La tutela da e per l'I.A.: prime riflessioni sulla governance dell'A.I. Act e sulla (nuova?) autorità di vigilanza

di Gianluigi Delle Cave - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 24 aprile 2024

Les jeux sont faits. Rien ne va plus. C'è un testo finale per l'A.I. Act e, sì, non dovrebbe cambiare in modo sostanziale. Il dibattito è acceso e le prime considerazioni in merito – costruttive e critiche – già alluvionali. Dall'approccio basato sul rischio all'obbligo di formazione, passando per la governance, sono diversi e rilevanti gli aspetti trattati dal regolamento UE in questione. Il presente post vuole soffermarsi, in particolare, sulla governance e sulla tutela dei cittadini dai sistemi di I.A.; tutela che, per quanto ritenuta da alcuni commentatori poco "ambiziosa", viene affidata alle cure di un (nuovo?) soggetto istituzionale pronto a battagliare per la difesa dei diritti: un'autorità nazionale di vigilanza del mercato dell'intelligenza artificiale.

Il dibattito sul nuovo Artificial Intelligence Act dell'Unione europea (si vedano anche i post dell'OSD qui, qui, qui e qui) – approvato il 13 marzo 2024 – è più che mai vivo e frizzante. Diversi studiosi lo hanno già "consacrato" quale eccellenza normativa eurounitaria. Altri, de contrario, ne hanno, da subito, evidenziato importanti criticità sia con riferimento al perimetro di applicazione (es. il livello dell'A.I. "ad alto rischio"), sia sotto il profilo delle plurime interconnessioni (aspetti non compiutamente disciplinati da un punto di vista di regolazione) che intercorrono tra l'intelligenza artificiale con altri istituti ad essa direttamente o indirettamente connessi (es. la proprietà intellettuale).

Con particolare riferimento alla governance (oggetto della presente, sintetica, disamina) dell'I.A. nel Regolamento di cui trattasi, un recente articolo dell'associazione Access Now (consultabile qui) ne ha censurato plurimi profili, tutti apparentemente accomunati dalla "cultura dell'impunità" in capo alle autorità deputate alla sicurezza pubblica, soprattutto avuto riguardo al dispiegamento di sistemi di intelligenza artificiale contro le comunità più marginalizzate. In particolare, il regolamento UE, a detta dell'articolo in questione, risulterebbe: (i) inidoneo quanto alla regolazione specifica degli usi più discussi dell'I.A., tra cui i sistemi di riconoscimento biometrico; (ii) poco incisivo con riferimento all'utilizzo dei sistemi "ad alto rischio" qualora utilizzati per esigenze di sicurezza nazionale; (iii) non "ambizioso" guardando alla protezione dei soggetti in flussi migratori, meno tutelati rispetto ai cittadini dell'Unione.

Ma allora quid iuris in punto di tutela dai sistemi di I.A.? La critica in questione offre, adunque, un prezioso assist per soffermarsi proprio su questo rilevantissimo aspetto, ossia quello dell'"autorità" preposta non solo al controllo ma anche all'uniformità di applicazione dei sistemi in questione pure in punto di tutela dei diritti fondamentali della persona (al di là, quindi, del mero, checché considerevole, dato tecnico).

La riflessione non può che prendere le mosse dal dato normativo. Anzitutto, il considerando 153 del regolamento UE (cfr. art. 70) bene illustra la sentita necessità di un ente "ad hoc" in tale settore: si prevede, infatti, che ciascuno Stato membro designi una autorità di vigilanza del mercato come autorità nazionale competente al fine di controllare l'applicazione e l'attuazione del regolamento medesimo. A tal proposito, si prevede che gli Stati membri possono decidere

di nominare qualsiasi tipo di entità pubblica per svolgere i compiti delle autorità nazionali competenti per l'I.A. (conformemente alle loro specifiche caratteristiche

ed esigenze organizzative nazionali), purché i rispettivi poteri siano esercitati in modo "indipendente, imparziale e senza pregiudizi", in modo da salvaguardare i principi di obiettività delle attività e dei loro compiti (considerando 154). Il considerando 156, poi, rappresenta, a parere di chi scrive, un passaggio fondamentale: l'autorità di vigilanza sull'I.A. non solo dovrebbe disporre di tutti i poteri di esecuzione previsti nell'A.I. Act (con precipuo riferimento, quindi, ai sistemi "ad alto rischio", per i quali si prevedono densi obblighi di progettazione, collaudo, monitoraggio, nonché responsabilità aggiuntive, qui non elencati per dovere di sinteticità), ma pure quello di adottare misure di regolazione "aggiuntiva" con riferimento a quei sistemi di I.A. non soggetti agli obblighi e ai requisiti specifici del regolamento eurounitario (purché, ovviamente, presentino profili di rischio tale da giustificarne l'intervento di dettaglio). Quindi se è vero che l'A.I. Act è stato pensato, de facto, prevedendo impatti normativi diversi a seconda della rischiosità dei sistemi è altresì vero che nulla vieta all'autorità di vigilanza preposta alla tutela da – e per – l'I.A. di prevedere meccanismi di tutela ulteriori "ad espansione" pure con riferimento a quei sistemi che "ad alto rischio" non sono o non sembrerebbero, prima facie, esserlo. Per fare ciò, l'art. 70, comma 3, del regolamento si premura di specificare che gli Stati membri "garantiscono" che le loro autorità nazionali competenti dispongano di risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti.

L'estrema rilevanza di siffatta autorità, in punto di tutela, viene poi ulteriormente rimarcata dal considerando 159, ove si sottolinea – proprio con riferimento al delicato settore della biometria e in aderenza all'art. 16, paragrafo 2, del T.F.U.E. – che non possono prescindersi poteri di indagine e correttivi efficaci nell'ipotesi in cui l'I.A. venga utilizzata ai fini di contrasto, migrazione, asilo e gestione del controllo delle frontiere, o per l'amministrazione della giustizia e dei processi democratici (impregiudicati i poteri conferiti dalla direttiva UE 2016/680 in materia di trattamento dei dati per prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali). Sul punto paiono convincenti, a tutta prima, le attività autorizzatorie e di verifica cristallizzate all'art. 26 in capo all'autorità de qua, anche in punto di protezione dei dati operativi "sensibili" relativi alle attività di contrasto.

Alle funzioni di controllo, indagine e monitoraggio, si accompagnano, poi, attività di consulenza e orientamento sull'attuazione dell'A.I. Act (si potrebbe qui consolidare, adunque, una potestà di tipo regolamentare) nonché, a chiusura del sistema, i poteri sanzionatori (sanzioni, specifica l'art. 99 del regolamento, "effettive, proporzionate e dissuasive"), questi ultimi soggetti a garanzie procedurali adeguate in conformità del diritto dell'Unione e nazionale, inclusi il ricorso giurisdizionale e il giusto processo. Qui un ulteriore passaggio fondamentale. Lo sforzo del regolamento di assicurare l'istituzione di una nuova autorità di vigilanza "a portata" di tutti (non solo dei cittadini UE) viene in risalto muovendo alla lettura dell'art. 85. Qui si prevede che, fatti salvi altri ricorsi amministrativi o giurisdizionali, "qualsiasi persona fisica o giuridica" che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del regolamento può presentare un reclamo motivato all'autorità di che trattasi. In conformità al regolamento (UE) 2019/1020, si precisa che tali reclami sono presi in considerazione ai fini dello svolgimento delle attività di vigilanza del mercato e sono trattati in linea con le procedure specifiche stabilite a tal fine dalle autorità supra.

Pare chiaro, quindi, che la governance regolamentare dell'I.A. preveda, in verità, l'istituzione di un'autorità di peso e carattere (di cui si aspettano i primi passi), volta proprio alla tutela dei

diritti di tutti quei soggetti che possono, in qualche modo, essere violati – lì dove la protezione ordinamentale è massima – dall'intelligenza artificiale (su tale profilo, in chiave comparatistica, si veda anche l'executive order USA del 30.10.2023 del Presidente Biden, qui, ove, con riferimento alla tutela, diverse sono le similitudini con l'A.I. Act, quantomeno con riferimento all'approccio basato sul rischio e agli obblighi in capo agli sviluppatori di I.A.; le competenze in materia di controllo, invece, risulterebbero spalmate su più dipartimenti a livello federale, es. quello del Commercio, della Giustizia e della Sanità, oltre che sul Consiglio di sicurezza nazionale).

Così brevemente introdotta la natura e le funzioni di detta autorità di vigilanza, siano però consentite alcune riflessioni immediatamente conseguenti. In particolare, di quale autorità si parla e quale in Italia?

Il regolamento UE non sembra, invero, fornire indizi preferenziali sul punto (eccezion fatta per l'individuazione diretta del Garante europeo dei dati personali-GEPD quale autorità competente per le istituzioni, gli organi e gli organismi dell'Unione che rientrano nella sfera di applicazione del regolamento stesso).

Diversamente, si rinviene una sorta di "rivendicazione" della competenza in materia di I.A., da ultimo nella segnalazione presentata dal Garante Privacy al Parlamento, il 25 marzo scorso, con cui il Garante ha richiesto di essere individuato quale autorità competente, rimarcando la stretta correlazione tra i sistemi di I.A. e i dati personali (cfr. sul punto anche il parere congiunto n. 5/2021 del EDPB e del GEDP). Alla luce di tale considerazione, si evidenzia che le autorità per la protezione dei dati dispongono già, in una certa misura, di conoscenze in materia di tecnologie basate sull'I.A., di dati e di sistemi di elaborazione degli stessi nonché di diritti fondamentali, disponendo altresì di competenze nella valutazione dei rischi che le nuove tecnologie comportano per tali diritti fondamentali.

Sul punto, si consideri che la designazione delle autorità per la protezione dei dati come autorità nazionali di controllo sull'I.A. assicurerebbe certamente un approccio normativo più armonizzato, contribuendo all'adozione di un'interpretazione coerente delle disposizioni in materia di trattamento dei dati nonché a evitare contraddizioni nella loro applicazione; ciò oltre al fatto che tutte le parti interessate della catena di valore dell'IA trarrebbero beneficio dall'esistenza di un punto di contatto unico per tutte le operazioni di trattamento dei dati personali che rientrano pure nell'ambito di applicazione dell'A.I. Act, oltre che dalla limitazione delle interazioni tra due differenti organismi di regolamentazione (quello sull'I.A. e quello sul GDPR).

Il trattamento dei dati personali, tuttavia, è solo un aspetto, una parte, dell'interazione dei diritti (fondamentali) con l'I.A. Se si guarda, infatti, agli obiettivi generali del regolamento UE in esame – ossia migliorare il funzionamento del mercato interno e promuovere la diffusione di un'I.A. antropocentrica e affidabile, garantendo nel contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, promuovendo l'innovazione – il Garante rischia di essere "troppo" o "troppo poco" con riferimento ad un settore così ampio e trasversale.

Ed è in tale incertezza di fondo che sembra farsi avanti – quale autorità sull'I.A. – l'Agenzia per l'Italia Digitale (AGID) insieme all'Agenzia Nazionale per la Cybersicurezza (ACN); candidatura apparentemente confermata nel recente documento "Strategia Italiana per

l'Intelligenza Artificiale 2024-2026", redatto proprio dall'AGID (documento che, nei suoi plurimi obiettivi e strategie, sembrerebbe costituire un vero e proprio programma di azione da neonata autorità; cfr. qui) così come nella bozza del disegno di legge italiano sull'I.A., recentemente resa pubblica (ove, per l'appunto, vengono indicate AGID e ACN quali soggetti deputati al ruolo di che trattasi; scelta, peraltro, verosimilmente "fondata" con riferimento a carenze in organico dell'autorità privacy tali da non consentire, in apparenza, il giusto focus sulle delicate tematiche in oggetto).

Nulla osterebbe, del resto, all'individuazione dell'Agenzia de qua quale "autorità" di vigilanza sull'I.A., pure in considerazione del fatto che l'A.I. Act non pregiudica comunque le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione della normativa dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati (considerando 157). Si porrebbe, al più, una riserva sulla scelta, non di poco momento, di un'agenzia di nomina governativa (l'AGID) quale autorità di vigilanza dell'I.A. rispetto ad una vera e propria autorità indipendente (come il Garante privacy), quest'ultima – si ritiene – più in linea rispetto alle caratteristiche prescritte dal regolamento UE. Sembra quindi ad oggi

esclusa una "terza via", ossia l'istituzione di una autorità ad hoc per l'I.A. (come nel caso spagnolo, ossia l'Agencia Española de Supervisión de Inteligencia Artificial di cui al Real Decreto n. 729/2023; cfr. qui).

A temporaneo dispetto, quindi, delle critiche all'A.I. Act sul piano della tutela dei diritti, sembrerebbe invece qui delinearsi addirittura un duplice ordine di tutela: (i) da un lato, infatti, potrà contestarsi la non conformità tecnica tout court del sistema di I.A. con il regolamento UE – o anche il suo utilizzo "non conforme" – avanti l'autorità di vigilanza del mercato; (ii) dall'altro e in parallelo, potrà comunque rilevarsi qualsiasi trattamento di dati personali non conforme alla normativa di settore avanti il Garante Privacy o l'autorità giudiziaria.

Al momento, dunque, peraltro in mancanza degli interventi di dettaglio da parte delle autorità di vigilanza nazionali, ritenere il regolamento UE poco "incisivo" o poco "ambizioso" rispetto alla tutela dei diritti fondamentali, costituisce conclusione certamente affrettata e, da diversi angoli visuali, pure inconsistente nello stesso modo in cui è tale pretendere di giocare a scacchi muovendo ortogonalmente l'alfiere: non si tratta di violare le regole del gioco ma è eo ipso giocare ad altro.