Il nuovo regolamento europeo sull'uso dell'intelligenza artificiale tra limiti e deroghe

Problemi di profilazione e sistemi di identificazione biometrica: alcune considerazioni

di Marco Biagiotti [*]

Il 12 luglio scorso è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il "Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)"[1]. Così, a meno di quattro mesi di distanza dall'approvazione del Parlamento UE e a meno di due mesi dall'approvazione del Consiglio UE, entra in vigore il c.d. AI Act, cioè il complesso di regole e disposizioni – parte integrante dell'agenda digitale europea - relative all'utilizzo dell'intelligenza artificiale in Europa.

Sebbene già durante il lungo iter di gestazione e approvazione la pubblicistica corrente e quella di settore abbiano dedicato a questo provvedimento legislativo un'ampia messe di studi, analisi e approfondimenti, forse si avverte ancora la mancanza di uno sguardo di più ampio respiro che riesca a dare conto simultaneamente di tutta la massa di innovazioni che esso introduce, a livello globale, in materia di sviluppo, immissione sul mercato e utilizzo dei sistemi di Intelligenza Artificiale, sia da parte di soggetti pubblici che privati. D'altronde, come spesso avviene per i documenti di fonte comunitaria, si tratta di un testo complesso e di non facile lettura con i suoi 180 "considerando", 113 articoli e 13 allegati. Peraltro, le nuove norme si applicheranno in tutti gli aspetti solo 24 mesi dopo la loro entrata in vigore, cioè ad agosto 2026, anche se per alcune specifiche parti (pratiche proibite, codici di condotta, norme di governance) sono previste scadenze più ravvicinate, mentre per altre (sistemi ad alto rischio) l'applicazione è posticipata di ulteriori 12 mesi[2]. Non è ovviamente questa la sede per addentrarsi in una disamina particolareggiata di tutte le disposizioni contenute nel Regolamento; ci si limiterà quindi a tentare di metterne in luce alcuni caratteri salienti che possano favorire una migliore comprensione dello spirito che lo sottende, con particolare riferimento al tentativo di regolamentare taluni aspetti dell'impiego dell'intelligenza artificiale concernenti i sistemi di profilazione e di identificazione (i quali, non incidentalmente, implicano ricadute importanti anche in materia di controllo e sorveglianza negli ambiti lavorativi), corredati da qualche riflessione sulle criticità che la loro attuazione inevitabilmente comporta.

Sin dalle considerazioni preliminari il Regolamento definisce un quadro abbastanza preciso di cosa si deve intendere per intelligenza artificiale nell'ottica regolatoria europea. Essa consiste in una *"famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali."* L'uso dell'IA può quindi *"fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi"*[3]. Il conseguimento di tali vantaggi, tuttavia, è possibile solo adottando consapevolmente l'IA secondo un principio di tecnologia antropocentrica che funga da "strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani"[4]. Il legislatore europeo sembra comunque avere ben presente che si tratta di una materia estremamente fluida ed in continua evoluzione, stante la velocità degli sviluppi tecnologici in atto e la pervasività della loro diffusione nei settori più disparati dell'economia e della società. La preoccupazione, in questa fase, appare soprattutto quella di fissare una serie di punti di riferimento comuni a tutti gli Stati dell'Unione per guidare in maniera coerente ed omogenea la circolazione dell'IA secondo criteri di affidabilità, sicurezza e rispetto di taluni diritti fondamentali. In tale chiave, ap-

pare altresì trasparente l'intento di agevolare lo sviluppo e la diffusione dei sistemi di IA in tutto lo spazio comunitario proprio grazie all'adozione di regole comuni capaci di scongiurare il rischio di frammentazioni normative e regolamentari derivanti dall'iniziativa dei singoli Stati[5]. Peraltro, la logica che ispira questo Regolamento comunitario non sembra tanto quella di produrre una lista di regole coercitive e limitanti, ma, al contrario, di fluidificare la crescita e la diffusione dell'IA predisponendo – se è consentita la metafora – corridoi ad alta velocità attraverso i quali un processo di trasformazione tecnologica chiaramente percepito come incombente e del tutto irreversibile potrà innervare in modo efficace il tessuto profondo del sistema economico e produttivo europeo.

Con riferimento all'ambito di applicazione, l'art. 2 definisce una lunga lista di soggetti pubblici e privati tenuti a rispettare i nuovi parametri di utilizzo dell'IA, il cui scopo (definito nell'art. 1) è quello di *"migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione."* Tuttavia, sempre nell'articolo 2, paragrafi 3 e seguenti, è elencata anche una serie di altri soggetti pubblici e privati che ne sono esentati e sui quali vale forse la pena di soffermarsi. Preliminarmente, corre l'obbligo di sottolineare che il Regolamento non ha valore giuridico al di fuori dell'ambito di applicazione del diritto dell'Unione, il che induce a riflettere sulla pur ovvia considerazione che in qualunque contesto non coperto dalla disciplina comunitaria lo sviluppo e l'utilizzo dei sistemi di IA, per quanto in contrasto con i principi definiti nel Regolamento stesso, continueranno a schivarne gli effetti regolatori.

Ma diverse eccezioni importanti all'applicazione della nuova disciplina si riferiscono allo stesso ambito UE, a cominciare dai sistemi di IA *"se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività."* Inoltre, il passaggio successivo del medesimo paragrafo 3 chiarisce che il nuovo Regolamento non si applica ai sistemi di IA che, pur non essendo "immessi sul mercato o messi in servizio nell'Unione", generino tuttavia "output" utilizzati nell'Unione *"esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività"*. Non rileva qui allargare la discussione abbozzando un censimento delle varie "entità" che utilizzano sistemi di IA nel territorio dell'Unione per finalità militari, di difesa o di sicurezza nazionale. Quello che interessa evidenziare è l'ampiezza del campo di non-applicazione del Regolamento, i cui fondamenti etico-giuridici disvelano la loro reale forza solo all'esito di una netta selezione delle condizioni generative dei diversi sistemi di IA utilizzati nell'ambito comunitario. In tale ottica va inquadrata, riteniamo, anche l'ulteriore eccezione di applicabilità individuata dal comma 4 dell'art. 2, concernente le "autorità pubbliche di un paese terzo" e le "organizzazioni internazionali" che utilizzano sistemi di IA nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie, *"a condizione che tale paese terzo o organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone"*.

Di più, la non applicazione del Regolamento riguarda anche i *"sistemi di IA o modelli di IA […] specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici"*, con il che si adombra un territorio dai contorni alquanto sfumati e all'interno del quale risulta teoricamente collocabile una gamma vastissima di attività pubbliche e private. Seguendo la

stessa falsariga, il nuovo Regolamento non si applica inoltre *"alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio"*, non si applica agli *"obblighi dei deployer*[6] *che sono persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale"*. Anche in questo caso ci troviamo di fronte a una definizione dai confini piuttosto incerti, la cui potenziale vastità sembra collocare al di fuori dell'ambito di applicazione del Regolamento una platea di distributori e/o di utilizzatori invero difficile da circoscrivere con precisione anche in chiave di gestione di possibili contenziosi interpretativi.

In ogni caso, pur al netto delle condizioni di non-applicabilità di cui sopra, i limiti imposti alla produzione, alla commercializzazione e all'utilizzo dell'intelligenza artificiale coprono un arco di situazioni di non trascurabile ampiezza, come si può evincere dalla lettura dell'intero articolo 5. È vietata, ad esempio, l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che utilizzino *"tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo";* oppure di sistemi che sfruttino *"le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo";* o, ancora, di sistemi *"per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste"*.

Inevitabilmente, la mente corre agli svariati esempi di sistemi di IA già da tempo in uso nella nostra società e che, sebbene in grado di esercitare una certa forma di condizionamento dei comportamenti individuali e sociali delle persone, fanno ormai parte della nostra vita di tutti i giorni, ma di cui è ormai difficile riconoscere gli effetti in termini di influenza subliminale sulla capacità di assumere 'decisioni informate' nei riguardi di se stessi e/o di tutti coloro che ne condividono il contesto di riferimento[7]. Allo stesso modo, non si può fare a meno di pensare alla pervasività con cui molte applicazioni di intelligenza artificiale possono stressare le attitudini cognitive delle coorti più giovani e più vulnerabili della popolazione, influenzandone le scale valoriali e, in certi casi, condizionandone gli orientamenti culturali proprio nella fase più complessa e delicata del processo di formazione psico-sociale degli individui. Senza la pretesa di volersi addentrare in un'analisi semantica del testo della norma comunitaria, mette conto segnalare come essa contenga – seppure, a nostro avviso, non intenzionalmente – una via di fuga giuridica in favore degli agenti più spregiudicati di sistemi di IA manipolativa, stante che le eventuali distorsioni comportamentali da esse derivanti sembrerebbero doversi riconoscere come tali solo laddove sussista un scopo dichiarato in tal senso, oppure l'effetto distorsivo sia manifestamente riconoscibile.

Con riguardo specifico al (lodevolissimo) tentativo di porre un freno al rischio di implementare e diffondere sistemi di IA finalizzati a modulare il grado di autonomia delle persone in base all'attribuzione di determinati punteggi sociali sulla base dei comportamenti individuali, la lettera c) del comma 1 dell'art. 5 chiarisce che il divieto scatta nel caso in cui il *"punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:*

i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità".

Qui, forse, il limite del divieto – si perdoni il barocchismo – consiste nel fatto che il presupposto da cui esso discende (ossia: mancato collegamento tra contesto di applicazione e contesto di rilevazione; effetto limitante dell'autonomia personale ingiustificato o sproporzionato rispetto alla gravità del comportamento) appaiono soggetti ad un ampio grado di discrezionalità applicativa nel quadro delle diverse legislazioni nazionali, a fronte del fatto che il processo di valutazione e classificazione di persone o gruppi di persone in base alla congruità dei loro

comportamenti sociali per finalità di pubblico interesse e/o sicurezza non può che essere appannaggio di una pubblica autorità.

Anche il divieto di immettere sul mercato e di impiegare sistemi di IA in grado di *"effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità"* appare attenuato dalla successiva precisazione che esso non si applica ai sistemi di IA utilizzati *"a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa":* circostanza, quest'ultima, potenzialmente estendibile a tutti i sistemi di profilazione algoritmica finalizzati a prevenire il rischio di commissione di reati, stante che le attività valutative personali effettuate dai sistemi di IA si basano comunque (e non potrebbe essere diversamente) sull'immissione e sull'elaborazione di informazioni relative a "fatti oggettivi e verificabili", associabili ad attività criminose che implementano il processo di addestramento dell'algoritmo.

Un'altra eccezione che merita un sia pur breve cenno di riflessione è quella riguardante il divieto di impiegare sistemi di IA in grado di *"inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione",* la cui apprezzabile tensione etica appare altresì smorzata dalla possibile apertura all'uso di tali tipologie di sistemi in ambito lavorativo laddove entrino in gioco "motivi medici o di sicurezza" che, di fatto, potrebbero configurare l'estensione a una gamma pressoché infinita di contesti e di situazioni organizzative nei luoghi di lavoro. Ci troviamo qui in presenza di un campo i cui confini potranno/dovranno certamente formare oggetto di definizione nell'ambito del sistema delle relazioni industriali, sia di livello nazionale che aziendale, il che potrà tuttavia avvenire solo nelle realtà produttive in cui le rappresentanze sindacali siano non solo presenti, ma anche sufficientemente solide, competenti e strutturate.

Il nuovo Regolamento affronta anche il delicato e controverso tema dell'identificazione biometrica delle persone fisiche e delle "deduzioni" che gli algoritmi, opportunamente addestrati, sono in grado di ricavare dalle caratteristiche biometriche degli individui in merito a *"razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale".* Tale tipologia di sistemi di IA viene genericamente vietata (art. 5, comma 1, lettera g), ma con la precisazione che il divieto non riguarda "l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente", ad esempio le immagini, e la loro relativa "categorizzazione" finalizzata ad "attività di contrasto". Analogamente, l'uso di "sistemi di identificazione biometrica remota «in tempo reale» risulta vietato in spazi accessibili al pubblico, *"a meno che, e nella misura in cui, tale uso sia strettamente necessario"* per le seguenti finalità: ricerca mirata di vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, ricerca di persone scomparse, "prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche", prevenzione di una "minaccia reale e attuale o reale e prevedibile di un attacco terroristico", localizzazione o identificazione di una persona "sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale" per reati punibili nello Stato membro interessato con una misura di privazione della libertà della durata di almeno quattro anni.

A parte l'ampiezza della casistica richiamata e, conseguentemente, la vastità della platea di persone fisiche potenzialmente assoggettabili ad identificazione in tempo reale e in spazi pubblici per ragioni ascrivibili alla sicurezza e al rispetto della legalità, ci sembra rilevante sottolineare anche la genericità del passaggio che, per "finalità di contrasto", rende possibile

l'uso di sistemi IA in grado di classificare individualmente le persone fisiche "sulla base dei loro dati biometrici" al fine di trarre "deduzioni o inferenze" in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale. Va peraltro evidenziato come il legislatore europeo qui appaia ben consapevole della necessità di stabilire dei paletti in grado di non trasformare le deroghe al divieto di identificazione biometrica nei luoghi pubblici in una sorta di liberatoria generale a discapito della riservatezza dei dati personali di immense platee di persone del tutto estranee agli scopi identificativi della "ricerca". Al riguardo, il comma 2 dell'art. 5 precisa: *"L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h) è applicato (…) solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti:*

a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema;

b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze".

E subito dopo aggiunge: *"L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), del presente articolo rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali."*

Ed infine: *"L'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico è autorizzato solo se l'autorità di contrasto ha completato una valutazione d'impatto sui diritti fondamentali come previsto all'articolo 27 e ha registrato il sistema nella banca dati UE conformemente all'articolo 49".* Qui, peraltro, il nuovo Regolamento avverte la necessità di fare salve le "situazioni di urgenza debitamente giustificate".

Il successivo comma 3, a sua volta, precisa che *"ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso (…)"*[8].

In conclusione, da una prima analisi degli aspetti sopra evidenziati ci sembra che emerga come il cosiddetto IA Act rappresenti il tentativo da parte del legislatore europeo di superare le difficoltà rappresentate dall'esigenza di contemperare i diritti di tutela della libertà di movimento e della riservatezza dei dati soggettivi delle persone con le possibili molteplici situazioni in cui i sistemi di intelligenza artificiale si trovano ad essere programmati, commercializzati e utilizzati per finalità di pubblico interesse e che, proprio per tali motivi, richiedono uno screening accurato di determinate caratteristiche personali degli individui, peraltro non sempre univocamente oggettivabili. Come accennato in esordio, la Direttiva, entrata in vigore il 2 agosto scorso, dispiegherà completamente i suoi effetti applicativi a partire dal 2 agosto 2026, sebbene per alcuni aspetti siano previste scadenze differenti. In questo intervallo occorrerà comprendere se la ponderosa mole della nuova disciplina comunitaria, qui peraltro analizzata solo in minima parte, sia in grado di conservare il suo valore regolatorio nel tempo a valle del processo di progressiva adozione di tutte le sue parti, stante la rapida evoluzione delle tecnologie che la Direttiva stessa intende normare. Si tratta, in ogni caso, di un primo indispensabile passo (che, è bene sottolinearlo, rappresenta sin qui un inedito assoluto a livello mondiale) per cercare di definire un quadro di regole entro le quali lo sviluppo di sistemi di IA sempre più sofisticati e pervasivi può essere ricondotto, onde evitare che gli "effetti nocivi" del progresso tecnologico possano mettere a repentaglio valori quali democrazia, stato di diritto, protezione delle libertà individuali e, con essi, tutti i principi essenziali posti a fondamento dell'Unione europea. ■

Note

[1] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689

[2] Così l'art. 113 ("Entrata in vigore e applicazione"): *"Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Si applica a decorrere dal 2 agosto 2026. Tuttavia: a) I capi I e II si applicano a decorrere dal 2 febbraio 2025; b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere*

dal 2 agosto 2025, ad eccezione dell'articolo 101; c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027".

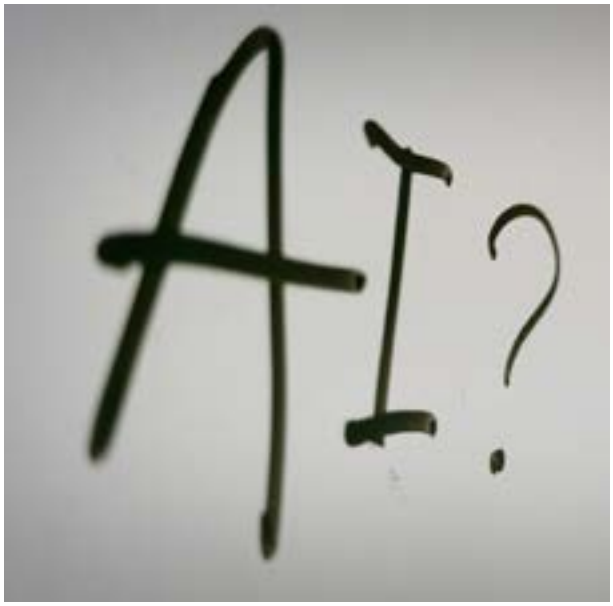
[3] Vedi "Considerando" n. (4).

[4] Vedi "Considerando" n. (6).

[5] Così, al riguardo, il "Considerando" n. (3): *"È pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione al fine di conseguire un'IA affidabile, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione, l'innovazione, la diffusione e l'adozione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno, stabilendo obblighi uniformi per gli operatori e garantendo la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno". E poco oltre, il successivo "Considerando" n. (8) sottolinea: "Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, come riconosciuti e tutelati dal diritto dell'Unione".*

[6] In base al "Considerando" n. (13): *"La nozione di «deployer» di cui al presente regolamento dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal deployer." La definizione viene peraltro ribadita anche al punto 4) dell'art. 3.*

[7] Una vasta letteratura internazionale è fiorita negli ultimi anni (talvolta non senza una certa inclinazione allarmista di matrice commerciale) per indagare gli effetti condizionanti che i sistemi di intelligenza artificiale, opportunamente programmati a tale scopo, riescono ad esercitare attraverso internet e i dispositivi mobili sui gusti individuali delle persone e sui comportamenti sociali, sino ad influenzare le idee politiche e a rimodellare i principi etici e i valori di riferimento di comunità composte da milioni e milioni di individui. Al riguardo, ci permettiamo qui di suggerire a chiunque gradisse avviare un approfondimento su un tema così complesso la lettura del volume di Alex Pentland: Fisica sociale. *Come si propagano le buone idee*, Milano,



Università Bocconi Editore, 2015.

[8] Anche qui, però, si ammette la possibilità che *"in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati".*

In ogni caso, *"L'autorità giudiziaria competente o un'autorità amministrativa indipendente la cui decisione è vincolante rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota «in tempo reale» in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, primo comma, lettera h), (…) e in particolare, rimane limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale (…). Nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota «in tempo reale»."*

---

[*] Dipendente del Ministero del Lavoro dal 1984 al 2009 e, dal 2009 ad oggi, del Consiglio Nazionale dell'Economia e del Lavoro. Ha collaborato alla realizzazione della collana di volumi "Lavoro e contratti nel pubblico impiego" per la UIL Pubblica Amministrazione. Dal 1996 al 2009 è stato responsabile del periodico di informazione e cultura sindacale "Il Corriere del Lavoro". Dal 2011 al 2023 ha collaborato alla redazione del notiziario "Mercato del lavoro e Archivio nazionale dei contratti collettivi" del CNEL.