 AI Act).

È evidente che l'obiettivo del legislatore europeo, nel caso dell'AI Act, non è tanto quello di assicurare – in ogni caso e a tutti i costi – la tutela dei diritti fondamentali, della persona piuttosto quello di bilanciare tutela della persona e del mercato favorendo soprattutto lo sviluppo dell'AI per facilitare un recupero dell'Europa in tale settore specifico, forse più utopico che reale.

Tale tensione intrinseca tra persona e mercato si rivela chiaramente nell'AI Act e spiega la ragione dell'approccio regolatorio focalizzato sulla sicurezza del prodotto e l'equilibrio scelto nella gestione del rischio secondo una prospettiva strategica europea più incline all'accettazione del rischio, considerata la previsione di numerose eccezioni e deroghe applicative, rispetto ad altri interventi legislativi più rigorosi come il GDPR.

Si pensi, a titolo esemplificativo, alle ampie eccezioni dell'art. 111 per le AI già operative prima dell'entrata in vigore dell'AI Act.

Alle ulteriori, eccessivamente ampie, eccezioni relative all'applicazione delle AI ad alto rischio nei casi di *sicurezza nazionale, difesa, ricerca e uso personale* si aggiungono esenzioni per l'industria della IA.

3. – L'AI Act contiene disposizioni progressivamente più stringenti articolate secondo quattro livelli di *gestione del rischio*:

— inaccettabile;
— alto;
— limitato;
— minimo.

Ai sensi dell'AI Act il rischio è la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso (art. 3, paragrafo 1, n. 2 AI Act).

I sistemi di AI sono sostanzialmente vietati perché considerati troppo pericolosi per i diritti fondamentali della persona e gli altri valori protetti dalla carta dei diritti fondamentali UE.

I sistemi di IA "ad alto rischio" devono rispettare una serie di stingenti requisiti e obblighi per poter accedere al mercato dell'Unione europea. In particolare, l'AI Act richiede una maggiore trasparenza per quanto riguarda lo sviluppo e l'utilizzo di tali sistemi.

Invece i sistemi di IA a rischio limitato "destinati direttamente a interagire con persone fisiche" sono soggetti a obblighi di trasparenza previsti dall'articolo 50 della legge sull'IA.

Infine, i sistemi di IA a rischio minimo o nullo esulano dall'ambito applicativo dell'AI Act.

Prima di utilizzare un sistema di IA ad alto rischio, i *deployer* che possono enti pubblici che forniscono servizi pubblici, oppure soggetti privati quali banche e

compagnie di assicurazione, devono effettuare una valutazione d'impatto sui diritti fondamentali[4].

Per alcuni altri usi dell'IA – come la manipolazione cognitiva del comportamento, i sistemi di valutazione sociale, il riconoscimento delle emozioni sul posto di lavoro e nelle istituzioni educative e il *social scoring* – i rischi sono invece ritenuti inaccettabili e quindi l'utilizzo di tale tipologia di sistemi è vietato.

L'AI Act vieta espressamente alcune applicazioni di IA che minacciando i diritti fondamentali delle persone comportano un rischio inaccettabile.

L'Art. 5 dell'AI Act individua espressamente le seguenti AI vietate:

— i sistemi di categorizzazione biometrica basati su caratteristiche sensibili e l'estrapolazione indiscriminata di immagini facciali da internet o dalle registrazioni dei sistemi di telecamere a circuito chiuso per creare banche dati di riconoscimento facciale;

— i sistemi di riconoscimento delle emozioni sul luogo di lavoro e nelle scuole;

— i sistemi di credito sociale, le pratiche di polizia predittiva basate esclusivamente sulla profilazione o sulla valutazione delle caratteristiche antropologiche di una persona;

— i sistemi che manipolano il comportamento umano o sfruttano le vulnerabilità delle persone.

Si segnalano sul tema rilevantissimo delle pratiche di AI vietate dall'AI Act le *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) della Commissione UE* del 25 febbraio 2025.

Tuttavia, pur apprezzandosi lo sforzo chiarificatore della *Commissione UE*, 140 pagine esplicative dell'art. 5 dell'AI Act paiono davvero eccessive, evidentemente causate dalla formulazione generica dell'AI Act, già stigmatizzata *supra*, più simile alla direttiva che al regolamento.

Il rischio di iper-regolazione e di incertezza applicativa si concretizza anche nell'eccesso di Linee Guida che rischiano di disorientare l'operatore prima ancora dell'interprete.

Un secondo livello di rischio contempla le AI ad altro rischio in relazione alle quali sono previsti obblighi stringenti in quanto potrebbero arrecare danni significativi alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia e allo Stato di diritto.

Rientrano in questa categoria gli usi di AI legati a:

— infrastrutture critiche;

— istruzione e formazione professionale;

— occupazione, servizi pubblici;

[4] Si vedano sul tema G. MALGIERI, C. SANTOS, *Assessing the (Severity of) Impacts on Fundamental Rights*, June 25, 2024), https://ssrn.com/abstract=4875937; A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, 54, 2024, pp. 106 ss.

— servizi privati di base: assistenza sanitaria, bancaria e assicurativa;
— alcuni sistemi di contrasto, migrazione e gestione delle frontiere;
— giustizia e processi democratici.

Per questi sistemi vige l'obbligo di valutare e ridurre i rischi, mantenere registri d'uso, essere trasparenti e accurati e garantire sempre la sorveglianza umana: il c.d. *human in the loop*.

I cittadini avranno diritto a presentare reclami sui sistemi di IA e a ricevere spiegazioni sulle decisioni basate su sistemi di IA ad alto rischio che incidono sui loro diritti.

L'AI Act si prefigge lo scopo di migliorare e promuove la protezione dei diritti tutelati dalla Carta: il diritto alla dignità umana (articolo 1), al rispetto della vita privata e alla protezione dei dati di carattere personale (articoli 7 e 8), alla non discriminazione (articolo 21)

Sono introdotte a tal fine alcune necessarie restrizioni alla libertà d'impresa (articolo 16) e alla libertà delle arti e delle scienze (articolo 13) al fine di assicurare il rispetto di motivi imperativi d'interesse pubblico quali la salute, la sicurezza, la tutela dei consumatori e la protezione di altri diritti fondamentali ("innovazione responsabile") nel momento in cui si diffonde e si utilizza una tecnologia di IA.

Tali restrizioni sono proporzionate e limitate al minimo necessario per prevenire e attenuare rischi gravi per la sicurezza e probabili violazioni dei diritti fondamentali.

In relazione alle AI a rischio limitato sono invece previste misure meno stringenti in particolare obblighi di trasparenza che si applicano ai sistemi che: i) interagiscono con gli esseri umani; ii) sono utilizzati per rilevare emozioni o stabilire un'associazione con categorie (sociali) sulla base di dati biometrici; oppure iii) generano o manipolano contenuti ("*deep fake*").

Inoltre, i maggiori obblighi di trasparenza non incideranno in maniera sproporzionata sul diritto alla protezione della proprietà intellettuale (articolo 17, paragrafo 2), dato che saranno limitati soltanto alle informazioni minime necessarie affinché le persone possano esercitare il loro diritto a un ricorso effettivo e alla necessaria trasparenza presso le autorità di controllo e di contrasto, in linea con i loro mandati.

I set di dati di addestramento, convalida e prova delle AI ad alto rischio devono essere pertinenti, rappresentativi, esenti da errori e completi.

Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o di una combinazione degli stessi.

La protezione dei dati personali è protezione della libertà e della dignità della persona, tanto più quando sono coinvolti i minori e i soggetti vulnerabili.

L'applicazione dell'intelligenza artificiale in campo neuroscientifico e, soprattutto i sistemi di *brain reading*, idonei almeno potenzialmente a decodificare il

pensiero, devono infatti sempre garantire, come primo dei "neurodiritti", la *privacy* mentale, condizione ineludibile di autodeterminazione, presupposto intangibile di libertà.

Varcata la soglia della lettura del pensiero, la deriva da impedire è rendere la persona un archivio liberamente accessibile dalle AI e altri dispositivi tecnologici, anche se con il consenso dell'interessato, frutto di un'autodeterminazione imperfetta e come tale inidonea a costituire una base giuridica per il trattamento dei propri pensieri, le cui idee siano messe a nudo senza più alcuno spazio per la libertà e l'autonoma volizione.

Siamo davvero disposti ad ammettere, in un prossimo futuro di cui già si discorre, le più evolute tecniche di pubblicità mentale, *neuromarketing*, su impianti cerebrali, solamente affidando la protezione della persona al consenso dell'interessato?

È evidente che la risposta non può che essere negativa essendo il consenso individuale e l'autodeterminazione informativa troppo deboli in determinati contesti tecnologici digitali altamente manipolativi, ora supportati dalle AI, ulteriore innovativo fattore di dirompente asimmetria. Trattasi dell'effetto *nudge tech* che concorre a disegnare con predeterminazione favorevole al contraente forte l'architettura delle scelte del contraente debole più in generale dell'utente digitale spingendo il soggetto interessato a scelte spesso inconsapevoli certamente gradite alla piattaforma digitale-contraente forte ma non necessariamente protettive della dignità personale[5].

Le nuove vulnerabilità digitali richiedono, pertanto, barriere precettive conformative inderogabili e rafforzate a prescindere dall'autodeterminazione personale che non può più da sola costituire un solido argine al fenomeno di sfruttamento commerciale dei dati personali da parte delle big tech e più in generale costituire

[5] Sul tema del consenso al trattamento dei dati personali, circolazione dei dati personali e ammissibilità di un consenso contrattuale assorbente dei profili inerenti al trattamento dei dati personali si vedano: V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018, 689 ss.; P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ.*, 2022, 1054 ss.; T. M. UBERTAZZI, *Ripensando alla revoca del consenso nella prospettiva funzionale della privacy*, in *Contratto impr.*, 2022, 27 ss.; S. ORLANDO, *Per un sindacato di liceità del consenso*, in *Persona merc.*, 2022, 527 ss.; S. ORLANDO, *Consenso al trattamento e liceità*, in *Persona merc.*, 2024, 333 ss.; S. ORLANDO (a cura di), *Libertà e liceità del consenso nel trattamento dei dati personali*, Firenze, 2024; e da ultimo E. TOSI, *Circolazione contrattuale dei dati personali tra contratto e responsabilità*, Milano, 2023, 78 ss. *cui adde* E. TOSI, *Dati personali e contratto: un ossimoro apparente*, in *European Journal of Privacy Law and Technologies*, 2023, 71 ss. *Contra* in ordine alla prevalente natura autorizzatoria, con varie sfumature interpretative, del consenso al trattamento dei dati personali: G. ALPA, G.RESTA, *Le persone fisiche e i diritti della personalità*, I, in *Trattato di Diritto Civile*, diretto da R. SACCO, Torino, 2006, *passim*, spec. 629 ss.; F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in questa *Rivista*, 2019, 34 ss.; ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, *passim*; P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; e C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, *passim.*

strumento di protezione efficace a presidio dei diritti fondamentali della persona, in ultima istanza della dignità personale[6].

Infine, criticità non trascurabile, risultano sostanzialmente ignorate dall'AI Act le AI a rischio minimo o nullo: in relazione a tale categoria residuale sarebbe forse stato più opportuno prevedere espressamente almeno l'applicazione di qualche principio generale di trasparenza e supervisione umana.

Si evidenzia, inoltre, importanti eccezioni applicative individuate dal paragrafo 3 del medesimo articolo 6 dell'AI Act.

Un sistema di IA non è considerato ad "alto rischio" se non presenta rischio significativo per salute, sicurezza e diritti fondamentali delle persone fisiche – anche nel senso di non influenzare materialmente il processo decisionale – e sono altresì soddisfatte una o più delle seguenti condizioni:

a) il sistema di IA è destinato a eseguire un compito procedurale limitato;

b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata;

c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è inteso a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o

d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III dell'AI Act.

Anche in questo caso le deroghe paiono troppo ampie e destinate a sottrarre dal campo applicativo sistemi di AI comunque meritevoli di regolazione stringente.

Si pensi *a contrariis* al maggior rigore protettivo dei diritti fondamentali della persona che traspare, invece, dall'art. 35 del GDPR:

«Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali».

Ben diverso dall'art. 27 dell'AI Act che non prevede invece una valutazione d'impatto sui diritti fondamentali della persona generalizzata ma limitatamente ai sistemi di AI ad alto rischio che costituiscono un sottoinsieme piuttosto circoscritto delle possibili AI potenzialmente lesive dei diritti fondamentali della persona.

[6] Si vedano in tal senso anche G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford, 2023; C. ROSCA, *Digital arms for digital consumer harms. Mapping Legal and Technical Solutions for Dark Patterns in EU Consumer Law*, Maastricht, 2024. Sulla compatibilità dello sfruttamento commerciale dei dati personali con il GDPR e sulla conseguente complementarietà tra GDPR e Codice del Consumo nella circolazione dei dati personali si vedano da ultimo Cons. Stato 2 dicembre 2024, n. 9614; Cons. Stato 7 gennaio 2025, n. 80.

Sono evidenti le difficoltà a replicare il caso esemplare del GDPR: allora si trattava di esportare nel mondo la tutela di un diritto fondamentale della persona universale, valido per tutti a livello globale.

Nel caso dell'AI Act si tratta invece di esportare un modello di regolazione di una nuova tecnologia secondo standard e certificazioni industriali europee – e non universali – che difficilmente potranno essere condivisi globalmente senza un processo di codificazione internazionale che in questo contesto sarebbe auspicabile per assicurare un livello minimi condiviso a livello globale di trasparenza, affidabilità e responsabilità da parte dei produttori di AI, dei *deployer* e di tutti gli altri soggetti della filiera.

4. – Le eterogenee finalità e i molteplici principi dell'AI Act meritano ulteriore approfondimento per una lettura sistematica della complessa orditura normativa.

L'AI Act della UE si propone di migliorare il funzionamento del mercato europeo istituendo un quadro giuridico uniforme in particolare per quanto riguarda:

— lo sviluppo, l'immissione sul mercato, la messa in servizio e "l'uso responsabile" di sistemi di intelligenza artificiale, in conformità ai valori dell'Unione Europea;

— la diffusione di un'intelligenza artificiale (IA) "antropocentrica, sicura, trasparente e affidabile" garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea;

— prevenendo la disinformazione, tutelando la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione nonché promuovere l'innovazione digitale assicurando un controllo umano di ultima istanza.

Tra le molteplici finalità di questo Regolamento epocale noto come AI Act – Regolamento UE 13 giugno 2024, n. 1689 – meritano di essere evidenziati i seguenti profili:

— le garanzie per i sistemi di intelligenza artificiale usati per finalità generali e specifiche regole per IA considerate ad alto rischio;

— limiti all'uso dei sistemi di identificazione biometrica da parte delle forze dell'ordine;

— divieto di utilizzo di sistemi di credito sociale o per manipolare e sfruttare le vulnerabilità degli utenti;

— tutela dei consumatori mediante diritto a presentare reclami e ricevere spiegazioni rilevanti.

La riforma europea introduce, inoltre, specifici obblighi di trasparenza e spiegazione: per tutelare diritti dei consumatori, dei lavoratori più in generale dei cittadini e in ultima istanza i mercati, quasi un ideale punto di partenza di una nuova governance tecnologica e di un rinnovato contratto sociale.

L'AI Act – così come il GDPR – stabilisce obblighi differenziati sempre più stringenti sulla base dei possibili rischi e del livello d'impatto sui diritti fondamentali della persona.

Risulta evidente il tentativo di contrastare l'opacità, la complessità, la faziosità, un certo grado di strutturale imprevedibilità – le *allucinazioni algoritmiche* – e un comportamento parzialmente autonomo di taluni sistemi di IA, onde garantirne la compatibilità con i diritti fondamentali e agevolare l'applicazione delle norme giuridiche europee.

Solo i primi esiti applicativi e i primi pronunciamenti della Corte di Giustizia della UE ci potranno dire qualcosa di più relativamente all'efficacia della nuova disciplina europea.

L'AI Act si segnala - pur nella sua complessità per certi aspetti ridondante e preludio di un rischio di "iper-regolazione" in fase attuativa – per la marcata prospettiva antropocentrica pur senza rinunciare ad assicurare lo sviluppo e la diffusione delle AI.

Si nota l'assenza di una norma riepilogativa dei principi generali applicabili alle AI sulla falsariga dell'art. 5 del GDPR.

I principi generali per le AI non sono formulati in modo esplicito e organico come nel GDPR ma vanno estrapolati dalla disamina delle singole norme e da una lettura sistematica del testo complessivo. Si menzionano qui di seguito quelli più significativi.

Innanzitutto, considerando le correlazioni essenziali tra principi ordinatori su cui si fonda tutto l'impianto normativo dell'AI Act ovverossia:

- "principio di *accountability*", fornitori e deployer sono tenuti ad autovalutare il rischio correlato all'AI sviluppata e immessa sul mercato dal "fornitore", documentando il processo valutativo aziendale, o impiegata sotto la propria autorità (*deployer*) e il corollario
- "principio di gestione del rischio", che richiede di applicare i precetti differenziati previsti dall'AI Act in misura minimale per le AI "a rischio limitato" e massima per le AI "ad alto rischio".

"Il principio di *accountability* e gestione del rischio" non sono certo, come noto, una novità: essendo, invero, già stati codificati, seppure con riferimento a differente, ma strettamente correlato, settore applicativo della tutela e circolazione dei dati personali, nei ben noti artt. 5. 2, art. 24 e 32 del GDPR.

In secondo luogo, evidenziando quelli più innovativi e applicabili a tutte le AI – a prescindere dalla classificazione del rischio con il *caveat* di applicazione rafforzata per le AI *ad alto rischio* – a partire dai seguenti:

- "principio di formazione", c.d. *AI Literacy:* art. 4, AI Act;
- "principio di sicurezza intrinseca ed estrinseca": tanto più elevato è il rischio tanto più elevate sono le misure di sicurezza e gli obblighi specifici da implementare: ma qualsiasi AI in ossequio a lettura assiologica protettiva, costituzionalmente

orientate, della persona deve, in ogni caso, essere sicura in sé e per sé in quanto resistente agli attacchi e non pericolosa per le persone;

- "principio di trasparenza": art. 50, AI Act;
- "principio di sostenibilità ambientale": art. 1, AI Act.

Iniziamo dall'art. 4 dell'Ai Act il principio di *AI literacy:* "alfabetizzazione in materia di IA" che statuisce un ampio e rilevantissimo obbligo formativo utile anche per misurare la responsabilizzazione e la responsabilità di fornitori e deployer*:* «I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati».

Segue, non certo per importanza, "il principio di trasparenza" relativo ai sistemi di IA destinati a interagire direttamente con le persone fisiche, a prescindere dal rischio, integrato dal corollario del "principio di equità e non discriminazione"*:* art. 13 "Trasparenza e fornitura di informazioni ai *deployer*" e 50 "Obblighi di trasparenza per i fornitori e i *deployers* di determinati sistemi di IA dell'AI Act". Il considerando 27 precisa che: «Con "trasparenza" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i *deployer* delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti. Con "diversità, non discriminazione ed equità" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da includere soggetti diversi e promuovere la parità di accesso, l'uguaglianza di genere e la diversità culturale, evitando nel contempo effetti discriminatori e pregiudizi ingiusti vietati dal diritto dell'Unione o nazionale».

Il considerando 72 aggiunge che: «Per rispondere alle preoccupazioni relative all'opacità e alla complessità di determinati sistemi di IA e aiutare i *deployer* ad adempiere ai loro obblighi a norma del presente regolamento, è opportuno imporre la trasparenza per i sistemi di IA ad alto rischio prima che siano immessi sul mercato o messi in servizio».

"Il principio di sostenibilità ambientale"*:* specialmente art. 1 "Oggetto dell'AI Act" che statuisce quanto segue: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione». La sostenibilità ambientale europea –

almeno nelle statuizioni di principio – diviene, dunque, parametro rilevante per disincentivare lo sviluppo di AI energivore e inquinante. Invero con scarsi risultati pratici a livello globale essendo – almeno allo stato – le istanze ambientali del tutto secondarie rispetto alla frenesia da sviluppo tecnologico e supremazia nel settore dell'AI.

Seguono poi principi applicabili solamente alle AI "ad alto rischio" cui pare prevalentemente orientato in larga parte lo sforzo regolatorio delle AI.

Primus inter pares non si può non partire dal fondamentale che, a parere di chi scrive, avrebbe potuto più coraggiosamente essere esteso nella sua portata generale oltre i limiti ristretti delle AI "ad alto rischio", come fatto per l'art. 4 in materia di *AI literacy:*

- "principio del rispetto dell'autonomia decisionale umana"*:* già per vero statuito nell'art. 22 del GDPR e nell'art. 25 del *Digital Service Act* emerge dagli artt. 13 "Trasparenza e fornitura di informazioni ai *deployer*" e 86 "Diritto alla spiegazione dei singoli processi decisionali dell'AI Act"; ulteriormente rafforzato dal complementare e innovativo
- "principio di sorveglianza umana"*:* art. 14 AI Act di cui si è già detto *amplius supra*;
- "principio di conformità"*:* art. 47 AI Act per effetto del quale il fornitore di AI ad alto rischio è obbligato sotto la propria responsabilità a rilasciare: (i) un'attestazione secondo cui il sistema di IA è conforme ai requisiti di cui alla sezione 2 e riporta le informazioni di cui all'allegato V dell'AI Act e, ove applicabile, a qualsiasi altra disposizione pertinente del diritto dell'Unione che preveda il rilascio di una dichiarazione di conformità UE; (ii) se un sistema di IA comporta il trattamento di dati personali, una dichiarazione attestante che tale sistema di IA è conforme ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680.

Emerge, inoltre, "il principio di sicurezza rafforzato per le persone e di sicurezza intrinseca delle AI ad altro rischio" *(safety and security):* il "principio di *accountability*" si traduce nei sistemi "ad alto rischio" nell'adozione di misure protettive, di sicurezza, di conformità, trasparenza e tracciabilità rafforzata: si vedano in particolare, senza pretese di esaustività, gli artt. 9 "Sistema di gestione dei rischi in continuo", 11 "Documentazione tecnica", 12 "Conservazione dei log degli eventi", 15 "Accuratezza, robustezza e cyber-sicurezza", 18 "Conservazione dei documenti" e 25 "Responsabilità lungo la catena del valore dell'IA". Analoghe considerazioni valgono per le misure protettive, di sicurezza, di conformità, trasparenza e tracciabilità rafforzata richieste per i modelli di AI per finalità generali con rischio sistemico (art. 55 AI Act).

Così pure prima di utilizzare sotto la propria autorità un AI "ad alto rischio" in attuazione dei principi ordinatori di accountability e gestione differenziata del rischio occorre predisporre un'accurata preliminare "Valutazione d'impatto dei diritti fondamentali per i sistemi ad altro rischio" ai sensi dell'art. 27 dell'AI Act che

statuisce quanto segue: «prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre».

Last but non least, "il principio di tutela della riservatezza, qualità dei dati personali e *data governance*" relativo alle AI "ad alto rischio": art 10 *AI Act*. Si veda in particolare il considerando 67 che precisa quanto segue: «Il requisito secondo cui i set di dati dovrebbero essere, per quanto possibile, completi ed esenti da errori non dovrebbe incidere sull'uso di tecniche di tutela della vita privata nel contesto dello sviluppo e della prova dei sistemi di IA. In particolare i set di dati dovrebbero tenere conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, contestuale, comportamentale o funzionale nel quale il sistema di IA ad alto rischio è destinato a essere usato. I requisiti relativi alla governance dei dati possono essere soddisfatti ricorrendo a terzi che offrono servizi di conformità certificati, compresa la verifica della governance dei dati, dell'integrità dei set di dati e delle pratiche di addestramento, convalida e prova dei dati, purché sia garantita la conformità ai requisiti in materia di dati di cui al presente regolamento»; con il corollario dell'innovativo "principio di standardizzazione dei dati di addestramento".

Il principio di standardizzazione dei dati di addestramento si applica alla conformità normativa nell'ambito dell'AI Act e riguarda la trasformazione dei dati in un formato coerente e uniforme per garantire una buona qualità e affidabilità nel processo di training dei modelli di intelligenza artificiale.

In particolare l'innovativo "principio di standardizzazione dei dati di addestramento" nell'AI Act si evince dall'art. 10 dell'AI Act che richiede per le AI ad alto rischio che i set di dati per addestramento, convalida e test siano soggetti a pratiche di governance e gestione che assicurino la qualità, l'origine, la pertinenza e la rappresentatività dei dati in modo appropriato agli scopi del sistema e dall'art. 53, comma 1, lett. d) che richiede ai fornitori delle AI per finalità generali di fornire una sintesi sufficientemente dettagliata dei dati utilizzati per l'addestramento dei modelli di intelligenza artificiale[7].

[7] L'art. 40 dell'AI Act statuisce che: «I sistemi di IA ad alto rischio o i modelli di IA per finalità generali che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea conformemente al regolamento (UE) n, 1025/2012 si presumono conformi ai requisiti di cui alla sezione 2 del presente capo o, se del caso, agli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento, nella misura in cui tali requisiti o obblighi sono contemplati da tali norme». Si sottovaluta spesso che l'AI Act si inserisce nella cornice del *New Legislative Framework* (NLF) UE (Reg. UE

I set di dati di addestramento devono rispettare requisiti rigorosi di qualità, trasparenza e gestione durante tutte le fasi del ciclo di vita del dato, dal *pre-training* al *fine-tuning* del modello. La standardizzazione è parte integrante di questo processo, in quanto permette di eliminare *bias*, fornire dati coerenti e affidabili, fondamentali per l'efficacia e la correttezza dei modelli di AI.

Il principio di standardizzazione è essenziale per assicurare che i processi di addestramento AI siano conformi all'AI Act e al GDPR, trasparenti, e affidabili, e che rispettino gli obblighi di protezione dei dati e di equità previsti dalla normativa europea. La standardizzazione dei dati agevola inoltre audit interni e da parte di revisori terzi indipendenti.

5. – Un primo aspetto positivo è che disponiamo ora di un quadro certo di regole, marcatamente antropocentrico, cui fare riferimento in un momento tecnologico di grande fermento.

Apprezzabile è l'introduzione di precetti normativi certi e vincolanti integrati, ma non sostituiti, da codici di condotta co-regolamentati e non certo autodisciplinati da codici autoreferenziali.

Ulteriore aspetto positivo che emerge dall'analisi comparata dei due testi normativi – GDPR e AI ACT – è che certamente la protezione dei dati personali rimane centrale e non recede rispetto all'AI: prevale dunque sempre il GDPR.

Un terzo aspetto, almeno parzialmente, positivo riguarda certamente la statuizione del "principio *human in the loop* per le AI ad alto rischio" (art. 14 AI Act).

Parzialmente perché manca un principio generale di sorveglianza umana – che nella formulazione attuale è per legge limitato alle sole AI ad alto rischio – a tutte le attività decisorie algoritmiche delegate ad intelligenze artificiali.

Non sfuggono tuttavia diverse criticità, anche a prima lettura.

Innanzitutto, una critica all'arco temporale di entrata in vigore eccessivamente differenziato e dilatato nel tempo.

La maggior parte delle nuove regole andrà a regime dopo 24 e addirittura 36 mesi per le AI "ad alto rischio": un periodo davvero troppo lungo, inaccettabile, che mette a rischio di obsolescenza una normativa così dipendente dall'evoluzione tecnologica.

Almeno i divieti relativi a pratiche vietate saranno efficaci solo 6 mesi dopo l'entrata in vigore.

765/2008). Questo quadro normativo è stato pensato per armonizzare le normative tecniche, semplificare il controllo di conformità dei prodotti all'interno del Mercato Unico Europeo e introdurre una politica comune sulla sorveglianza del mercato, focalizzando l'attenzione sull'applicazione delle normative durante l'intero ciclo di vita dei prodotti. Allo stato tali norme armonizzate non sono ancora state pubblicate creando problemi applicativi di non poco momento.

I codici di buone pratiche verranno implementati non prima di 9 mesi.

Le norme sui sistemi di IA per finalità generali (*General Purpose AI Systems*), incluse quelle relative alla governance, saranno in vigore dopo 12 mesi.

Una seconda criticità – riguarda ad avviso dello scrivente – l'ambito di applicazione che con un errore di prospettiva di non poco momento esclude due settori strategici piuttosto pericolosi:

– sistemi utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale;

– sistemi di intelligenza artificiale utilizzati solo a scopo di ricerca e innovazione.

Qualche dubbio anche per l'esclusione dell'utilizzo dell'AI per scopi non professionali: forse sarebbe stato il caso di precisare espressamente, sebbene possa apparire ovvio, ma in questo contesto estremamente nuovo e per certi aspetti imprevedibile non è opportuno dare nulla per scontato, purché trasparente e lecito considerate le molteplici finalità illecite che potrebbero non sempre rilevare sotto il profilo penalistico.

Proprio l'utilizzo di AI per scopi militari è stato giustamente stigmatizzato anche dal Santo Padre al G7 ospitato dall'Italia con un fermo monito al divieto di armi automatizzate per uccidere senza sorveglianza umana.

Così pure non convince del tutto l'assenza di principi generali applicabili anche alle AI a rischio minimo che paiono disinteressare il legislatore europeo, forse con un pericoloso difetto di regolazione.

Anche l'approccio del legislatore ai profili della tutela dei diritti fondamentali pare ben più timido rispetto al GDPR.

Le esigenze e i rischi dell'uso dell'intelligenza artificiale variano in modo significativo a seconda che ciò avvenga in un ambiente privato o in un contesto accessibile al pubblico.

Le eccezioni di cui all'articolo 5, paragrafo 1, lettera d), per l'uso di applicazioni biometriche di identificazione remota in tempo reale in spazi accessibili al pubblico a fini di contrasto sono di portata eccessiva e non corrispondono un'ingerenza proporzionata nei diritti fondamentali dei cittadini.

Anche l'uso di applicazioni biometriche di identificazione remota a fini di contrasto costituisce un'ingerenza intensiva nei diritti fondamentali dei cittadini e avrebbe pertanto dovuto essere incluso nell'elenco delle pratiche vietate di cui all'articolo 5.

La classificazione come applicazione di IA ad alto rischio non pare sufficiente al potenziale di rischio associato all'uso di tali applicazioni.

L'articolo 54, paragrafo 1, prevede un'autorizzazione generale, indifferenziata e orizzontale al trattamento dei dati personali nell'ambito di test reali.

Dal punto di vista della protezione dei dati, questa disposizione è troppo vaga e non può costituire una base giuridica per il trattamento dei dati compatibile con il GDPR.

Il riutilizzo dei dati personali raccolti per uno scopo specifico, per finalità che non sono in alcun modo correlate allo scopo della raccolta, non è in alcun modo prevedibile per l'interessato.

Nella misura in cui la disposizione è intesa come una forma di "riutilizzo compatibile" ai sensi dell'articolo 6, paragrafo 4, del RGPD, l'articolo 54, paragrafo 1, non è una misura necessaria e proporzionata in una società democratica per proteggere gli obiettivi di cui all'articolo 23, paragrafo 1, conformemente all'articolo 6, paragrafo 4, del RGPD.

Inoltre, la norma dell' AI Act citata non distingue tra categorie particolari di dati personali ai sensi dell'articolo 9, paragrafo 1, del GDPR e altri dati personali.

L'articolo 54, paragrafo 1, pare difficilmente compatibile con il principio minimizzazione dei dati personali ai sensi dell'articolo 5, paragrafo 1, lettera c), del GDPR, in quanto né l'ambito né le categorie di dati personali potenzialmente trattati in laboratori reali sono limitati in alcun modo.

E ancora ai sensi dell'articolo 47 della legge europea sull'IA, i fornitori di sistemi di IA ad alto rischio sono tenuti a redigere vari documenti denominati congiuntamente "dichiarazione di conformità UE". Questi documenti saranno tenuti a disposizione delle autorità nazionali competenti 10 anni[8].

L'aspetto interessante è che l' Allegato IV spiega cosa deve includere questa "dichiarazione di conformità UE". Il paragrafo 5 prevede quanto segue:

«Se un sistema di IA comporta il trattamento di dati personali, una dichiarazione che attesti che tale sistema di IA è conforme ai regolamenti (UE) 679/2016 e (UE) 1725/2018 e alla direttiva (UE) 680/2016».

È chiaro che questa norma è stata redatta con una logica di conformità alla sicurezza dei prodotti e senza valutare una piena compatibilità con la protezione dei dati personali.

Non può essere il "sistema" — che sia AI o meno — ad essere oggetto di valutazione di compatibilità preventiva con il GDPR, se non in linea del tutto teorica, quindi, priva di rilevanza, ma semmai solo i trattamenti dei dati personali effettivamente operati, in concreto, con quel sistema.

[8] Art. 47 AI Act: «Il fornitore compila una dichiarazione scritta di conformità UE leggibile meccanicamente, firmata a mano o elettronicamente, per ciascun sistema di IA ad alto rischio e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio. La dichiarazione di conformità UE identifica il sistema di IA ad alto rischio per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è presentata alle pertinenti autorità nazionali competenti».

La conformità al GDPR è sempre riferibile ai trattamenti di dati personali effettuati. Risulta evidente che non si può garantire con una dichiarazione generale *ex ante* che un sistema di IA sarà sempre conforme al GDPR senza prevedere le tipologie di trattamenti che potranno essere effettuati e le categorie di dati personali utilizzate (comuni oppure anche particolari).

Sarebbe stato forse più opportuno formulare la norma, fermo restando che la conformità operativa dell'AI al GDPR non può che verificarsi in relazione ai trattamenti di dati personali effettivamente operati, richiamando espressamente l'osservanza già in fase di sviluppo ai precetti conformativi generali del "principio di minimizzazione dei dati personali" (art. 5 lett. *c*) GDPR) e della "*privacy by design* e *by default*" (art. 25 GDPR) nello sviluppo e utilizzo delle AI.

Per analizzare se le attività di trattamento dei dati personali sono conformi, le diverse fasi di vita di un sistema di IA devono essere suddivise (ad esempio, sviluppo iniziale, formazione, implementazione, utilizzo dopo l'implementazione) e analizzate dettagliatamente.

L'AI Act pare meno incisivo rispetto al GDPR nella protezione dei diritti fondamentali e più incline ad assecondare le logiche di mercato.

6. – L'AI Act si segnala, pur nella sua complessità per certi aspetti ridondante e preludio di un rischio di "iper-regolazione" in fase attuativa, per la marcata prospettiva antropocentrica pur senza tentare, con esito non particolarmente felice in un contesto di *compliance* altamente burocratizzato con competenze frammentate tra troppe Autorità, di assicurare anche lo sviluppo e la diffusione delle AI.

Il considerando 27 dell'AI Act evidenzia che: «Sebbene l'approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un'IA affidabile del 2019 elaborati dall'AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che sono intesi a contribuire a garantire che l'IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. Fatti salvi i requisiti giuridicamente vincolanti del presente regolamento e di qualsiasi altra disposizione di diritto dell'Unione applicabile, tali orientamenti contribuiscono all'elaborazione di un'IA coerente, affidabile e antropocentrica, in linea con la Carta e con i valori su cui si fonda l'Unione»: tali principi riecheggiano quelli statuiti dall'AI Act sebbene il regolamento europeo rinuncia a una declaratoria di applicazione universale a tutte le AI prediligendo una parcellizzazione regolatoria[9].

[9] Secondo gli orientamenti dell'AI HLEG con "intervento e sorveglianza umani" si intende che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter

Tuttavia, la tutela dei diritti fondamentali è recessiva rispetto al modello del GDPR essendo semmai prevalente nell'AI Act la conformità a standard e certificazioni di prodotto, strumenti utilissimi ma che non sono automaticamente protettivi della persona, dei dati personali e in ultima istanza della dignità personale.

Come si è osservato *supra* l'AI Act rinuncia a una declaratoria dei principi applicabili a tutte le AI. Principi che pure sono, tuttavia, rilevabili da una attenta lettura sistematica assiologica costituzionalmente orientata: si pensi per tutti al "principio di *accountability*, gestione del rischio e trasparenza".

In tale prospettiva si segnalano la necessità di superamento interpretativo di taluni limiti normativi letterali relativi al rispetto limitato alle AI "ad alto rischio": il pensiero corre al rilevantissimo "principio dell'autonomia decisionale umana" e al "principio di tutela della riservatezza" e "qualità dei dati personali". Si tratta di limiti formali irrazionali, superabili in via interpretativa, in attuazione dei generali principi superiori di ragionevolezza, proporzionalità e solidarietà, in ossequio a lettura sistematica assiologica italo-europea, costituzionalmente orientata, a tutela dei diritti fondamentali della persona.

Il rispetto dell'autonomia decisionale umana, la tutela della riservatezza, la tutela e qualità la qualità dei dati personali devono essere giustamente osservati sempre e comunque in tutti i contesti di sviluppo, immissione sul mercato e impiego sotto la propria autorità di sistemi di AI, parendo irragionevole il contrario, a

essere adeguatamente controllati e sorvegliati dagli esseri umani. Con "robustezza tecnica e sicurezza" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire la robustezza nel caso di problemi e resilienza contro i tentativi di alterare l'uso o le prestazioni del sistema di IA in modo da consentire l'uso illegale da parte di terzi e ridurre al minimo i danni involontari. Con "vita privata e governance dei dati" si intende che i sistemi di IA sono sviluppati e utilizzati nel rispetto delle norme in materia di vita privata e protezione dei dati, elaborando al contempo dati che soddisfino livelli elevati in termini di qualità e integrità. Con "trasparenza" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i *deployer* delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti. Con "diversità, non discriminazione ed equità" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da includere soggetti diversi e promuovere la parità di accesso, l'uguaglianza di genere e la diversità culturale, evitando nel contempo effetti discriminatori e pregiudizi ingiusti vietati dal diritto dell'Unione o nazionale. Con "benessere sociale e ambientale" si intende che i sistemi di IA sono sviluppati e utilizzati in modo sostenibile e rispettoso dell'ambiente e in modo da apportare benefici a tutti gli esseri umani, monitorando e valutando gli impatti a lungo termine sull'individuo, sulla società e sulla democrazia. L'applicazione di tali principi dovrebbe essere tradotta, ove possibile, nella progettazione e nell'utilizzo di modelli di IA. Essi dovrebbero in ogni caso fungere da base per l'elaborazione di codici di condotta a norma del presente regolamento. Tutti i portatori di interessi, compresi l'industria, il mondo accademico, la società civile e le organizzazioni di normazione, sono incoraggiati a tenere conto, se del caso, dei principi etici per lo sviluppo delle migliori pratiche e norme volontarie.

prescindere dalla classificazione del rischio dell'AI come limitato o basso e a prescindere dalla sovrapposizione prevalente dei precetti inderogabili del GDPR

L'AI Act pare, inoltre, cedere in diversi non condivisibili passaggi alle tentazioni mercatorie.

Alcuni spunti di riflessione in tal senso:

— disinteresse per AI a rischio minimo o nullo;

— divieti limitati in relazione, per esempio, alla sorveglianza biometrica nelle aree accessibili al pubblico ma ignorati nelle aree private;

— la maggior parte dei requisiti si applicano fondamentalmente solo all'IA ad alto rischio, ad eccezione dell'articolo 6(3) delle deroghe e alcune IA già immesse sul mercato;

— tra l'IA ad alto rischio, abbiamo qualche IA controversa, come i rilevatori di menzogne; noleggio-*tech* con riconoscimento delle emozioni; polizia predittiva basata sui big data profiling;

— la marcatura CE non significa di per sé "AI legale", dal momento che il *deployer* deve ancora garantire il rispetto delle leggi applicabili, compresa, *ex multis*, la protezione dei dati personali ai sensi del GDPR.

Infine, non condivisibili tempistiche applicative eccessivamente ritardate per le AI già immesse sul mercato, ben oltre il normale "termine di grazia".

L'AI Act prevede, all'articolo 111, dei termini entro i quali i sistemi di IA già immessi sul mercato o messi in servizio devono conformarsi ai requisiti e agli obblighi ivi previsti.

In particolare, fatta salva l'applicazione delle disposizioni di cui all'articolo 5 ("Pratiche di IA vietate"), a partire da 6 mesi dalla data di entrata in vigore dell'AI Act:

- i sistemi di IA che costituiscono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'Allegato X e che sono stati immessi sul mercato o messi in servizio prima di 36 mesi dalla data di entrata in vigore dell'AI Act, devono essere resi conformi all'AI Act entro il 31 dicembre 2030;
- l'AI Act si applica agli operatori di sistemi di IA ad alto rischio, diversi dai sistemi descritti nel precedente punto, che sono stati immessi sul mercato o messi in servizio prima di 24 mesi dalla data di entrata in vigore della legge stessa, solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione.

Nel caso di sistemi di IA ad alto rischio destinati ad essere utilizzati da parte delle autorità pubbliche, i fornitori e i *deployer* di tali sistemi dovranno adottare le misure necessarie per conformarsi ai requisiti e agli obblighi previsti dall'AI Act entro 6 anni dalla sua entrata in vigore.

L'articolo 111 prevede altresì che i fornitori di modelli GPAI immessi sul mercato prima di 12 mesi dalla data di entrata in vigore dell'AI Act adottino le misure

necessarie per conformarsi agli obblighi della legge stessa entro 36 mesi dalla sua entrata in vigore.

Nonostante quanto rilevato, tra luci e ombre, allo stato rimane comunque uno degli atti legislativi più avanzati al mondo per quanto riguarda il riconoscimento e la protezione delle vulnerabilità umane nel contesto relazionale tecnologico digitale.

I presidi a tutela della dignità della persona oltre che dei suoi dati personali e degli altri diritti fondamentali, nel contesto tecnologico digitale, presente e ancor più in futuro, devono essere sempre meno affidati esclusivamente alle scelte di autodeterminazione individuale e sempre più a una dimensione di etero-conformazione dettata dai precetti di legge inderogabili e di tutela collettiva di categorie di soggetti vulnerabili.

Occorre, dunque, a prudente avviso di chi scrive, demitizzare il ruolo giuridico delle scelte individuali dell'autodeterminazione informativa e del consenso nel contesto digitale fortemente asimmetrico e aggravato dalla crescente diffusione delle AI: pare, invero, necessario spostare l'attenzione sempre più verso tutele e rimedi meta-individuali, prevedendo sanzioni amministrative e rafforzando obblighi generalizzati di *accountability*, *compliance* e *audit* indipendenti dei *big tech* a prescindere dalle scelte individuali del singolo soggetto.

Per sottrarsi al rischio di dominio opaco dell'algoritmo, si registra, come già nel contesto del GDPR, anche e soprattutto per la crescente diffusione delle AI, a protezione della persona e dei diritti fondamentali, secondo una lettura assiologica italo-europea costituzionalmente orientata, la necessità di rafforzare le regole di *accountability*, *compliance*, *audit*, responsabilità e sanzionatorie, anche in relazione al "rapporto privatistico" come già utilmente operato nell'esperienza consumeristica delle pratiche commerciali scorrette.

Il genere umano deve sottrarsi all'effimera seduzione commerciale della "privatizzazione della conoscenza" di AI generativa magnificate per creare rapidamente opere d'arte di ogni genere – musicale, grafico-pittorico e letterario – al nostro posto costringendoci a continuare a svolgere attività manuali ripetitive e noiose.

Una rivoluzione tecnologica antropocentrica e sostenibile deve semmai proteggere e valorizzare la dignità umana e tutelare l'ambiente in cui l'uomo vive: consentire di liberare risorse speculative a favore della persona, aumentare il tempo libero dedicato ad attività intellettuali creative in quanto le AI si sostituiranno all'uomo per l'esecuzione di attività manuali, seriali e banali e non consumare inutilmente risorse ambientali preziose.

Non il contrario: la creatività, la conoscenza e il sapere devono rimane patrimonio comune dell'umanità.

Si tratta di coltivare, è il caso di dire con sapienza, un nuovo "umanesimo digitale" a servizio e promozione della libertà, solidarietà e dignità personale come ci insegna la nostra Costituzione e la Carta dei diritti fondamentali dell'Unione Europea: ricordiamocelo sempre.

Occorre tutelare, dunque, in ultima istanza, la dignità della persona nel contesto del mercato asimmetrico digitale delle intelligenze artificiali aderendo pienamente a una lettura sistematica funzionale protettiva rafforzata in conformità al metodo assiologico costituzionalmente orientato nel sistema italo-europeo delle fonti particolarmente fecondo nello specifico contesto di cui trattasi.

Rifuggendo dalla *deregulation* federale statunitense ma senza incorrere nei rischi opposti della soffocante, disordinata e controproducente "iper-regolazione" europea: occorre cercare il giusto equilibrio, la giusta regola, il giusto rimedio, in ossequio ai generali "principi di ragionevolezza, trasparenza, proporzionalità e solidarietà"[10].

Abstract

FIRST REFLECTIONS ON THE PROTECTION OF PERSONS AND PERSONAL DATA BETWEEN GDPR AND AI ACT

Il presente saggio intende formulare prime riflessioni civilistiche relativamente all'AI Act in prospettiva antropocentrica e protettiva dei diritti fondamentali della persona evidenziando il necessario dialogo normativo con il GDPR. Tale prospettiva ricostruttiva assiologica, anche alla luce dei principi generali dell'AI Act, risulta necessaria al fine di assicurare un'effettiva protezione della persona e dei dati personali dalla bulimia di dati utilizzati costantemente per addestrare e ottimizzare le intelligenze artificiali.

***

This essay aims to formulate first civilistic reflections regarding the AI Act in an anthropocentric perspective protective of fundamental human rights, by highlighting the necessary regulatory dialogue with the GDPR. Such a reconstructive axiological perspective, even in the light of the general principles of the AI Act, is necessary in order to ensure effective protection of the person and personal data from the bulimia of data constantly used to train and optimize artificial intelligence.

---

[10] L'espressione "giusto rimedio", frutto dell'interpretazione sistematica e funzionale, in applicazione del metodo assiologico costituzionalmente orientato, che segna il superamento dell'interpretazione esegetica rigidamente formale, si deve a P. PERLINGIERI, *Il "giusto rimedio" nel diritto civile*, in *Giusto proc. civ.*, 2011, 1 ss.; recentemente si vedano S. POLIDORI, *Ragionevolezza, proporzionalità e "giusto rimedio": le tendenze evolutive e un'occasione mancata (dalla Cassazione)*, in G. PERLINGIERI, A. FACHECHI (a cura di), *Ragionevolezza e proporzionalità nel diritto contemporaneo*, Napoli, 2017, II, 907 ss.; e da ultimo F. LONGOBUCCO, *Smart contract e "giusto rimedio civile" del re-coding tra Rule by Design e Rule of Law*, in A. Trezzini (a cura di), *Giornate della Ricerca del Dipartimento di Economia di Roma Tre*, Roma, 2023, 175 ss.