**Audizione sulla proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull’intelligenza artificiale (legge sull’intelligenza artificiale) e modifica alcuni atti legislativi dell’Unione**

**Prof. Avv. Oreste Pollicino**

**Università Bocconi ed Agenzia per la protezione dei diritti fondamentali**

La proposta di Regolamento sull’Intelligenza Artificiale (di seguito, AIA o AI Act) si inserisce nel solco di quell’obiettivo già inaugurato dalla Presidente della Commissione Europea, Ursula Von Der Leyen, la quale, sin dalla sua elezione, ha sottolineato la priorità di delineare un percorso di sviluppo di questi sistemi che non vada a sacrificare né l’innovazione né i diritti fondamentali.

In questo quadro, dunque, si inserisce la proposta in commento, la quale, anche sul piano nazionale, pone delle importanti domande e sfide per il futuro con riguardo al funzionamento e allo sviluppo del mercato interno. Difatti, è negli intrinsechi scopi di un Regolamento quello di istituire un quadro giuridico uniforme e imporre agli Stati Membri una serie di obiettivi che impattino l’interesse pubblico. Una delle finalità dell’AIA è proprio quella di assicurare la promozione del mercato interno per fare dell'industria europea un vantaggio competitivo a livello globale. In quest’ottica, si vieta agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del Regolamento. L’Italia, dal canto suo, ha dato prova di voler dare un contributo significativo a queste necessità, tramite l’adozione della “Strategia sull’Intelligenza Artificiale”. Come è noto, la strategia contiene 24 politiche che hanno lo scopo di aumentare la competitività tecnologica del Paese internazionalmente e di mettere a servizio di alcuni settori chiave le eccellenze della ricerca in campo IA. Il filo conduttore della Strategia parte dall’istruzione e dal plasmare nuove competenze: un aspetto innovativo per l’Italia che, anche nell’ultimo Digital economy and society index (Desi), pubblicato dalla Commissione europea, spicca per le scarse competenze digitali di cittadini, imprese e PA. L’Italia, dunque, può a ben vedere agire come promotore e traghettatore di un’idea che non porti a frammentazione, ma favorisca l’Unione, per assicurare che l’IA faccia bene al mondo della produzione e della ricerca, a quello sociale e a quello ambientale.

Se, da un lato, come si diceva, l’AIA apre all’armonizzazione, d’altro canto, dà anche una libertà significativa con riguardo alle direzioni di mercato degli Stati membri. Questo può creare una frammentazione del mercato unico dell’UE, in contrasto con l’obiettivo dell’AIA di far rispettare le regole orizzontali prima che i paesi inizino a legiferare individualmente. Pur comprendendo la *ratio* specificata dal Considerando 68, ossia che “per motivi eccezionali di pubblica sicurezza o di tutela della vita e della salute delle persone fisiche nonché della proprietà industriale e commerciale, gli Stati membri possano autorizzare l'immissione sul mercato o la messa in servizio di sistemi di IA che non sono stati sottoposti a una valutazione della conformità”,tuttavia, tale previsione fa sorgere, da un lato, una serie di problematiche con riguardo alla *compliance* con le regole del Regolamento stesso, dall’altro, un problema, come si diceva, di frammentazione del mercato. I rinvii ivi messi in rilievo necessitano di una serie di interventi in capo agli Stati Membri, i quali, per garantire un'applicazione razionale delle norme, ed evitare interpretazioni creative e incoerenti, dovranno sviluppare le competenze necessarie in materia di IA e allocare sufficienti risorse umane e finanziarie. Difatti, un’altra delle previsioni della proposta di Regolamento è l’istituzione di uno *European AI Board*: una nuova autorità che, assieme alla Commissione Europea, e in stretta collaborazione con l'industria tecnologica, dovranno svolgere un ruolo chiave nel coordinare e consigliare gli Stati membri, i quali, d’altro canto, dovranno possedere i poteri necessari per assicurare un'applicazione coerente del Regolamento.

La mancanza di raccordo che si è voluto evidenziare emerge anche con riguardo alla scelta della definizione di “sistemi di IA”. Quella proposta dall’art. 3 del Regolamento è: “software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono”. Questa definizione “aperta” sarebbe, come si rileva dall’ explanatory memorandum in apertura della proposta, in grado di garantire la massima conformità ai valori europei.Tuttavia, ad una lettura più attenta, si nota come manchi del tutto il riferimento ai principi costituzionali, se non per il richiamo ai termini “umano” e “dignità”. Se si legge l’art. 3 (1) in combinato disposto con l’Allegato I, si evince come il termine AI comprende praticamente qualsiasi programma di computer, definendo in modo quanto meno ampio (e, dunque, discrezionale), cosa debba essere ricompreso al suo interno, e cosa no. Da un lato, un’ampia definizione di “sistemi IA” può essere giustificata alla luce delle pratiche vietate AI delineate nell’art. 5 AIA per compensare le minacce poste da diversi tipi di software ai diritti fondamentali degli individui. Il discrimine in questo caso non dovrebbe essere sul fatto che tali pratiche vietate sono abilitate dall’apprendimento automatico o logico, quanto piuttosto dal pericolo che pongono ai diritti dei cittadini interessati. I requisiti obbligatori previsti per questi sistemi nel titolo III, capitolo 2, si basano sull'osservazione che un certo numero di diritti fondamentali sono influenzati negativamente, in particolare, dalle caratteristiche speciali del *machine learning*, come l'opacità, la complessità, la dipendenza dai dati. Poiché queste caratteristiche non sono presenti, o lo sono solo in parte, nei semplici algoritmi (basati sulla logica), l’ampia definizione di IA potrebbe portare potenzialmente a una regolamentazione eccessiva.

Un altro aspetto che desidero menzionare riguarda il coinvolgimento degli Stati Membri nel prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, lettera d), e ai paragrafi 2 e 3. A questo riguardo, giova ricordare che l’Italia ha recentemente previsto la sospensione di utilizzazione e installazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici fino al 2023 (si veda art. 9 co. 9 Decreto Capienze, DL 139/2021). Una decisione che potrebbe entrare in contrasto con l’impianto delineato dall’AI Act. Il Regolamento, difatti, pur vietando in via generale l’utilizzo di *biometric identification systems* a meno che tale uso sia strettamente necessario per la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato. Dunque, è possibile parlare di una certa apertura nelle eccezioni delineate dalla Commissione, in cui gli Stati Membri possono definirne l’utilizzoper scopi di pubblica sicurezza/*law enforcement,* come delineati anche dall’omonima Direttiva. Non salvaguarda nemmeno il paragrafo 3 dell’art. 4, ove si prevede che “ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo durante o dopo l'uso”.

Tale apertura, oltre a comportare una serie di problematiche dal punto di vista dei diritti degli individui, ha delle conseguenze, come si diceva prima, anche sul piano del mercato interno, in quanto andrebbe a favorire la frammentazione dell’utilizzo di questi strumenti invasivi e, dunque, la commercializzazione di essi in alcune aree dell’Unione a scapito di altre. Si osserva in tal caso che la proibizione di alcuni usi, a differenza di altri, non viene ben giustificata in nessun tipo. Difatti, senza fare distinzione tra pubblico e privato, se si vogliono abolire determinate pratiche considerate pericolose per i diritti fondamentali degli individui, allora dovrebbero essere applicata tale proibizione dovrebbe essere applicabile a tutti gli usi dei sistemi di IA biometrica - pubblici o privati.Inoltre, le eccezioni individuate dalla Commissione sono troppo ampie, poiché la proposta stabilisce eccezioni non solo per la ricerca di vittime di crimini e la prevenzione di attacchi terroristici, ma anche per l'individuazione di sospetti criminali interessati da una pena detentiva di tre anni. Tale aspetto è di una certa criticità anche secondo l’EDPBS che recentemente ha ordinato all’Europol di cancellare i dati raccolti da individui per i quali non hanno riscontrato alcun legame di attività criminale.

E, venendo anche all’ultimo spettro di problematiche, occorre rammentare che si sta trattando di dati considerati dalla normativa a protezione dei dati personali, in particolare dall’art. 9 del GDPR, dati sensibili. Per questa ragione, possono essere processati alla presenza di determinati requisiti, oltre che previa individuazione in una corretta base giuridica del trattamento (ex art. 6 del GDPR). Tale aspetto sembra entrare in conflitto con la libertà concessa agli Stati Membri di autorizzare utilizzi emergenziali della biometria.

Inoltre, all’interno della normativa a protezione dei dati personali, è possibile rintracciare un obbligo/diritto molto specifico. L’art. 22 del GDPR prevede che “l’interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona”. Pertanto, tale norma assegna all’interessato il diritto di rifiutare l’essere sottoposto a una decisione automatizzata. I problemi con questo articolo sono già allo stato dell’arte numerosi con l’IA, primo per la sua implementazione, secondo perché non troviamo un suo effettivo corrispettivo nella proposta di Regolamento. Difatti, l’art. 22 (1) introduce un meccanismo di contestazione, stabilendo il diritto a non essere soggetti a una decisione basata unicamente su un trattamento automatizzato, e il mancato raccordo con l’IA potrebbe essere problematico in quanto quest’ultima possiede un ambito di applicazione ben più vasto raccogliendo sia dati personali sia dati non personali; secondariamente, quando in contatto con sistemi automatizzati particolarmente complessi, come, ad esempio, il riconoscimento facciale, di cui si è detto sopra, l’art. 22(3) del GDPR non fornisce una protezione sufficiente in quanto una delle problematicità intrinseche di questo tipo di tecnologie è proprio il fatto che l’interessato non è sempre a conoscenza del fatto che sia stato sottoposto a questo trattamento. L’aspetto che, sicuramente, preoccupa maggiormente è che le tecnologie algoritmiche non forniscono solo un “mezzo” per eseguire una decisione presa da un soggetto umano agente, ma, sempre più spesso, sono esse stesse ad assumere decisioni rilevanti per gli esseri umani e le loro libertà.

A tale scopo non sembra, difatti, sorreggere la previsione dell’art. 14 della proposta, ossia la predisposizione di una supervisione umana dell’algoritmo. Anzitutto, questa norma non prevede in alcun modo un effetto intervento da parte dei soggetti interessati. In secondo luogo, vi sono una serie di impraticabilità dal lato tecnico, nel termine di comprendere appieno da parte di un essere umano le capacità e i limiti di un sistema AI ad alto rischio (si veda l’art. 14 (4)(a) dell’AIA). Tale impraticabilità condurrebbe all’imposizione di un divieto indiretto di utilizzo di tali sistemi: se fosse questa l’intenzione della proposta, dovrebbe essere definita a chiare lettere nell’AIA una direzione di questo tipo anche nell’ottica di chiarire ai fornitori di IA fino a che punto possono usare sistemi di AI ad alto rischio opachi.

In terzo luogo, l’art. 14 AIA non specifica quando, come e in quale fase del “trattamento” viene richiesta la supervisione umana, nonché sull’effettivo obbligo in capo agli utenti di garantire la supervisione umana. Dal punto di vista tecnico, una supervisione umana completa deve comportare la supervisione del sistema di IA durante il suo intero ciclo di vita, assicurando misure obbligatorie di trasparenza sull'uso delle applicazioni di IA, comprese le statistiche pubbliche sulle distribuzioni, gli obiettivi, lo scopo e gli sviluppatori.

Le misure previste per garantire la supervisione umana ai sensi dell'art. 14(3) AIA e la disposizione corrispondente dell’art. 14(4) AIA tacciono anche su aspetti come la non discriminazione e l’equità. A questo proposito, sarebbe prudente coinvolgere i “National Centers of Expertise on AI” con un forte impegno e coinvolgimento della società civile, degli organismi di uguaglianza e dei diritti umani per fornire input qualitativi alle misure individuate per garantire la supervisione umana ai sensi dell'art. 14(3) dell’AIA e proporre una proposta di modifica della legge che consenta di valutare i pregiudizi nei sistemi di IA.

In conclusione, un ultimo spunto di riflessione è posto dalla disciplina delle sanzioni. Difatti, il Regolamento assegna agli Stati Membri il compito di “adottare tutte le misure necessarie per assicurare l'attuazione delle disposizioni di cui al presente regolamento, anche stabilendo sanzioni effettive, proporzionate e dissuasive in caso di violazione. Per talune violazioni specifiche, è opportuno che gli Stati membri tengano conto dei margini e dei criteri stabiliti nel presente regolamento. Il Garante europeo della protezione dei dati dovrebbe disporre del potere di infliggere sanzioni pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento” (Cons. 84). Ivi si rinviene un ulteriore possibile terreno di frammentazione. Come menzionato nella sezione 5.3 e nella sezione 5.4, l'AIA non stabilisce forti strutture sanzionatorie, perché prevede principalmente un'autovalutazione interna da parte dei fornitori di IA per i sistemi di IA ad alto rischio, combinata con standard armonizzati che devono essere sviluppati da ESO privati. Anche se si assegna agli Stati membri il potere di prevedere norme sulle sanzioni, e le autorità di sorveglianza del mercato possono richiedere che un sistema di IA non conforme sia ritirato o richiamato dal mercato, questo potrebbe non essere sufficiente a garantire un'applicazione efficace. L'esperienza con il GDPR mostra che un eccessivo affidamento sull'applicazione da parte delle autorità nazionali porta a livelli molto diversi di protezione in tutta l'UE a causa delle diverse risorse delle autorità, ma anche a causa delle diverse opinioni su quando e come (spesso) intraprendere azioni. Inoltre, le autorità degli Stati membri non possiedono gli standard per valutare se i fornitori di sistemi di IA ad alto rischio stanno violando l'AIA. Poiché la proposta non stabilisce alcun requisito preciso per i sistemi AI ad alto rischio, ma lascia questo all'autovalutazione dei fornitori (così come alle organizzazioni di standardizzazione), non ci sono standard (uniformi) secondo i quali l'AIA potrebbe essere applicata, lasciando sostanzialmente gli Stati Membri senza una solida guida su questo tema, imponendo loro un ulteriore sforzo per adattarsi alla struttura del Regolamento.