

«La sorveglianza di massa è vietata e pericolosa»

— Alice Oliverio, 31 luglio 2026

Rieducational channel L'avvocato Blengino: «Al di là delle correzioni, sull'Ai il governo va in rotta con la Ue»

Carlo Blengino, avvocato specializzato nel diritto penale legato alle nuove tecnologie e all'utilizzo dei dati personali. La maggioranza adesso frena, ma sin qui quali sono le principali differenze tra il regolamento europeo sull'intelligenza artificiale e il modo con cui l'Italia lo sta recependo?

L'Ai Act mira ad armonizzare il mercato unico europeo in relazione alla commercializzazione e all'uso di sistemi di intelligenza artificiale. Solo per alcuni specifici settori, dove un sistema tratta dati particolari come quelli biometrici in ambiti sensibili come il law enforcement, l'Ai Act mira anche a tutelare direttamente il diritto alla protezione dei dati personali. Dico questo perché le evidenti criticità del decreto legislativo predisposto dal governo non sono tanto i contrasti, presenti ma emendabili, con l'Ai Act, quanto un'impostazione complessivamente incompatibile direttamente con i principi della Carta dei diritti fondamentali Ue e in violazione della direttiva 680/2016 che regola il trattamento dei dati nel settore della prevenzione e repressione dei reati. Si tratta di un contrasto che potremmo definire ontologico perché pone diverse previsioni del decreto, in particolare gli articoli 8, 10 e 13, fuori dalla cornice normativa dell'Europa. Il diritto alla protezione dei dati personali è presente ormai in quasi tutti i paesi del mondo, ma è stato consacrato a diritto fondamentale e incluso nella Carta dei diritti fondamentali solo in Europa perché l'Europa aveva vissuto sulla sua pelle la sorveglianza di massa attuata dai regimi totalitari del '900, soprattutto dalla Stasi. Questo diritto fondamentale dovrebbe difenderci non tanto o non solo dall'invasività delle cosiddette big tech quanto proprio dallo Stato e dalla bulimica fame di dati e informazioni che hanno tutti i governi, anche i più democratici. L'utilizzo di sistemi di Ai, in un mondo datificato e costantemente mediato dal digitale, nel settore della prevenzione e repressione dei reati o dell'ordine pubblico o della abusata "pubblica sicurezza" (per non parlare della sicurezza nazionale) è uno dei rischi più concreti e attuali di quella tecnologia. Il decreto legislativo di fatto estende e mira a fornire un'apparente base giuridica a pratiche di sorveglianza di massa vietate e pericolose, inaccettabili al di là dell'Ai Act.

Le schedature biometriche effettuate "in diretta" o addirittura "a posteriori" non violano la normativa sulla privacy?

Da un punto di vista tecnico, il trattamento dei dati biometrici è comunque assai complesso e dipende dalle modalità di acquisizione e di elaborazione del dato: un'impronta digitale o una menomazione fisica hanno una valenza diversa da un riconoscimento facciale o comportamentale. Un sistema di identificazione biometrica remota è diverso da una verifica biometrica

e da un riconoscimento facciale. L’Ai Act pone i sistemi di identificazione biometrica remota (cioè senza partecipazione del soggetto interessato) tra i sistemi vietati o ad alto rischio proprio perché estremamente invasivi non solo per la privacy o la riservatezza, ma per l’esercizio di tutti i diritti fondamentali. Il Garante ha indicato alcune criticità tecniche allo schema di decreto del governo, ma c’è da dire che l’attuale collegio dell’autorità di garanzia italiana non sembra interpretare al meglio il ruolo assegnatogli di guardiano terzo ed indipendente.

Da un punto di vista giudiziario questi riconoscimenti sarebbero materiale probatorio valido?

A decreto in vigore, sì, salvo sollevare appunto complesse questioni di costituzionalità o pregiudiziali alla Corte di giustizia europea. Però il problema vero della sorveglianza di massa non è in tribunale, nelle aule di giustizia, e non riguarda il delinquente: riguarda il cittadino estraneo a qualsivoglia illegalità che passava per la stazione monitorata o nel corteo sbagliato, i cui dati sono comunque a sua insaputa trattati, archiviati e usati per finalità non necessariamente di giustizia. Riguarda le fasce marginalizzate e deboli, la cui vita dipende da un permesso o da un daspo frutto di chissà quale algoritmo.

Questo decreto legislativo cade in un contesto di continua introduzione di nuovi reati da parte del governo in nome della sicurezza, da avvocato penalista considera efficace l’azione del governo?

Sono 20 anni che inseguiamo un soluzionismo tecnologico con la stessa cecità con cui questo governo utilizza il diritto penale. Non essendo in grado di affrontare i problemi, si sceglie la soluzione più facile e a buon mercato. C’è un quartiere ad alta devianza? Non si analizzano le cause, la mancanza di spazi di aggregazione, la povertà economica e culturale e così via. Si piazzano le telecamere, magari con riconoscimento facciale, e si adotta un daspo urbano per chi disturba o spaccia, spostando il problema e aggravandolo, generando “scarti” e “carichi residuali”. Allo stesso modo, ma con finalità ancora più meschine, a ogni fatto di cronaca si adotta un nuovo reato e si aumentano le pene. È gratis e consente efficaci post sui social. Inoltre, aumentare le pene è utile per aumentare la capacità intrusiva dello Stato: più la pena è alta, più elevata sarà la percezione di gravità e più sarà consentito allo stato violare riservatezza, privacy e dati degli indagati. In trent’anni di professione forense non ho mai visto un delinquente che valutasse la gravità della pena prima di commettere il reato.