# Position paper sul disegno di legge recante disposizioni e delega al governo

## *In materia di intelligenza artificiale*

In premessa, osserviamo che il testo oggetto del presente Position Paper è un disegno di legge. Pertanto, siamo consapevoli che nuovi interventi sono **possibili e necessari**. Le osservazioni che seguono servono ad indicare gli elementi che ad avviso di Privacy Network destano preoccupazione e che dovrebbero essere indirizzati dal legislatore.

Le opinioni espresse rappresentano quindi la posizione ufficiale di Privacy Network alla data odierna e sono formulate sulla base della versione attuale del testo.

Invitiamo lettori e stakeholder a considerare questo position paper come un **contributo al dibattito pubblico**, che mira a promuovere una comprensione più approfondita e un'analisi critica della proposta di legge.

# Premesse e aspetti generali

• Emerge una **visione dell'IA** come un'entità a cui vengono attribuite capacità umane e una visione della società e del rapporto uomo-macchina incentrata sull'aspetto tecnologico, ancorché su quello umano, nella quale l'IA è un **essere pensante e non uno strumento al servizio della persona**.

• L'elencazione dei diritti e dei principi fondamentali è un elenco così ridondante da risultare "vuoto". Innanzitutto, il richiamo costante, nei primi articoli della bozza, ad un universo di **principi ammassati l'uno all'altro senza un ordine logico** appare come un esercizio di stile da cui non traspare alcuna reale volontà di dettare specifiche norme di tutela per i cittadini e le cittadine. In secondo luogo, i diritti citati sono già presenti nella Carta dei Diritti fondamentali di Nizza, espressamente richiamata dall'AI ACT, che è atto giuridicamente superiore rispetto a qualsiasi altra norma interna che intenderà legiferare su tematiche già affrontate dal Regolamento Europeo.

• Il documento **non rivela un vero intento regolatorio**; a nostro avviso appare un atto di indirizzo politico; prova ne è che viene rimandato a successivi decreti la regolamentazione dei temi delegati ai Paesi Membri.

• In generale, emerge una scarsa conoscenza dell'attuale contesto tecnico e giuridico, che potrebbe dare vita a **contrastati normativi e incertezza** per gli operatori del settore, evidenziati (ad esempio, dal mancato richiamo alle definizioni previste dall'AI Act)

# Punti specifici

**Art. 1** - L'atto dovrebbe specificamente indicare, in quanto norma gerarchicamente inferiore rispetto al Regolamento Europeo, che lo scopo è **esclusivamente quello di normare gli aspetti delegati** dall'AI ACT all'autonomia legislativa dei Paesi Membri. Più in generale, crediamo che adottare una legge prettamente nazionale, in aggiunta alla normativa europea e alla conseguente legge di attuazione, potrebbe comportare un eccesso di atti normativi e una scarsa coerenza dell'impianto regolatorio. L'indicazione di cui al comma 2, che fa salve le disposizioni della normativa comunitaria, non risulta sufficiente a garantire l'armonizzazione con l'AI Act.

**Artt. 2-3** - A nostro avviso si dovrebbero richiamare le definizioni e i principi generali già indicati all'interno della normativa comunitaria citata, trattandosi quest'ultimo di atto gerarchicamente superiore.

**Art. 4.4** - L'imposizione del consenso dei genitori per l'accesso di minori di anni 14 ai sistemi di IA appare non ragionevole e **difficile da mettere in pratica**. In una società dove l'IA è parte integrante di dispositivi di ogni tipo (anche e soprattutto appartenenti all'Internet of Things) verificare costantemente l'età di chi accede a questi sistemi e raccogliere la volontà dei genitori risulterebbe complesso e poco utile. Simili considerazioni si possono applicare anche all'utilizzo dell'IA nei sistemi educativi. Diversamente, riteniamo utile imporre speciali condizioni per il **trattamento dei dati personali dei minori** nel contesto dell'utilizzo di sistemi di Intelligenza Artificiale (circostanza cui pare riferirsi la seconda parte del comma 4).

**Art. 5, co.1 lett. d)** - Privilegiare sistemi di IA con data center in Italia nelle attività di procurement appare un elemento anacronistico e assolutamente **contrario all'idea di mercato comune europeo**. Anche le imprese italiane gioverebbero di una maggiore interoperabilità tra dataset europei, ad esempio, in fase di training (si pensi al framework del federated learning). Questa disposizione non pare tenere conto nelle normative che garantiscono livelli di sicurezza e protezione dei dati personali all'interno dello Spazio Economico Europeo.
• Al contrario, riteniamo necessario ed urgente che il processo di selezione dei fornitori della Pubblica Amministrazione tenga conto

delle necessità di ricorrere a strumenti legali ed etici, conformi alla normativa e agli standard di settore. Alle PA dovrebbe essere richiesto di individuare fornitori che garantiscano tali requisiti e le piattaforme e-procurement orientate in questo senso.

**Art. 7** - L'articolo parla di accessibilità ma si discosta sostanzialmente da come il termine viene inteso sia in ambito di ricerca IA, che all'interno dell'AI Act. L'articolo di per sé sembra essere **ridondante** (come anche l'Art 23 al Capo IV) in quanto ripete richieste dell'AI Act (vedasi Art. 52 sulla disclosure dell'interazione con tutti i sistemi IA, non solo quelli da altro rischio) con un focus in ambito sanitario, la quale casistica già rientra nel novero dei sistemi di IA ad "alto rischio" indicati nell'Annex III dell'AI Act. Tale 'ridondanza' riguarda potenzialmente tutto il Capo II.

**Art. 8.2** - Le disposizioni sono in chiaro contrasto con i principi del Reg. UE n. 2016/679 (GDPR) e con i principi di informativa e trasparenza citati dalla norma stessa. In particolare, il dominio del trattamento dei dati personali in ambito di ricerca è già ampiamente coperto dallo stesso GDPR, oltre che dalle linee guida e provvedimenti del Garante Italiano ed europeo. A tal proposito il disegno di legge, al comma 2 dello stesso articolo, **dimentica in modo preoccupante** come qualsiasi uso di dati personali, anche secondario rispetto alla finalità principale, debba comunque essere effettuato nel rispetto dei principi di privacy by design e by default e in ogni caso con l'implementazione di adeguate misure tecniche e organizzative.

***Inoltre***, il riferimento a "dati personali privi degli elementi identificativi diretti" nell'ambito della ricerca e sperimentazione scientifica, "ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base" desta molta **preoccupazione per una serie di motivi**: innanzitutto la de-identificazione non equivale ad anonimizzazione, per cui il legislatore sembra dimenticarsi i preoccupanti e crescenti rischi di "linkability", vale a dire quegli episodi di re-identificazione della persona interessata, mediante specifiche combinazioni di attributi raccolti in altri e distinti dataset. Come noto, non è vietato l'utilizzo di dati pseudonimizzati in ambito di ricerca, ma in ragione del rischio di linkability prima menzionato - dovuto anche alla odierna potenza computazionale dei sistemi IA, in grado di effettuare correlazioni tra i

dati neppure immaginabili qualche anno fa - riteniamo che il Disegno di Legge avrebbe dovuto piuttosto porre l'accento su altri aspetti; prima di tutto **incentivare l'uso di PETs** (Privacy Enhancing Technologies) e di misure di sicurezza di avanguardia nella protezione dei dati personali, tanto più se si fa esplicito riferimento anche ai dati particolari di cui all'art. 9 Reg. UE n. 679/16.

**Art. 12** - Sebbene il comma 1 dell'articolo sia condivisibile, problemi interpretativi nasceranno certamente in relazione al comma 2 che prescrive di informare, nell'ambito delle attività professionali intellettuali, i clienti in merito all'uso di sistemi di IA. Non solo non è chiaro quindi se qualsiasi utilizzo dovrà essere "denunciato", o solo quando prevalente e determinante ai fini dell'attività professionale in oggetto, ma rimane un'area grigia anche in termini di verifica dell'effettivo utilizzo e sanzionabilità in caso di mancata comunicazione. Alla luce del largo utilizzo di sistemi di IA in tutti i settori professionali, un articolo così **generico** produrrà incertezza e confusione che riteniamo opportuno sia chiarita al più presto.

**Art. 14** - Riteniamo che debba essere **riformulato il primo comma**, nella parte in cui si autorizza l'uso di sistemi IA per la ricerca giurisprudenziale e dottrinale. In particolare, il legislatore non sembra tenere conto dell'attuale capacità dell'IA generativa: la risposta ai prompts, creati da giudici ed altri collaboratori giudiziari, sarà infatti sempre di carattere interpretativo; non si dovrebbe infatti associare l'IA generativa ad un semplice database di ricerca. Proponiamo dunque come nuova formulazione della finalità la seguente dicitura: "*per assistere l'interpretazione giurisprudenziale e dottrinale*".

**Art. 18** - L'indicazione dell'AGID e ACN come autorità competenti è un passo indietro rispetto alla richiesta della società civile (PN + TheGoodLobby + Hermes) di **designare un'Autorità indipendente**. Come già osservato, l'AgID non fornisce i requisiti essenziali di indipendenza necessari per garantire imparzialità nell'applicazione della legge.

**Art. 22** - La delega al Governo per adottare decreti legislativi atti ad adeguare l'ordinamento interno all'AI ACT europeo è piuttosto singolare. Riteniamo infatti che sarebbe dovuto essere lo scopo primario di questo stesso disegno di legge.

**Art. 23** - L'introduzione di **obblighi di watermarking** e labelling di contenuti generati - anche solo parzialmente - con IA risulta estremamente **debole** proprio in quanto non viene definito un quadro di riferimento che consideri modalità di comunicazione, evoluzioni tecnologiche, conseguenza specifiche in caso di violazione. Il tema è al centro di un dibattito internazionale che ha visto anche il legislatore europeo poco propenso ad indicare modalità concrete di pubblicità. Rimane fondamentale definire una standard e delle metriche omogenee e consistenti che permettano la tutela dei consumatori.

**Art 24** - Nonostante l'esplicita esclusione di una tutela intellettuale su opere create completamente o parzialmente con l'utilizzo di modelli di IA, sulla questione della violazione o meno di diritti di proprietà intellettuale nei dati usati per training AI manca ancora quella presa di posizione utile a dirimere una questione centrale del mercato dell'IA:

• L'indicazione secondo la quale l'estrazione, la riproduzione e l'estrazione di dati (Text & Data Mining) è legittima fintanto che i diritti non sono stati riservati dei titolari lascia ancora adito a zone d'ombra. La scelta potrebbe essere strategica per lasciar spazio interpretativo in sede giudiziale, ma **non tiene conto** degli effettivi diversi livelli di tutela possibili e della fluidità intrinseca della tutela del diritto d'autore.

**Art. 25.3** - La sanzione da euro 51 a euro 2.065 per le attività di Text & Data Mining (di cui all'articolo precedente) in violazione dei relativi articoli della legge sul diritto d'autore, appare **irrisoria** e priva di concreti effetti dissuasivi.

# La nostra richiesta

Riteniamo, in linea generale, che le disposizioni del presente testo sarebbero dovute essere inserite all'interno della normativa di recepimento dell'AI Act, in modo da garantire una maggiore riflessione sul tema, un attento confronto con gli stakeholders e una migliore armonizzazione tra normativa nazionale e comunitaria (ribadendo, che la seconda costituisce fonte di rango superiore rispetto alla prima).

Pertanto, chiediamo al Governo e al Parlamento (i) di **coinvolgere le parti sociali** nella definizione finale del testo in oggetto, valutando anche **l'adozione di un documento unitario** per recepimento AI Act e normazione italiana, e (ii) di lavorare insieme per elaborare una legge che sia realmente utile a chiarire alcune delle numerose zone d'ombra legate allo sviluppo ed utilizzo di sistemi di IA, senza invece creare maggiore incertezza o rischiare di non tutelare adeguatamente i diritti dei consumatori e delle consumatrici italiane. Riteniamo, inoltre, che i seguenti punti dovrebbero essere indirizzati all'interno della normativa nazionale in materia:

• Designazione di **un'autorità di controllo indipendente** incaricata *dell'enforcement* dell'AI Act, una volta recepito;

• Previsione di **fondi e risorse** per la diffusione di programmi di sensibilizzazione e formazione, sia tra i cittadini e le cittadine italiane che tra le aziende e le Pubbliche Amministrazioni, volti a incoraggiare l'utilizzo responsabile degli strumenti di Intelligenza Artificiale;

• Obbligo di inserire il requisito di **sistemi di IA legali, etici e robusti** nelle gare d'appalto delle Pubbliche Amministrazioni.

***Andrea Baldrati:*** *Presidente****; Gabriele Ientile:*** *Legal Officer****;***

***Bianca Stella Bruschi:*** *Legal Officer****; Luna Bianchi:*** *Legal Officer****;***

***Gabriele Tori:*** *Legal Officer*