Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

La proposta di Regolamento UE sull'Intelligenza Artificiale: i profili operativi del nuovo quadro normativo europeo – Parte Prima

Prof. Avv. Alessandro del Ninno
Studio Legale Tonucci & Partners

§ 1. Introduzione: un quadro di insieme della proposta europea di l'Artificial Intelligence Act

Il presente contributo rappresenta il primo di quattro articoli di commento che saranno pubblicati con cadenza settimanale, con l'obiettivo di analizzare in una prospettiva operativa struttura e contenuti della proposta di *Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale (l'Artificial Intelligence Act) e che modifica talune norme legislative dell'Unione* (di seguito, per brevità, il "*Regolamento IA*"). L'importante iniziativa legislativa – uno dei pilastri di quello che la Commissione UE ha definito *Decennio Digitale* nell'Agenda Digitale 2030 - presentata lo scorso 21 Aprile 2021, è il primo atto normativo al mondo che si propone di regolamentare in modo generale e organico questa tecnologia emergente, e chissà se – come già successo con il Regolamento Generale UE sulla protezione dei dati personali 679/2016 – anche questo (futuro) Regolamento assumerà una sorta di valore "paradigmatico", ponendosi come modello legislativo anche per analoghe iniziative di regolamentazione che saranno assunte a livello nazionale e internazionale.

In questo primo articolo di commento, saranno affrontati: i profili generali del Regolamento IA, l'oggetto e le finalità delle nuove regole, l'ambito di applicazione, le principali definizioni giuridiche dei concetti per poi approfondire le scelte legislative circa i divieti importi a particolari "*pratiche di intelligenza artificiale*".

La proposta di Regolamento IA fa seguito a recenti e importanti iniziative della UE (particolarmente attivo è stato in questi mesi il Parlamento europeo, con il suo c.d. "*October 2020 Framework on AI*") che in un certo senso hanno preparato il terreno politico e legislativo della proposta presentata il 21 aprile. Ci si riferisce soprattutto al *Libro Bianco sull'Intelligenza Artificiale* presentato dalla Commissione UE il 19 Febbraio 2020. In quell'importante e assai interessante (per i profili pratici) documento, la Commissione fissava – tra gli altri – anche i presupposti dei futuri interventi regolatori delle tecnologie emergenti e della stessa IA, chiarendo che la via maestra da seguire è caratterizzata da due fondamentali direttrici: (a) valutare l'efficacia applicativa all'IA di normative già vigenti, senz'altro utili per regolamentare anche taluni profili innovativi e criticità dell'IA (es: dal Regolamento Generale sulla protezione dei dati personali alla direttiva sulla sicurezza generale dei prodotti; dalla direttiva sulla responsabilità del produttore alle norme UE a tutela dei diritti e delle libertà fondamentali); (b) procedere ad interventi normativi specifici e *ad hoc* (il c.d. "*ecosistema legislativo per una IA affidabile*") solo in caso di un approccio *risk based* basato su due criteri specifici la cui presenza deve essere contestuale

per giustificare un intervento normativo specifico sull'IA in base ad un *rischio significativo* correlato all'IA:

- il primo criterio è l'impiego ed utilizzo di sistemi di IA in un settore in cui, date le caratteristiche delle attività abitualmente svolte, si possono prevedere rischi significativi. Questo primo criterio garantisce che l'intervento normativo sia mirato ai settori in cui i rischi sono generalmente ritenuti più probabili. I settori interessati – chiarisce la Commissione UE nel Libro Bianco - dovrebbero essere elencati (e rivisti periodicamente) in maniera specifica ed esaustiva nel nuovo quadro normativo (es: settori dell'assistenza sanitaria, dei trasporti; dell'energia, sicurezza pubblica);
- il secondo criterio è quello della applicazione dell'IA nel settore in questione che deve essere però impiegata in modo tale da poter generare rischi significativi. Questo secondo criterio riconosce il fatto che non tutti gli usi dell'IA nei settori selezionati comportano necessariamente rischi significativi. Ad esempio, per quanto l'assistenza sanitaria in genere possa essere certamente un settore ad alto rischio ove impiegare sistemi di IA, un eventuale difetto del sistema di prenotazione degli appuntamenti in un ospedale non presenta, in linea di massima, rischi tali da giustificare un intervento legislativo.

Dunque, è in questa prospettiva di "*ecosistema legislativo*" specifico che va letto il nuovo Regolamento IA, di cui uno degli obiettivi rilevanti (fin dal titolo) è quello di dettare "*norme armonizzate*" e di coordinare le nuove regole *ad hoc* sull'IA con le altre norme già vigenti nell'ordinamento UE, pure applicabili all'Intelligenza Artificiale (in particolare, 19 tra Regolamenti e Direttive settoriali di cui all'Allegato II della proposta di Regolamento IA). Ovviamente, questa iniziativa legislativa si coordina anche con altre strategie UE in corso, come la *Strategia europea sui dati* (cfr. Comunicazione della Commissione UE 2020/66), la proposta di Regolamento UE sulla c.d. *Data Governance* o la c.d. *Direttiva Open Data* 2019/1024 sul riuso delle informazioni nel settore pubblico.

Un Regolamento, quello in esame, che conferma inoltre - oltre all'approccio *risk based* quale asse portante dell'intero assetto regolatorio – anche la cosiddetta "filosofia" dell'Intelligenza Artificiale *antropocentrica*, con l'essere umano al centro (si veda l'articolo 14 del regolamento IA rubricato "*Sorveglianza umana*", tra gli altri) che riveste diversi ruoli: (a) utilizzatore e terminale ultimo dei benefici di questa nuova tecnologia; (b) destinatario delle tutele normative a protezione dei diritti e delle libertà fondamentali, potenzialmente a rischio rispetto a determinati impieghi dell'IA che potrebbero determinare effetti distorsivi e discriminatori; (c) presidio di controllo, onde garantire che non si verifichino scenari (comuni alla trama di molte produzioni cinematografiche) in cui i sistemi di Intelligenza Artificiale raggiungono un tale livello di autonomia e auto-consapevolezza (c.d. "*singolarità*") da sottrarsi al controllo umano.

Ovviamente, l'altra finalità è quella di garantire il buon funzionamento a livello UE del mercato dei beni, servizi e soluzioni di Intelligenza Artificiale, in un quadro regolatorio armonizzato che garantisca una Intelligenza Artificiale *sicura, etica ed affidabile.*

* * * * * *

Sono sostanzialmente quattro i principali obiettivi perseguiti dalla proposta di Regolamento IA:

- garantire che i sistemi di IA immessi sul mercato dell'Unione e poi utilizzati siano sicuri e rispettosi delle norme esistenti a tutela dei diritti fondamentali e dei valori dell'Unione;
- garantire la certezza del diritto per facilitare gli investimenti e l'innovazione nell'IA;
- migliorare la *governance* e l'effettiva applicazione delle norme sui diritti fondamentali e potenziare i requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico, prevendendo frammentazioni, per applicazioni di Intelligenza Artificiale che siano legali, sicure ed affidabili.

Per raggiungere tali obiettivi, leggiamo nella relazione di accompagnamento alla proposta di Regolamento IA che:

"*la presente proposta presenta un approccio regolatorio all'IA orizzontale, equilibrato e proporzionato, onde limitare al minimo necessario i requisiti per affrontare i rischi e le problematiche legate all'IA, senza vincolare od ostacolare indebitamente gli sviluppi tecnologici o in altro modo aumentando in modo sproporzionato il costo di immissione sui mercati di soluzioni di IA. La proposta stabilisce un quadro giuridico solido e flessibile. Da un lato, tale quadro normativo è completo e a prova di futuro nelle sue scelte normative fondamentali, inclusi i principi fondamentali di base sui quali deve fondarsi ogni sistema di IA. Dall'altro, mette in atto un sistema normativo proporzionato centrato su una regolamentazione ben definita basata sull'approccio risk based che non crea inutili restrizioni al commercio, per cui l'intervento legale è su misura per quelle situazioni concrete in cui vi è un motivo di preoccupazione giustificato o dove tale preoccupazione può essere ragionevolmente prevista nel prossimo futuro. Allo stesso tempo, il quadro legale include meccanismi flessibili che gli consentono di essere adattato dinamicamente agli sviluppi della tecnologia ed ai nuovi scenari*".

Le norme proposte saranno applicate tramite un sistema di *governance* a livello di Stati membri, con la previsione della istituzione di Autorità nazionali di vigilanza sull'IA che si riuniranno nel Comitato europeo per l'intelligenza artificiale, replicando il medesimo meccanismo già operativo da anni nel settore della data protection (autorità *data protection* nazionali Comitato Europeo per la protezione dei dati personali).

La proposta di Regolamento IA è composta da 13 Titoli e 85 articoli che dettano una disciplina organica e complessiva su:

- finalità, ambito di applicazione e definizioni;
- pratiche di Intelligenza Artificiale vietate;
- classificazione e regole sui sistemi di Intelligenza Artificiale "*ad alto rischio*"
- obblighi di trasparenza per alcuni sistemi di Intelligenza Artificiale;

- misure di supporto all'innovazione;
- attuazione del Regolamento mediante istituzione di un sistema di governance
- previsione di codici di condotta
- sistema sanzionatorio e disposizioni finali

§ 2. Regolamento IA: l'oggetto e le diversificate finalità del nuovo quadro normativo sui sistemi di Intelligenza Artificiale.

Il Legislatore europeo fissa all'articolo 1 le finalità e l'oggetto del nuovo quadro normativo, avendo come riferimento una triplice prospettiva, che difatti poi è richiamata sempre nell'articolato come una serie di attività-presupposto a cui sono ricollegate regole e responsabilità dei vari soggetti:

1. la prospettiva della *immissione sul mercato* di sistemi di Intelligenza Artificiale;
2. la prospettiva della *messa in servizio* di sistemi di Intelligenza Artificiale;
3. l'*utilizzo* di sistemi di Intelligenza Artificiale.

Il Regolamento mira difatti a introdurre norme armonizzate che disciplinino uniformemente e in maniera organica nell'Unione tutte queste fasi (le prime due delle quali oggetto anche di specifiche definizioni giuridiche all'articolo 3. nn. 9, 10 e 11).

Altro scopo del Regolamento è quello di vietare – come spiegheremo – determinate "*pratiche di intelligenza artificiale*": fin dai primi articoli, il Legislatore è pienamente consapevole che tra gli obiettivi generali del suo intervento (rigoroso, tanto da introdurre un divieto) vi è anche quello di evitare criticità e rischi connessi a sistemi già ampiamente disponibili e dalla tecnologia sofisticata, il cui impiego può rappresentare una minaccia ai diritti e alle libertà fondamentali (e anche democratiche) su cui si fonda l'Unione (si pensi ai sistemi di riconoscimento biometrico e ai tentativi passati della UE di introdurre una moratoria quinquennale sui sistemi di *face recognition*).

L'obiettivo centrale è poi quello di regolamentare i requisiti specifici per sistemi di IA definiti "*ad alto rischio*" e gli obblighi per gli operatori (diversificati per tipo di attività svolta, come si vedrà nell'analisi delle definizioni) di tali sistemi.

Molto importante e degna di interesse è l'ulteriore finalità di introdurre regole armonizzate che introducono rigorose prescrizioni di trasparenza (si vedano ad esempio gli artt. 52 e ss. della proposta di regolamento IA) per i sistemi di IA destinati a interagire con le persone fisiche - ivi inclusi i sistemi per il riconoscimento delle emozioni basato sul trattamento dei dati biometrici e i sistemi di classificazione biometrica (es: per età, sesso, etc) – e per quelli utilizzati per generare o manipolare contenuti di immagini, audio o video (una prima disciplina normativa sui cc.dd *deepfake*).

Conclude la nostra rassegna delle finalità, l'introduzione di norme in materia di monitoraggio e sorveglianza del mercato, che rappresentano (insieme alle norme di tutela e si supporto alla innovazione) la parte di attenzione "commerciale" ai sistemi di Intelligenza Artificiale.

§ 3. Regolamento IA: l'ambito di applicazione soggettiva e l'efficacia potenzialmente su scala globale delle nuove regole.

L'articolo 2 è di assai interessante lettura, per una serie di spunti che confermano la convinzione di chi scrive di come la tecnologia abbia cambiato in questi ultimi anni il paradigma applicativo delle norme, prima legate al territorio ed ora del tutto e chiaramente svincolate da confini di Stati ed organizzazioni sovranazionali per divenire – ricorrendo determinati presupposti – applicabili sostanzialmente su scala globale, come si cercherà di spiegare poco oltre.

Intanto: il Regolamento IA si applica ai soli sistemi IA ad uso civile, essendo esclusi dall'ambito di applicazione i sistemi IA sviluppati o utilizzati esclusivamente per scopi militari (che pure pongono urgenti criticità di ordine politico, legislativo ed etico). Viene in mente la lettera aperta all'ONU con la quale nel 2017 114 esperti di intelligenza artificiale e robotica (tra cui gli amministratori delegati di TESLA, Google, etc) chiesero ai governi mondiali la messa al bando di sistemi militari letali autonomi, i robot killer (più di recente può farsi riferimento anche alla *Risoluzione del Parlamento europeo del 12 settembre 2018 sui sistemi d'arma autonomi*).

Il Regolamento troverà applicazione:

a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che tali fornitori siano stabiliti all'interno dell'Unione o in un paese terzo;
b) utenti di sistemi di IA situati all'interno dell'Unione;
c) fornitori e utenti di sistemi di IA che si trovano in un paese terzo, laddove l'output prodotto come risultato dalla operatività del sistema di IA venga utilizzato all'interno dell'Unione.

L'ambito di applicazione soggettiva rivela al tempo stesso quanto più sopra si diceva circa il mutato paradigma applicativo di norme che disciplinano tecnologie che per loro natura dispiegano i loro effetti al di là e indipendentemente da confini territoriali o politici. Difatti: il fornitore che immette un sistema IA nell'Unione da un Paese extra UE e senza aver alcuna sede o stabilimento nella UE sarà soggetto alle (integrali) norme del Regolamento, ovunque si trovi. Se tale presupposto si inquadra ordinariamente in una ovvia logica commerciale (si pensi ai distributori o esportatori extra UE di sistemi IA), peculiare è l'ulteriore presupposto di applicabilità: indipendentemente da attività commerciali di immissione sul mercato di sistemi IA, basterà che un sistema IA utilizzato

e/o ubicato in un qualsiasi Paese terzo produca un risultato (*output*) che venga però utilizzato all'interno della UE per rendere applicabile il Regolamento IA tanto al fornitore extra UE di quel sistema quanto agli utenti nel paese terzo.

Come si vede, si replica un meccanismo di potenziale applicabilità di norme europee a soggetti appartenenti ad ordinamenti (e Paesi) extra UE che già abbiamo imparato a conoscere nel Regolamento Generale UE sulla protezione dei dati personali 679/2016 [si legga l'art. 3.2 del GDPR, che rende potenzialmente applicabili le regole sul trattamento dei dati personali a titolari del trattamento ovunque stabiliti nel mondo e privi di sede o stabilimento nella UE al ricorrere dei presupposti specificati alle lettere 3.2(a) e 3.2(b)].

Dal punto di vista soggettivo, si noterà inoltre che quando il Legislatore europeo specifica che il Regolamento IA si applica agli "utenti" persone fisiche, questi sono individuati senza alcun riferimento a formali requisiti di cittadinanza o nazionalità europee o alla residenza o domicilio nella UE, ma semplicemente in base alla verifica oggettiva: (a) della loro presenza di fatto (non giuridica) nella UE; (b) della mera circostanza dell'utilizzo di un sistema di IA. Anche in tale prospettiva si replica una scelta (che rafforza la protezione "etica" delle persone fisiche ovunque stabilite) che già il Legislatore del GDPR aveva effettuato, prevedendo in quel caso l'applicazione del Regolamento "*indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*" (cfr. art. 3.1 GDPR) e con riferimento a "*interessati che si trovano nell'Unione*" (cfr. art. 3.2 GDPR).

Per i sistemi di IA ad alto rischio che siano componenti di sicurezza di prodotti o sistemi, o che siano essi stessi prodotti o sistemi, rientranti nell'ambito di applicazione di specifici atti normativi dell'Unione (es: il Reg. 300/2008 sulla sicurezza dell'aviazione civile; i regolamenti sui veicoli a motore, etc), il Regolamento IA trova applicazione solo con riferimento a quanto prevede l'articolo 84 (revisione ogni tre anni dell'Allegato III al Regolamento sulla classificazione dei sistemi ad alto rischio).

Il Regolamento, infine, non si applica:

a) alle autorità pubbliche di un paese terzo o ad organizzazioni internazionali, se tali autorità o organizzazioni utilizzano sistemi di IA nel quadro di accordi internazionali per l'applicazione della legge e la cooperazione giudiziaria;
b) alla responsabilità di prestatori intermediari di servizi della società dell'informazione. Esaminando tale ipotesi di esclusione viene in considerazione la Direttiva 2000/31 sui servizi della società dell'informazione – che sarà presto sostituita dal *Digital Services Act* presentato dalla commissione nel 2020 – e che in un certo evidenzia un conflitto – sul punto della *liability* (sia pure chiarita nella sua portata applicativa da non poche sentenza della Corte di Giustizia UE) - con il Regolamento IA, se solo si pensa alle prerogative degli intermediari in merito alla responsabilità per la fornitura dei servizi della società dell'informazione e al principio dell'assenza dell'obbligo generale di sorveglianza.

§ 4. Regolamento IA: le principali definizioni giuridiche, tecnologiche, commerciali (ed etiche)

L'analisi delle ben 44 definizioni introdotte dall'articolo 3 del Regolamento IA può essere effettuata raggruppandole per categorie:

1. le definizioni relative alla tecnologia IA, alla sua progettazione, utilizzo ed operatività;
2. le definizioni dei soggetti a vario titolo implicati dalla operatività dei sistemi IA;
3. le definizioni di attività commerciali aventi ad oggetto i sistemi IA;
4. le definizioni specifiche su particolari sistemi di IA che utilizzano la biometria; e infine,
5. le definizioni inerenti alle *autorità pubbliche* che vengono in considerazione o perché utilizzano i sistemi (es: forze di polizia, autorità amministrative, autorità giudiziarie, autorità di *law enforcement* in generale) o perché incaricate nell'ambito della *governance* generale di sorvegliare i sistemi IA.

§ Segue 4.1: le definizioni relative alla tecnologia IA, alla sua progettazione, utilizzo ed operatività.

Cominciando la disamina pratica delle *definizioni relative alla tecnologia IA, alla sua progettazione, utilizzo ed operatività*, non si può non partire dalla definizione di "*Sistema di intelligenza artificiale*" *(sistema AI):* "qualsiasi software sviluppato con una o più delle tecniche e approcci elencati nell'Allegato I al Regolamento che può, per un dato insieme di obiettivi definiti dall'uomo, generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono".

La Commissione UE ritiene tale definizione "*a prova di futuro*" e cioè sufficientemente neutra e generale da includere anche futuri sviluppi tecnologici senza subire una sorta di "obsolescenza definitoria" a seguito dei notoriamente rapidissimi sviluppi che caratterizzano queste tecnologie.

Sorge più di qualche dubbio circa la effettiva capacità di una tale definizione - limitata alla concezione dell'IA come mero software - di ricomprendere davvero qualsiasi "sistema IA", per esempio se compariamo tale definizione con altre che pure si ritrovano nei numerosi documenti e testi sull'Intelligenza Artificiale resi disponibili in questi anni dalle istituzioni europee: si pensi ad esempio alla definizione contenuta nella *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - L'intelligenza artificiale per l'Europa, Bruxelles* del 25.4.2018:

"'Intelligenza artificiale' (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)".

La definizione di *sistema di Intelligenza Artificiale* è integrata da uno specifico Allegato I (che la Commissione UE potrà ai sensi dell'art. 4 della bozza rivedere e aggiornare periodicamente in linea con gli sviluppi tecnologici) che fa in realtà riferimento sostanzialmente alle metodologie di apprendimento dell'IA, elencando le diverse modalità operative che seguono:

a) l'apprendimento automatico (detto *machine learning*), inclusi il *supervised learning*, *l'unsupervised learning* e il *reinforcement learning* che impiegano svariati metodi e tecniche di apprendimento, incluso il *deep learning*;
b) la logica e la acquisizione di una *knowledge base*, inclusa la rappresentazione della conoscenza, la programmazione (logica) induttiva, le *knowledge bases*; i motori di ricerca basati su tecniche e logiche di inferenza e/o deduttive; il ragionamento (simbolico) e i sistemi esperti;
c) l'operatività basata sulla statistica; i metodi di ricerca e ottimizzazione e le previsioni cc.dd. *bayesiane* (nella *Teoria della Stima*, le regole bayesiane sono quelle azioni o regole di decisione che minimizzano il valore atteso della probabilità a posteriori o di una funzione di perdita, cioè la perdita attesa a posteriori).

Meglio sarebbe probabilmente stato fornire una definizione più "inclusiva" dei sistemi IA, come ad esempio quella che segue: sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti.

Prima di procedere con l'analisi pratica delle definizioni, appare opportuno offrire al lettore una sintetica illustrazione dei principali metodi di apprendimento impiegati dai sistemi di IA come elencati nell'Allegato I della proposta di Regolamento IA.

Nell'apprendimento automatico sorvegliato (*supervised learning*), invece di impartire regole di comportamento al sistema, vengono forniti esempi di comportamento di input-output nella speranza che esso riesca a generalizzare a partire da tali esempi (che tipicamente descrivono il passato) e a comportarsi correttamente in situazioni non

illustrate negli esempi (che potrebbero essere incontrate in futuro). Nell'apprendimento sorvegliato un essere umano ha il compito di istruire il sistema e di dare un riscontro alle decisioni che il sistema IA poi prende in autonomia. Un esempio noto di apprendimento sorvegliato sono i filtri antispam: sulla base di determinate caratteristiche il sistema decide se l'e-mail debba finire nella casella di posta in entrata oppure se in quella dello spam. Se il sistema dovesse fare un errore, in seguito è possibile impostare di nuovo manualmente i parametri a cui il filtro dovrà fare riferimento in futuro.

Nel settore della prevenzione delle frodi finanziarie (come la clonazione della carta di credito o i furti di dati e identità) abbiamo altri esempi di *supervised learning:* gli algoritmi imparano ad agire mettendo in correlazione eventi, abitudini degli utenti, preferenze di spesa, ecc.; informazioni attraverso le quali riescono poi a identificare eventuali comportamenti anomali che potrebbero appunto implicare un furto o una frode.

Interessanti esempi di *supervised learning* arrivano poi dal settore della ricerca scientifica in campo medico dove gli algoritmi imparano a fare previsioni sempre più accurate per prevenire lo scatenarsi di epidemie oppure per effettuare diagnosi di tumori o malattie rare in modo accurato e tempestivo. E infine, sempre nell'ambito dell'apprendimento sorvegliato, ci sono interessanti applicazioni di *machine learning* a livello di riconoscimento vocale, traduzione automatica delle lingue o identificazione della scrittura manuale.

Per quanto riguarda l'*unsupervised learning*, l'apprendimento non sorvegliato, non è più presente la figura dell'insegnante: in questa seconda categoria machine learning vengono forniti al sistema IA solo set di dati senza alcuna indicazione del risultato desiderato. Lo scopo di questo secondo metodo di apprendimento è di far risalire il sistema IA a schemi e modelli nascosti, ossia identificare negli input una struttura logica senza che questi siano preventivamente etichettati. Il programma tenta di riconoscere per conto suo i modelli ricorrenti. Per farlo ha ad esempio la possibilità di servirsi del *clustering*: dalla raccolta di tutti i dati seleziona quindi un elemento le cui caratteristiche sono analizzate e confrontate con quelle già esaminate. Se il programma ha già analizzato elementi simili, allora l'oggetto attuale sarà aggiunto a questi; in caso contrario sarà invece isolato.

I sistemi che si basano sull'apprendimento non sorvegliato sono attuati nella sicurezza delle reti.

Nel *machine learning* detto dell'apprendimento per rinforzo (*reinforcement learning*) il processo di addestramento del sistema di Intelligenza Artificiale è molto simile – ad esempio – all'addestramento di animali ed in generale si basa sul concetto di premio. Il sistema di Intelligenza Artificiale riceve in input un obiettivo da raggiungere: conosce l'obiettivo ma non sa raggiungerlo, perché non ha un *dataset* di esempi per fare l'addestramento, né una base di conoscenza pregressa. Il sistema di Intelligenza Artificiale deve imparare dall'esperienza e costruirsi da sé una *knowledge base*, osservando l'ambiente che lo circonda. Quando tale sistema IA prende una decisione, analizza il cambiamento dello stato dell'ambiente valutando i *feedback* tramite una funzione di rinforzo. La funzione di rinforzo (o funzione di rafforzamento) misura il grado di successo di un'azione o decisione, rispetto a un obiettivo predeterminato.

Se il *feedback* è positivo, il sistema IA si è avvicinato all'obiettivo dopo l'azione e la funzione di rinforzo assegna un premio alla (la ricompensa è un valore reale positivo). Se il feedback è negativo e il sistema di IA si è allontanato dall'obiettivo dopo l'azione, la funzione di rinforzo assegna una penalizzazione (un valore reale negativo). Mentre fa esperienza il sistema IA raccoglie preziose informazioni sui *feedback* delle azioni e le registra nella sua *knowledge base*.

I sistemi IA che si basano sul *reinforcement learning* sono impiegati nello sviluppo delle auto a guida autonoma che infatti imparano a riconoscere l'ambiente circostante mediante la raccolta di dati dal mondo fisico attraverso sensori, GPS, ecc. e a adattare il loro comportamento in base alle specifiche situazioni che devono affrontare/superare.

Anche i cosiddetti *sistemi di raccomandazione* sfruttano il *reinforcement learning* imparando dal comportamento e dalle preferenze degli utenti che navigano su siti web, piattaforme o applicazioni *mobile*; ne sono un esempio quelli che comunemente ci siamo abituati a vedere ed utilizzare sulle piattaforme di eCommerce come Amazon o di intrattenimento e accesso a contenuti come Netflix o Spotify.

Infine, vi è il *deep learning* o apprendimento profondo. Il deep machine learning è lo sviluppo in atto verso una nuova fase dell'Intelligenza Artificiale, modello di auto-apprendimento utilizzato da sistemi IA che affrontano problemi tipici dell'intelligenza umana, come pianificare, comprendere linguaggi verbali, riconoscere immagini e suoni, apprendere, definire e risolvere problemi. Il *deep learning* scende appunto in profondità per emulare i meccanismi di apprendimento degli esseri umani, automatizzando analisi e previsioni: esso si serve delle *reti neurali* per analizzare grandi quantità di dati, semplificarli, apprendere dalle decisioni sbagliate, che riconosce e corregge man mano che lavora, trattando sempre più dati e costruendo modelli via via più complessi onde realizzare previsioni sempre più accurate e risolvere problemi sempre più complessi con maggiore efficienza.

* * * * * *

Tornando ora all'esame del gruppo di definizioni di cui all'articolo 3 del Regolamento IA che abbiamo catalogato come pertinenti alla tecnologia IA, alla sua progettazione, utilizzo ed operatività, possiamo elencare le seguenti:

"*scopo previsto*": indica l'uso per il quale un sistema di intelligenza artificiale è destinato dal fornitore, compreso il contesto specifico e le condizioni di utilizzo, come specificato nelle informazioni fornite dal fornitore nelle istruzioni per l'uso, nei materiali promozionali o di vendita e nelle dichiarazioni, così come nella documentazione tecnica;

"*prestazioni di un sistema di intelligenza artificiale*": la capacità di un sistema di intelligenza artificiale di raggiungere il proprio scopo previsto.

Come è evidente, le due definizioni appena sopra riportate assumono rilevanza anche nella prospettiva delle eventuali responsabilità civilistiche per difetti o

malfunzionamento di sistemi di IA che non li rendano in grado di assicurare le prestazioni attese e idonee al raggiungimento dello "scopo previsto" (anche se in tale tematica può entrare in gioco il c.d. "*uso improprio ragionevolmente prevedibile*" altra definizione che significa: "l'uso di un sistema di IA in un modo diverso da quello conforme allo scopo previsto, ma che può ragionevolmente derivare da un comportamento umano prevedibile oppure dalla interazione con altri sistemi").

Interessante poi il gruppo di definizioni "tecnologiche" che attengono alle varie fasi di sviluppo di un sistema di IA, dall'addestramento, alla convalida dei risultati, all'intervento di un certificatore esterno indipendente per la validazione definitiva del sistema, prima dell'avvio delle fasi di sua commercializzazione:

- "*dati di addestramento*": i dati utilizzati per l'addestramento di un sistema di IA attraverso l'adattamento dei parametri di apprendimento, inclusi i nodi di una rete neurale;

- "*dati di convalida*": indica i dati utilizzati per fornire una valutazione dei sistemi di IA – una volta addestrati - e per mettere a punto i suoi parametri non apprendibili e il suo processo di apprendimento, tra altre cose, al fine di prevenire il sovradattamento (c.d. overfitting); anche considerato che il dataset di convalida può essere un dataset separato oppure una parte del dataset di addestramento, sia fisso che variabile;

- "*dati di test*": i dati utilizzati per fornire una valutazione indipendente del sistema di IA una volta che questo sia stato addestrato e validato al fine di confermare le prestazioni attese di tale sistema prima della sua immissione sul mercato o della messa in servizio;

- "*dati di input*": indica i dati forniti a un sistema di IA o acquisiti direttamente da un sistema di intelligenza artificiale e sulla base dei quali il sistema di IA produce un output;

Non è infine illogico classificare la definizione che segue nella categoria che abbiamo definito come pertinente alla *tecnologia IA, alla sua progettazione, utilizzo ed operatività*:

- "*incidente grave*": qualsiasi incidente che, direttamente o indirettamente, comporta, potrebbe aver comportato o potrebbe comportare (si noti l'incertezza del "*potrebbe aver comportato*": in effetti il funzionamento o malfunzionamento di certi sistemi IA – come quelli che utilizzano il *deep learning* o le reti neurali e possono assumere decisioni autonome – può risultare sconosciuto anche ai suoi operatori, che ad esempio non hanno alcuna possibilità di verificare o controllare cosa avviene nei "nodi" più profondi del sistema IA e come vengono precisamente assunte le decisioni operative…) quanto segue:

(a) la morte di una persona o gravi danni alla salute di una persona, alla proprietà o all'ambiente,
b) un'interruzione grave e irreversibile della gestione e del funzionamento di infrastruttura critica.

§ Segue 4.2: le definizioni relative ai soggetti a vario titolo implicati dalla operatività dei sistemi IA.

Quanto alle definizioni dei soggetti a vario titolo implicati dalla operatività dei sistemi IA, vanno elencate le seguenti:

- "*fornitore*" indica una persona fisica o giuridica, autorità pubblica, agenzia o altro ente che sviluppa un sistema di intelligenza artificiale o che ha un sistema di intelligenza artificiale sviluppato nell'ottica di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio, sia a pagamento che a titolo gratuito (la definizione include sia il fornitore-sviluppatore che il fornitore che a diverso titolo ha la disponibilità di un sistema IA non sviluppato da lui);

- "*utente*" indica qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro ente che utilizza un sistema di intelligenza artificiale sotto la sua autorità; tale definizione di utente non si applica al caso di utilizzo di un sistema di intelligenza artificiale nell'ambito di un'attività personale o di un'attività non professionale (va evidenziata l'ampiezza di tale definizione, atta a ricomprendere soggetti e situazioni anche molto diverse tra di loro, oltre alla inapplicabilità della medesima definizione al cosiddetto "*uso domestico*" di un sistema di IA) ;

- "*rappresentante autorizzato*" indica qualsiasi persona fisica o giuridica stabilita nell'Unione che ha ricevuto un mandato scritto da un fornitore di un sistema di intelligenza artificiale che non sia stabilito nella UE per, rispettivamente, eseguire e svolgere per suo conto gli obblighi e le procedure stabilite dal Regolamento (si veda la procedura e gli obblighi di cui all'articolo 25 del Regolamento IA, che introduce un obbligo di nomina di un rappresentante nella UE del fornitore non stabilito laddove sia sconosciuto l'importatore del sistema IA e prima che questo venga immesso sul mercato; tale obbligo ricorda quello analogo del rappresentante del titolare del trattamento di cui all'articolo 27 del GPDR);

- "*importatore*": qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato o mette in servizio un sistema di IA che reca il nome commerciale o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione;

- "*distributore*": qualsiasi persona fisica o giuridica nella *supply chain*, diversa dal fornitore o dall'importatore, che rende disponibile un sistema di IA sul mercato dell'Unione senza che siano coinvolte o impattate sue proprietà;

- "*operatore*": significa il fornitore, l'utente, il rappresentante autorizzato, l'importatore e il distributore.

§ Segue 4.3: le definizioni pertinenti alle attività commerciali aventi ad oggetto i sistemi IA

Quanto al gruppo di definizioni che abbiamo definito come pertinenti alle *attività commerciali aventi ad oggetto i sistemi IA*, vanno elencate le seguenti che attengono a diverse fasi:

(a) preventive alla commercializzazione e di valutazione e controllo della conformità:

"*valutazione della conformità*": il processo per verificare se i requisiti stabiliti al titolo III, capitolo 2 del presente regolamento relativo a un sistema di IA sono stati soddisfatti;

"*autorità di notifica*": l'autorità nazionale responsabile dell'istituzione e dello svolgimento delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio;

"*marchio di conformità CE*" *(marchio CE):* un marchio mediante il quale un fornitore indica che un sistema di IA è conforme ai requisiti di cui al Titolo III, Il capo 2 del Regolamento e ad altra normativa dell'Unione applicabile che armonizza le condizioni per la commercializzazione dei prodotti ("normativa di armonizzazione dell'Unione") recanti detto marchio;

"*specifiche comuni*": indica un documento, diverso da uno standard, contenente soluzioni tecniche che forniscono un mezzo per soddisfare determinati requisiti e obblighi stabiliti ai sensi del presente regolamento;

(b) di immissione sul mercato e di operatività funzionale:

"*immissione sul mercato*": significa la prima messa a disposizione di un sistema di IA sul mercato dell'Unione;

"*messa a disposizione sul mercato*": qualsiasi fornitura di un sistema di IA per la distribuzione o uso sul mercato dell'Unione nel corso di un'attività commerciale, indipendentemente dal fatto che ciò avvenga verso corrispettivo oppure gratuitamente;

"*messa in servizio*": la fornitura di un sistema di IA per il primo utilizzo direttamente all'utente o per uso proprio sul mercato dell'Unione per lo scopo previsto;

"*istruzioni per l'uso*": le informazioni fornite dal fornitore per informare l'utente, in particolare, dello scopo previsto e dell'uso corretto di un sistema di intelligenza artificiale, incluse le informazioni sulle impostazioni relative al contesto geografico, comportamentale o funzionale specifico all'interno del quale il sistema di IA ad alto rischio è destinato ad operare;

(c) di eventuale intervento successivo alla immissione sul mercato, come in caso di non conformità, difetti o malfunzionamento del sistema IA:

"*richiamo di un sistema di IA*": qualsiasi misura volta a ottenere il ritorno al fornitore di un sistema di IA messo a disposizione degli utenti;

"*ritiro di un sistema di IA*" indica qualsiasi misura volta a prevenire la distribuzione, la visione e l'offerta di un sistema AI;

"*componente di sicurezza di un prodotto o sistema*": indica un componente di un prodotto o di un sistema che svolge una funzione di sicurezza per quel prodotto o sistema oppure il guasto o il malfunzionamento che mettono in pericolo la salute e la sicurezza di persone o cose;

"*modifica sostanziale*": indica una modifica al sistema di intelligenza artificiale in seguito alla sua immissione mercato o messa in servizio che influisce sulla conformità del sistema di IA ai i requisiti di cui al Titolo III, Capitolo 2 del Regolamento o si sostanzia in una modifica dello scopo previsto per il quale il sistema di IA è stato progettato;

(d) di eventuale monitoraggio successivo alla immissione sul mercato del sistema IA:

"*monitoraggio successivo all'immissione sul mercato*": tutte le attività svolte dai fornitori di sistemi di IA per raccogliere e rivedere in modo proattivo l'esperienza acquisita dall'uso dei sistemi di intelligenza artificiale da loro immessi sul mercato o messi in servizio al fine di individuare eventuali necessità applicare immediatamente tutte le azioni correttive o preventive necessarie;

"*autorità di vigilanza del mercato*": l'autorità nazionale che esegue le attività e adotta le misure ai sensi del Regolamento (UE) 2019/1020 (detta autorità assicura che i prodotti siano conformi alla normativa di armonizzazione dell'Unione e pertanto soddisfino prescrizioni che offrono un livello elevato di protezione di interessi pubblici quali la salute e la sicurezza in generale, la salute e la sicurezza sul luogo di lavoro, la tutela dei consumatori, la protezione dell'ambiente, la sicurezza pubblica e la protezione di qualsiasi altro interesse pubblico protetto da tale normativa);

§ Segue 4.4: le definizioni relative a particolari sistemi di IA che utilizzano la biometria.

Quanto al gruppo di definizioni che abbiamo definito come *specifiche su particolari sistemi di IA che utilizzano la biometria*, vanno elencate le seguenti:

"*dati biometrici*": dati personali risultanti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che consentono o confermano l'identificazione univoca di quella persona fisica, come ad esempio

immagini del viso o dati dattiloscopici (identica definizione riresa dall'articolo 4, n. 14 del Regolamento Generale UE 679/2016 sulla protezione dei dati personali);

"*sistema di riconoscimento delle emozioni*": indica un sistema di IA che ha lo scopo di identificare o dedurre emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici (e non si può non notare quanto sia sorprendente – e anche un po' inquietante… - una tale definizione giuridica che dà una sorta di "veste legale" alle sofisticate capacità di sistemi di IA di "*dedurre*" tanto "*emozioni*" quanto possibili "*intenzioni*" di un essere umano, ciò che ci avverte sul radicale cambio dei paradigmi definitori usuali cui ci costringono tecnologie come quelle in esame);

"*sistema di classificazione biometrica*": un sistema di IA con lo scopo di assegnare persone fisiche a categorie specifiche, come sesso, età, colore dei capelli, colore degli occhi, tatuaggi, origine etnica o orientamento sessuale o politico, sulla base dei loro dati biometrici (a tali sistemi sono riconnessi i più alti rischi di *bias*, o discriminazioni derivanti dalle cc.dd distorsioni algoritmiche);

"*sistema di identificazione biometrica remota*": un sistema di intelligenza artificiale allo scopo di identificare persone fisiche a distanza attraverso il confronto dei dati biometrici di una persona con i dati biometrici contenuti in un database di riferimento e senza conoscere preliminarmente l'utente del sistema AI o sapere se la persona sarà presente possa essere identificata (si intuisce come a tali sistemi siano riconnessi i più elevati pericoli per l'essenza democratica ove impiegati in maniera abusiva o sproporzionata, anche da autorità pubbliche);

"*sistema di identificazione biometrica a distanza in tempo reale*": indica un sistema di identificazione biometrica remota mediante il quale l'acquisizione di dati biometrici, il confronto e tutte le identificazioni avvengono senza ritardi significativi. Questo comprende non solo la identificazione istantanea, ma anche brevi e limitati ritardi onde evitare l'elusione;

"*sistema di identificazione biometrica a distanza ex post*": indica un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota in tempo reale;

"*spazio accessibile al pubblico*": qualsiasi luogo fisico accessibile al pubblico, indipendentemente dal fatto che possano essere applicate determinate condizioni di accesso (includiamo tale definizione in questo gruppo definitorio poiché è esclusivamente utilizzata come "luogo fisico" della operatività dei sistemi biometrici di cui all'elenco che precede).

§ Segue 4.5: le definizioni relative alle autorità pubbliche utilizzano o sono incaricate della sorveglianza sui sistemi IA.

Quanto, infine, al gruppo di definizioni che abbiamo definito come inerenti alle *autorità pubbliche* (che utilizzano i sistemi o sono incaricate della sorveglianza sui sistemi IA), vanno elencate le seguenti:

"*Autorità deputata all'applicazione della legge/Forze dell'Ordine*" significa:

a) qualsiasi autorità pubblica competente per la prevenzione, l'indagine, l'individuazione o il perseguimento di reati o per l'esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione delle minacce per la pubblica sicurezza; oppure

b) qualsiasi altro ente incaricato dal diritto dello Stato membro di esercitare la pubblica autorità o poteri pubblici ai fini della prevenzione, indagine, accertamento o perseguimento di reati o esecuzione sanzioni penali, compresa la salvaguardia e la prevenzione delle minacce alla sicurezza pubblica.

"*Autorità nazionale di sorveglianza*": l'autorità nazionale alla quale uno Stato membro assegna la responsabilità dell'attuazione e dell'applicazione del presente regolamento, inclusa la responsabilità di coordinare le attività affidate a tale Stato membro e la competenza di agire da unico punto di contatto per la Commissione e di rappresentare lo Stato membro presso il Comitato europeo per l'intelligenza artificiale (si noti come viene replicato il meccanismo del GDPR che all'articolo 68 ha istituito il Comitato Europeo per la protezione dei dati personali);

"*Autorità nazionale competente*": l'autorità nazionale di sorveglianza, l'autorità di notifica e l'autorità di vigilanza del mercato.

§ 5. Le pratiche di intelligenza artificiale vietate.

Di grande interesse per i risvolti etici e politici – oltre che per le ovvie conseguenze pratiche e giuridiche – è la disciplina introdotta dall'articolo 5 (che da solo costituisce il Titolo II del Regolamento IA) sulle cosiddette *pratiche di IA vietate* (si noti il linguaggio quasi di tipo "consumeristico" o "antitrust").

Si noti inoltre come il Legislatore europeo non vieti direttamente i sistemi IA, ma introduca divieti su *pratiche* tecnologiche e commerciali (che naturalmente possono includere sistemi di IA diversi quanto a specifiche tecnologiche, operative e funzionali) come le seguenti.

Intanto, l'Unione Europea vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA:

- che utilizzano tecniche subliminali che vanno al di là della consapevolezza di una persona al fine di distorcere materialmente il comportamento di una persona in un modo che causa o è probabile che possa causare a quella persona o a un'altra persona danni fisici o psicologici;
- che sfruttano una qualsiasi delle vulnerabilità di un gruppo specifico di persone a causa della loro età, disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona appartenente a quel gruppo in un modo che causa o è probabile che possa causare a quella persona o a un'altra persona danni fisici o psicologici.

La *ratio* di tale divieto è la ovvia protezione delle persone rispetto a modalità subliminali e soprattutto dei cosiddetti *soggetti vulnerabili* (minori, anziani, diversamente abili, richiedenti asilo; si ricordi che sono considerati *soggetti deboli* anche i consumatori e i lavoratori).

* * * * * *

La UE vieta poi – per la prima volta in un testo legislativo – il cosiddetto *social credit scoring* (che ad esempio in Cina è sempre più impiegato dalle autorità cittadine), e cioè quella pratica di valutazione sociale basata su un sistema a punti che in base al comportamento sociale dei cittadini può comportare penalizzazioni se si scende al di sotto di una determinata soglia (es: un cittadino che prende molte contravvenzioni; un cittadino che non fa la raccolta differenziata dei rifiuti, etc) fino alla impossibilità di fruire di determinati servizi pubblici (iscrizione a scuole, ammissione a servizi quali mense, etc). Ovvio che per controllare il comportamento dei cittadini serve il largo impiego di sistemi di identificazione biometrica da remoto e in tempo reale attivati nei luoghi pubblici). Ecco perché la UE vieta:

(a) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte di pubbliche autorità o per loro conto allo scopo di procedere alla valutazione o alla classificazione dell'affidabilità delle persone fisiche in un determinato contesto temporale in base al loro comportamento sociale o a caratteristiche personali o di personalità note o previste, con un punteggio sociale che porti a uno o ad entrambe delle seguenti conseguenze:
(i) trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono correlati ai contesti nei quali i dati sono stati originariamente generati o raccolti;
(ii) trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che risulti ingiustificato e sproporzionato rispetto al loro comportamento sociale o alla sua gravità.

* * * * * *

Particolare è la scelta legislativa in merito all'impiego di sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico ai fini dell'applicazione della legge (con particolare riferimento alle attività di prevenzione, indagine e

accertamento dei reati). In tale ambito il divieto non è assoluto ma derogabile nella misura in cui tale uso è strettamente necessario per uno dei seguenti obiettivi:

(i) la ricerca mirata di specifiche potenziali vittime di reati, compresi bambini scomparsi;
(ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o sicurezza fisica delle persone fisiche o di un attacco terroristico;
(ii) l'individuazione, la localizzazione, l'identificazione o il perseguimento di un autore o sospettato autore di un reato di cui all'articolo 2, paragrafo 2, del Consiglio Decisione quadro 2002/584 / GAI62 sul mandato di arresto europeo (es: partecipazione a un'organizzazione criminale, terrorismo, tratta di esseri umani, sfruttamento sessuale dei bambini e pornografia infantile, traffico illecito di stupefacenti e sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, corruzione, frode, etc) che sia punibile nello Stato membro interessato con una pena detentiva o un ordine di detenzione per un periodo massimo di almeno tre anni, come determinato dalla legge dello stesso Stato membro.

L'uso di sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico ai fini che precedono deve comunque basarsi su un sistema doppio di garanzie sostanziali e procedurali. Tra le prime, vanno considerate:

a) la natura della situazione che dà luogo al possibile utilizzo del sistema di identificazione biometrica a distanza in tempo reale, in particolare la gravità, probabilità e entità del danno che sarebbe causato in assenza dell'uso del sistema di identificazione biometrica a distanza in tempo reale;
b) le conseguenze dell'uso del sistema di identificazione biometrica a distanza in tempo reale per i diritti e le libertà di tutti persone interessate, in particolare la gravità, la probabilità e l'entità di tali persone conseguenze.

Quanto alle necessarie e proporzionate garanzie procedurali in relazione all'uso di detti sistemi, ogni singolo utilizzo ai fini di legge di sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico ai fini che abbiamo sopra elencato deve essere soggetto all'autorizzazione preventiva concessa da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro nel quale deve avvenire l'uso, e tale autorizzazione va rilasciata su istanza motivata e in conformità con le norme specifiche del diritto nazionale. Solo in casi di urgenza debitamente giustificata l'uso del sistema può essere avviato senza autorizzazione e l'autorizzazione può essere richieste durante o dopo l'impiego del sistema.

L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione esclusivamente quando è soddisfatto e comprovato - sulla base di prove oggettive o di chiare indicazioni presentate - che l'uso del sistema di identificazione biometrica remota in tempo reale in questione risulta necessario e proporzionato al raggiungimento di uno degli obiettivi leciti specificati nella casistica sopra riportata. Nel decidere sulla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi sopra

specificati (natura della situazione, gravità, entità del danno che sarebbe causato in assenza di autorizzazione, conseguenze per i diritti e le libertà di tutte le persone coinvolte e gravità e entità delle conseguenze).

Ciascuno Stato membro resta comunque libero di decidere di prevedere la possibilità di impiego totale o parziale di sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico ai fini di prevenzione o accertamento. Tale Stato membro stabilisce nella legislazione nazionale le norme dettagliate necessarie per la richiesta, l'emissione ed esercizio, nonché vigilanza sulle autorizzazioni che devono essere rilasciate dall'autorità giudiziaria o amministrativa. Tali regole devono infine specificare anche in relazione a quali degli obiettivi elencati ai punti (i) e (ii) più sopra e in relazione a quali reati di cui al punto (iii), le autorità competenti possono essere autorizzate a utilizzare tali sistemi ai fini indagine, prevenzione o accertamento dei reati.

La scelta legislativa in merito alle deroghe al divieto di impiego di sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico ai fini di prevenzione, indagine e accertamento dei reati risulta essere assistita da efficaci garanzie sostanziali e procedurali, anche se occorrerà esaminare in pratica se autorità ad esempio di polizia o di indagine si atterranno sempre rigorosamente ai vincoli normativi previsti per cui l'utilizzo di tali sistemi di IA basati sulla biometria deve essere inteso come deroga eccezionale a un divieto, o se - al contrario (come avvenuto per altre tecnologie, come ad esempio gli accertamenti sul DNA) - il ricorso a tali sistemi così invasivi non rischi di diventare un ordinario mezzo di indagine o di contrasto.