

«Lo Stato deve dotarsi di tecnologie. Non ci si può affidare solo al mercato»

intervista a Giovanni De Gregorio, di Bruno Ruffilli

TORINO – «L'AI Act europeo, pensato inizialmente come una regolazione del rischio di prodotti e servizi, è diventato una normativa che mira allo stesso tempo alla tutela dei diritti, e il decreto del Governo è perfettamente allineato con il Considerando 1 dell'AI Act, che indica come obiettivo dell'Ue la promozione di un'intelligenza artificiale antropocentrica», osserva Giovanni De Gregorio, docente di Law and Technology alla Católica Global School of Law di Lisbona e scientific advisor per Pollicino AI Advisory.

Per il riconoscimento biometrico in tempo reale c'è un limite di 15 giorni e la richiesta di un'autorizzazione giudiziaria. Bastano davvero a escludere il rischio di una sorveglianza di massa?

«Nell'articolo 5 dell'AI Act il riconoscimento biometrico in tempo reale e in spazi pubblici fa parte degli usi proibiti ed è consentito alle autorità di polizia solo sulla base di regole e condizioni stringenti. Alcune sono definite direttamente dall'AI Act, come la necessità dell'autorizzazione dell'autorità giudiziaria, altre sono lasciate alla normativa degli Stati membri, e l'Italia riempie lo spazio che le viene lasciato. Parliamo di un riconoscimento per fini molto restrittivi, casi di urgenza, in luoghi pubblici e in tempo reale. Quindi direi che viene limitato il rischio di sorveglianza di massa».

C'è un altro tema controverso: la possibilità che i sistemi di Ai siano forniti da aziende private.

«Il problema vero è la capability, vista l'evoluzione di strumenti sempre più articolati spesso derivanti da soggetti privati. La grande questione, che non investe solo la biometria ma anche il welfare più in generale, riguarda la capacità dell'attore pubblico di comprendere quali tecnologie dovranno essere proprietarie, interne, e quali dovranno essere ricercate tra quelle disponibili sul mercato».

Come si fa a impedire che l' algoritmo prenda decisioni al posto di un essere umano?

«Il rischio è comunque presente. Il decreto ha dei passaggi decisivi che riguardano il training, la necessità di dotare l'individuo (ad esempio un magistrato) delle capacità critiche per comprendere come l'utilizzo di strumenti di Ai debba essere considerato un supporto. Non è facile, non c'è una regola che risolve la questione, ed è ovvio che l'esposizione ad un output di un sistema di Ai tende già a influenzare il modo in cui decidiamo. L'attività di training serve proprio a garantire che l'attività umana abbia una rilevanza, e non sia solo un presidio formale. È un tema che ritorna nel campo del lavoro, dove si prevede che assunzioni, licenziamenti e sanzioni disciplinari non possano basarsi solo su trattamenti automatizzati. La società in cui viviamo sta dando priorità al fatto che la decisione umana abbia un valore, anche per una questione di responsabilizzazione dei soggetti che sviluppano e utilizzano sistemi di Ai. Non possiamo immaginare di governare l'intelligenza artificiale mancando

quelle competenze che dovrebbero essere alla base di un uso consapevole di tali sistemi. La formazione quindi risulta centrale».

Agid, ACN, Garante della privacy, Banca d'Italia, Consob, IVASS: questa molteplicità di enti con ruoli diversi rafforza i controlli o rischia di creare frammentazione?

«È un tema problematico; non dico che la soluzione sia la centralizzazione, nazionale o sovranazionale, però attribuire un ruolo a più autorità in questo ambito richiede un grande coordinamento istituzionale, specie quando si considera che il tema non riguarda solo l'Italia, ma anche gli Stati membri e le istituzioni europee».