Anitec-Assinform

Position paper

Osservazioni sullo schema di D.lgs in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità penale e civile (A.G. 418)

Anitec-Assinform condivide l'obiettivo di garantire la sicurezza dei sistemi di intelligenza artificiale. Si osserva, in via preliminare, che il settore è già oggi destinatario di una significativa stratificazione di obblighi regolatori - dall'AI Act alla disciplina su dati personali, cybersicurezza e responsabilità da prodotto - a fronte di standard armonizzati non ancora disponibili. L'introduzione di ulteriori livelli di responsabilità penale e civile, ove non proporzionati e coordinati con il quadro esistente, rischia di **accrescere tale pressione regolatoria, con effetti negativi sulla competitività degli operatori e sull'attrattività del Paese** in un settore strategico per la crescita europea.

In tale prospettiva, si segnala che il Titolo II, nella formulazione attuale, rischia di introdurre un regime di responsabilità penale e civile più esteso di quanto previsto dal regolamento (UE) 2024/1689, di sovrapporsi a strumenti di tutela già esistenti nel diritto dell'Unione e di generare un'incertezza giuridica tale da **disincentivare l'offerta di intelligenza artificiale in Italia**. Per non incorrere in responsabilità penale e civile gli operatori nazionali ridurrebbero gli investimenti in ricerca e sviluppo, mentre i fornitori internazionali potrebbero non considerare il mercato italiano per i propri prodotti. Al tempo stesso, **la Pubblica Amministrazione, che si sta preparando a adottare nuove tecnologie di IA per migliorare i propri servizi, sarebbe sottoposta a un regime stringente** che penalizzerebbe la trasformazione in atto e ne rallenterebbe l'adozione.

Un intervento nazionale che ecceda il perimetro fissato dalla normativa europea espone il Decreto a un rischio di censura in sede europea e a successive esigenze di correzione, con un ulteriore effetto di incertezza a carico degli operatori. Appare pertanto opportuno che **lo schema si mantenga entro gli spazi di intervento che il Regolamento riserva al legislatore nazionale**.

Il provvedimento interviene in una fase decisiva per il mercato digitale italiano. Nel 2025 il mercato ha raggiunto 84.420[1] milioni di euro (+3,4%) e l'intelligenza

[1] Dati da "Il Digitale in Italia 2026", Anitec-Assinform.

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967

artificiale ne rappresenta la componente più dinamica, con un valore di 1.380 milioni di euro e una crescita del 47,6% su base annua. L'adozione resta però fragile e diseguale - solo il 16,4% delle imprese con almeno dieci addetti utilizza tecnologie di IA, con un divario netto tra grandi imprese (53,1%) e PMI (15,7%) - e l'impulso del PNRR è destinato a esaurirsi entro il 2027.
Un regime di responsabilità che ecceda il quadro europeo rischia di aggravare tali dinamiche, frenando l'adozione dell'IA proprio nella fase in cui il Paese dovrebbe accelerarla e gravando in misura asimmetrica sulle imprese di minori dimensioni.

1. CRITICITÀ PRINCIPALI

1.1. Titolo I: utilizzo dei sistemi di IA per l'attività di polizia

Collaborazioni per ricerca e sperimentazione. La previsione secondo cui la titolarità dei modelli addestrati su dati operativi sensibili deve in ogni caso appartenere alle Forze di polizia merita un chiarimento in punto di proprietà intellettuale. **Occorre in particolare evitare dubbi circa la sorte della tecnologia preesistente, del know-how, dei modelli di base e degli altri asset proprietari sviluppati dagli operatori privati prima o indipendentemente dalla collaborazione**, la cui titolarità deve restare impregiudicata. In assenza di tale chiarimento, il rischio è quello di disincentivare la partecipazione degli operatori privati alle collaborazioni con le Forze di polizia.

Requisiti tecnici, accuratezza e bias. La previsione che demanda a un successivo decreto ministeriale l'individuazione di requisiti tecnici minimi di affidabilità e accuratezza, nonché delle relative soglie operative, appare in tensione con l'impostazione dell'AI Act, che è basata sul rischio e non prevede soglie di accuratezza armonizzate applicabili in modo uniforme a tutte le tipologie di sistemi. Sarebbe auspicabile mantenere un approccio fondato sul contesto d'uso, sul livello di rischio e sullo stato dell'arte, evitando l'introduzione di parametri tecnici rigidi, suscettibili di discostarsi dall'impianto europeo o di risultare rapidamente superati dall'evoluzione tecnologica.

Identificazione biometrica remota e riconoscimento facciale. Pur condividendo l'impostazione generale delle disposizioni, sostanzialmente allineata alle deroghe e alle garanzie previste dall'AI Act, **si suggerisce di verificare che i concetti utilizzati dal legislatore nazionale - quali quelli relativi alle "banche dati adeguate" di riferimento o ai requisiti tecnici dei sistemi - non introducano standard nazionali autonomi** o criteri interpretativi suscettibili di discostarsi dal quadro armonizzato europeo. In un settore particolarmente sensibile, è opportuno mantenere il massimo allineamento possibile alle definizioni, alle condizioni e alle garanzie dell'AI Act.

1.2. Titolo II: Disposizioni civili, penali e processuali, in materia di realizzazione e impiego dei sistemi di IA

1.2.1. Certezza del diritto e assenza di un porto sicuro (safe harbour)

Il regolamento (UE) 2024/1689 (di seguito "AI Act") costituisce la norma che, nel mercato unico, stabilisce i requisiti armonizzati di sicurezza dei sistemi di intelligenza artificiale, affidandone la declinazione tecnica alle standard armonizzati in corso di elaborazione da parte degli organismi europei di normazione (CEN-CENELEC), non ancora disponibili. In tale contesto, lo schema di decreto introduce conseguenze di natura penale e civile **senza fornire ai destinatari parametri di riferimento oggettivi e senza riconoscere alla conformità al regolamento il valore di porto sicuro** ("safe harbour").

Sul piano penale, la fattispecie di cui all'art. 437-bis c.p. àncora la responsabilità all'adozione di "misure tecniche idonee", nozione priva di parametri predefiniti in assenza di standard armonizzati. Sul piano civile, l'art. 19 stabilisce espressamente che neppure la piena conformità all'AI Act, ancorché certificata, esclude la responsabilità. In entrambi i casi, l'impresa che abbia integralmente attuato i requisiti della norma di riferimento potrebbe nondimeno risultare esposta a responsabilità.

A fronte di un'esposizione penale non prevedibile ex ante e non neutralizzabile attraverso la conformità al regolamento, **è concreta la possibilità che gli operatori decidano di non rendere disponibili le proprie soluzioni basate sull'intelligenza artificiale**, rilasciandole sul mercato italiano in ritardo o in versioni depotenziate. L'effetto sarebbe una perdita di competitività dell'intero sistema Paese, che si troverebbe ad accedere alle tecnologie di IA a condizioni deteriori rispetto agli altri Stati membri. **Un'ulteriore conseguenza sarà quella di scoraggiare l'adozione, da parte di imprese e pubbliche amministrazioni, di strumenti di IA nei propri sistemi e servizi.** Per fare un esempio, si pensi all'adozione di algoritmi di IA per il riconoscimento di patologie da parte del Servizio Sanitario Nazionale, che potrebbe divenire fonte di responsabilità penale in caso di eventuali diagnosi errate.

1.2.2. Sovrapposizione con normativa europea in materia di responsabilità civile

Un secondo profilo trasversale attiene al rapporto tra disposizioni in materia già approvate o proposte dalla Commissione. Lo schema tende, in più punti, ad aggiungere un ulteriore livello di responsabilità laddove una disciplina è già prevista.

Sul piano penale, l'AI Act ha costruito il proprio impianto sanzionatorio su sanzioni amministrative pecuniarie e su misure di vigilanza (art. 99), coerentemente con la natura tecnica e in evoluzione della materia. L'introduzione di un autonomo regime

penale imperniato su omissioni tecniche solleva profili di tensione con il principio del *ne bis in idem,* perché lo stesso comportamento sarebbe sottoposto a più sanzioni.

Sul piano civile, gli articoli 17 e 18 riproducono nella sostanza i meccanismi contenuti nella proposta di direttiva sulla responsabilità civile da intelligenza artificiale (AI Liability Directive – AILD). La proposta è stata formalmente ritirata dalla Commissione europea, in ragione di preoccupazioni relative alla frammentazione del mercato interno. Il ritiro era volto inoltre a evitare la stratificazione di norme sul settore dell'intelligenza artificiale, uno dei principali motori di crescita e produttività per l'economia europea. **Replicare lo stesso strumento in Italia rischia di ostacolare la competitività delle imprese**.

A ciò si aggiunge che la direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi (di seguito, "PLD") include già espressamente il software e i sistemi di intelligenza artificiale nella nozione di "prodotto". Con specifico riguardo allo scenario del consumatore danneggiato da un prodotto basato sull'intelligenza artificiale, **una tutela equivalente è dunque già assicurata da uno strumento del diritto dell'Unione che l'Italia dovrà comunque recepire**.

1.2.3. Sovrapposizione con l'AI Act

Il terzo profilo di criticità riguarda l'incidenza dello schema sul riparto di competenze in materia di sicurezza dell'intelligenza artificiale. L'effetto combinato delle disposizioni in esame rischia di **rimettere all'autorità giudiziaria la determinazione, caso per caso e a posteriori, di ciò che debba intendersi per "sicurezza" dell'intelligenza artificiale in Italia**.

La valutazione della conformità ai requisiti dell'AI Act è affidata dal regolamento a un sistema compiuto e armonizzato, imperniato sugli standard elaborati dagli organismi europei di normazione (CEN-CENELEC), sulle procedure di valutazione della conformità, sugli organismi notificati e sulle autorità nazionali di vigilanza (AgID e ACN). Si arriverebbe dunque a **duplicare l'accertamento di conformità, sottrarlo alle autorità competenti e ottenere una nozione giudiziale di "sicurezza dell'IA" concorrente rispetto a quella europea**, in diretta tensione con la finalità di armonizzazione perseguita dal regolamento.

Un simile assetto rischia di sovrapporsi alla norma europea di riferimento introducendo obblighi e conseguenze ulteriori rispetto a quelli da essa previsti, e ciò proprio nel segmento che il regolamento ha inteso disciplinare in modo armonizzato a livello di Unione. Il profilo si riverbera sull'intero Titolo II, poiché è la medesima nozione indeterminata di adeguatezza tecnica a fondare, sul versante penale, il giudizio di responsabilità e, sul versante civile, la valutazione della condotta del convenuto.

Infine, **l'AI Act distingue con cura gli obblighi dei fornitori (Art. 16), dei deployer (Art. 26), degli importatori (Art. 23), dei distributori (Art. 24), calibrando le responsabilità in base al ruolo e all'influenza**. Applicare un unico standard penale indifferenziato a tutti gli attori, creando un disallineamento con il quadro europeo ed esponendo attori con un controllo limitato a una responsabilità sproporzionata.

2. ANALISI PER ARTICOLO

2.1. Profili penali — art. 12 (nuovo art. 437-bis c.p.)

- **Determinatezza:** La nozione di "misure tecniche idonee a prevenire malfunzionamenti" è priva di parametri oggettivi e, in assenza di standard armonizzati, rischia di essere definita solo a posteriori in sede giudiziale. Si suggerisce pertanto di ancorare la responsabilità penale alla violazione di obblighi normativi o di conformità chiaramente individuabili — in primo luogo quelli discendenti dall'AI Act e dagli standard armonizzati — anziché a una clausola aperta di adeguatezza tecnica. Diversamente, la definizione sostanziale degli standard di sicurezza dell'intelligenza artificiale finirebbe per essere rimessa all'interprete, in contrasto con l'impianto del regolamento, che affida tale compito agli organismi tecnici competenti.
- **Proporzionalità***:* Le pene giungono a 2-8 anni (omissione) e 3-10 anni (alterazione) sul solo pericolo concreto, in assenza di danno e anche a titolo di colpa grave: un livello pari o superiore a quello dei reati IA dolosi introdotti dalla stessa legge n. 132/2025 (artt. 612-quater c.p., 294 c.p., 2637 c.c., 185 TUF) e più severo dell'art. 437 c.p., che prevede i 3-10 anni solo per dolo e in presenza di un disastro o infortunio effettivo.
- **Catena del valore***:* La fattispecie raggiunge l'intera filiera, inclusi i fornitori di modelli per finalità generali e i rilasci open source, privi di controllo effettivo sull'impiego a valle che qualifica il sistema come ad alto rischio. L'AI Act calibra gli obblighi in base al ruolo di ciascun attore, mentre l'Art. 437-bis impone la stessa responsabilità penale a tutti indistintamente - disallineandosi dal quadro UE e penalizzando eccessivamente chi ha minor controllo sul sistema IA.
- **Strutture societarie complesse**: Il criterio del "livello effettivo di controllo dell'agente" assume rilievo dirimente nei gruppi societari, nei quali modelli e strumenti di IA — in particolare i modelli per finalità generali — sono sviluppati e gestiti a livello centrale. Gli obblighi, e con essi la responsabilità penale, non possono essere imputati automaticamente alle entità locali che non esercitano alcun controllo effettivo sulla progettazione, sull'addestramento o sulle decisioni di rilascio del sistema. Si suggerisce di

rendere esplicita l'esclusione della responsabilità penale in assenza di controllo effettivo sull'uso del sistema o del modello.

- **Coerenza con la delega***:* Alcuni profili meritano verifica di stretta aderenza all'art. 24, comma 5, della legge n. 132/2025: l'estensione alle fasi di "progettazione" e "addestramento" non elencate; la natura commissiva del reato di alterazione, estranea al criterio incentrato sull'omissione; il criterio del "livello effettivo di controllo dell'agente", da rendere esplicito.
- **Ne bis in idem***:* La medesima condotta può cumulare la sanzione amministrativa dell'art. 99 e la sanzione a carico dell'ente.
- **Assenza di un meccanismo premiale per le misure correttive**: La fattispecie non attribuisce alcun rilievo alla condotta dell'operatore successiva alla scoperta della non conformità o del malfunzionamento. Ne deriva un incentivo perverso: l'operatore che individua autonomamente una criticità nel proprio sistema, la segnala e vi pone rimedio si espone alle medesime conseguenze penali di chi resti inerte, e anzi contribuisce a documentare la propria stessa responsabilità. Tale impostazione è disallineata dalla logica che il diritto dell'Unione ha adottato per la gestione dei rischi tecnologici in evoluzione: il regolamento (UE) 2024/2847 (Cyber Resilience Act) e la direttiva (UE) 2022/2555 (NIS2) costruiscono l'intero impianto della risposta alle vulnerabilità di sicurezza informatica su obblighi di segnalazione tempestiva e di adozione di misure correttive; nella medesima direzione muovono gli artt. 20 e 73 dell'AI Act, che impongono al fornitore di adottare senza indugio le azioni correttive necessarie e di notificare gli incidenti gravi.

  Si suggerisce pertanto di introdurre una causa di esclusione della responsabilità penale in favore dell'operatore che, venuto a conoscenza di una non conformità, di un malfunzionamento o di un rischio derivante dal sistema di IA, adotti spontaneamente e senza ritardo ingiustificato le misure correttive necessarie a ripristinare la conformità e a neutralizzare il rischio, dandone comunicazione all'autorità competente. L'operatività della causa di esclusione potrebbe essere subordinata alla ricorrenza di tre condizioni: (i) la tempestività dell'intervento; (ii) l'assenza di un danno concreto ai diritti fondamentali, alla salute o alla sicurezza delle persone; (iii) l'assenza di dolo o colpa grave nella genesi della non conformità.

2.2. Strumenti processuali civili — artt. 15-20

Il regime civile tende a duplicare la Product Liability Directive dove vi si sovrappone e a eccederla dove va oltre il suo perimetro (utilizzatore professionale, ambito contrattuale, voci di danno non contemplate). In particolare:

- **Art. 15 (responsabilità dell'ente).** Sanzione pecuniaria dell'ordine di 155.000-1.550.000 euro e sanzioni interdittive, tra cui il divieto di contrattare con la pubblica amministrazione e di pubblicizzare i propri servizi, sono estremamente gravose per un fornitore ICT.
- **Art. 17 (accesso alle prove).** Lo strumento dell'ordine di esibizione presenta, nella formulazione attuale, tre profili di criticità.
    - *(i) Ambito di applicazione.* Il meccanismo si applica a **qualsiasi sistema di intelligenza artificiale**, in termini più ampi persino della proposta di direttiva sulla responsabilità da IA poi ritirata dalla Commissione. Ne consegue che anche comuni prodotti di consumo dotati di funzionalità di IA risulterebbero esposti a ordini di esibizione di documentazione tecnica e informazioni riservate. Si propone di circoscrivere l'accesso alle prove ai sistemi ad alto rischio o, quantomeno, alle azioni fondate su violazioni del regolamento.
    - *(ii) Soglia di ammissibilità.* La soglia richiesta per la concessione dell'ordine è particolarmente bassa e rischia di favorire richieste di carattere meramente esplorativo. Si propone di innalzarla, subordinando l'ordine alla previa allegazione di elementi di fatto e di prova sufficienti a sostenere la plausibilità della domanda risarcitoria, secondo il modello della PLD.
    - *(iii) Segreti commerciali e sicurezza.* Gli obblighi di *disclosure* non dovrebbero comportare la divulgazione di informazioni proprietarie, architetture dei modelli, parametri, dati di addestramento o misure di sicurezza, la cui diffusione comprometterebbe la sicurezza del sistema o la proprietà intellettuale dell'operatore, salvo i casi strettamente necessari e proporzionati e con adozione di misure di protezione effettive (art. 78 dell'AI Act).
    - *(iv) Conseguenze dell'inottemperanza.* La regola per cui l'inottemperanza documentale comporta di ritenere ammessi i fatti allegati rischia di incidere sulla parità delle parti e dovrebbe essere calibrata in termini di proporzionalità e di effettiva disponibilità della prova: l'automatismo non dovrebbe operare quando la documentazione tecnica, i log o i materiali di modello non siano concretamente nella disponibilità dell'operatore chiamato a produrli.
- **Art. 18 (presunzione di causalità).** Opera in modo pressoché automatico da qualsiasi violazione, in termini più ampi e di natura diversa rispetto alla presunzione condizionata prevista dalla PLD, che lega la presunzione a una non conformità qualificata e pertinente al rischio verificatosi. Non tutte le violazioni dell'AI Act presentano la medesima rilevanza rispetto al verificarsi del danno: alcune hanno natura prevalentemente amministrativa o documentale (registrazione, tenuta della documentazione tecnica,

adempimenti informativi). Si suggerisce pertanto di sostituire la presunzione automatica con una previsione secondo cui **la violazione degli obblighi dell'AI Act costituisce un elemento rilevante che il giudice può considerare nella valutazione del nesso causale**, unitamente alle ulteriori circostanze del caso concreto.

- **Art. 19 (rilevanza della conformità). La previsione per cui la conformità, anche certificata, non esclude la responsabilità è il profilo di maggiore criticità**: rimuove ogni certezza per l'operatore conforme e muove in senso opposto anche alla logica della normativa europea sui prodotti, che alla conformità riconosce rilievo a favore del convenuto. La formulazione attuale rischia di disincentivare l'adozione di rigorosi modelli di governance fondati sull'AI Act. Pare opportuno, pertanto, ai fini di spingere le imprese a adottare i modelli di governance promossi dalla normativa, di riconoscere alla conformità il valore di porto sicuro.
- **Art. 20 (copertura assicurativa).** La disposizione prevede che, a fronte di una richiesta del danneggiato, il soggetto ritenuto responsabile comunichi l'esistenza e gli estremi di un'eventuale polizza di responsabilità civile, ricollegando alla omessa o incompleta comunicazione la possibilità per il giudice di desumere argomenti di prova ai sensi dell'articolo 116 del codice di procedura civile. Pur non introducendo formalmente un obbligo assicurativo, tale meccanismo rischia di **esercitare una pressione indiretta verso la stipula di una copertura, poiché associa una conseguenza processuale sfavorevole alla posizione dell'operatore non assicurato**. Il mercato assicurativo per il rischio da intelligenza artificiale è ancora in fase di sviluppo, con offerta limitata e criteri di sottoscrizione non consolidati: ne risulterebbero penalizzate tanto le imprese che legittimamente scelgano di non assicurarsi, quanto quelle che non riescano a reperire sul mercato una copertura adeguata. Si osserva pertanto che **l'assenza di una copertura assicurativa non dovrebbe, di per sé, essere valutata a sfavore dell'operatore.**

CONCLUSIONE

L'Italia può affermarsi quale riferimento europeo nella governance responsabile dell'intelligenza artificiale, a condizione di un quadro fondato su regole chiare e prevedibili, capaci di offrire certezza giuridica alle imprese che operano sul territorio nazionale. Anitec-Assinform rinnova la propria disponibilità a fornire ogni utile contributo tecnico nel prosieguo dell'iter.