MISSIONE 1 DIGITALIZZAZIONE, INNOVAZIONE, COMPETITIVITA' – L'intelligenza artificiale nel contesto del diritto vivente europeo

PNRR

Dossier

L'IA nell' EU: strumento per le persone e un fattore positivo per la società

Con il termine intelligenza artificiale si indica una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali. L'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea. La riflessione giuridica in tale ambito applicativo è particolarmente necessaria in settori ad alto impatto, tra i quali figurano quelli dei cambiamenti climatici, dell'ambiente e della sanità, il settore pubblico, la finanza, la mobilità, gli affari interni e l'agricoltura. Tuttavia gli stessi elementi e le stesse tecniche che alimentano i benefici socio-economici dell'IA possono altresì comportare nuovi rischi o conseguenze negative per le persone fisiche o la società. In considerazione della velocità dei cambiamenti tecnologici e delle possibili sfide, l'UE si impegna a perseguire un approccio equilibrato. L'interesse dell'Unione è quello di preservare la leadership tecnologica dell'UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione. In tale ambito è possibile collacore lo sviluppo della riflessione giuridica in analisi, resa viente e in continua evoluzione in aderenza con gli orientamenti politici per la Commissione 2019-2024 nel particolare compito di implementare un approccio normativo europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale.

In una prospettiva di evoluzione storica è utile evidenziare che la Commissione ha pubblicato il 19 febbraio 2020 il Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia[1]. Il Libro bianco definisce le opzioni strategiche su come conseguire il duplice obiettivo di promuovere l'adozione dell'IA e affrontare i rischi associati a determinati utilizzi di tale tecnologia.

In tale ambito assume grande importanza sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile. La rilessione normativa si basa sui valori e sui diritti

[1] Commissione europea, Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia (COM(2020) 65 final).

fondamentali dell'UE e si prefigge di dare alle persone e agli altri utenti la fiducia per adottare le soluzioni basate sull'IA, incoraggiando al contempo le imprese a svilupparle.

L'IA dovrebbe rappresentare uno strumento per le persone e un fattore positivo per la società, con il fine ultimo di migliorare il benessere degli esseri umani. Le regole per l'IA disponibili sul mercato dell'Unione o che comunque interessano le persone nell'Unione dovrebbero pertanto essere incentrate sulle persone, affinché queste ultime possano confidare nel fatto che la tecnologia sia usata in modo sicuro e conforme alla legge, anche in termini di rispetto dei diritti fondamentali. In seguito alla pubblicazione del Libro Bianco, la Commissione ha lanciato un'ampia consultazione dei portatori di interessi, accolta con grande attenzione dai vari operatori, che ha espresso il proprio favore a un intervento normativo volto ad affrontare le sfide e le preoccupazioni sollevate dal crescente utilizzo dell'IA.

In tale sentiero di riflessione vengono valorizzate le indicazioni esplicite del Parlamento europeo e del Consiglio europeo, che hanno ripetutamente chiesto un intervento legislativo che assicuri il buon funzionamento del mercato interno per i sistemi di intelligenza artificiale nel contesto del quale tanto i benefici quanto i rischi legati all'intelligenza artificiale siano adeguatamente affrontati a livello dell'Unione. In tale prospettiva è possibile contribuire all'obiettivo dell'Unione di essere un leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica, come dichiarato dal Consiglio europeo[2], anche garantendo la tutela dei principi etici, come richiesto specificamente dal Parlamento europeo[3]. Nel dettaglio del passaggio storico in analisi è possibile evidenziare che, già nel 2017 il Consiglio europeo ha invitato a dimostrare la consapevolezza dell'urgenza di far fronte alle tendenze emergenti, comprese questioni quali l'intelligenza artificiale, garantendo nel contempo un elevato livello di protezione dei dati, diritti digitali e norme etiche. Nelle sue conclusioni del 2019 sul piano coordinato sullo sviluppo e l'utilizzo dell'intelligenza artificiale di matrice europea, il Consiglio ha inoltre posto l'accento sull'importanza di garantire il **pieno rispetto dei diritti dei cittadini dell'unione e ha esortato a rivedere la normativa pertinente in vigore con l'obiettivo di garantire che essa fosse idonea a cogliere le nuove opportunità e sfide poste dall'intelligenza artificiale**. Il Consiglio europeo ha inoltre invitato a definire in maniera chiara le applicazioni di IA che dovrebbero essere considerate ad alto rischio. Scorrendo l'asse del tempo, nei testi ufficiali vergati nel 21 ottobre 2020 si esortava inoltre ad affrontare l'opacità, la complessità, la faziosità, un certo grado di imprevedibilità e un comportamento parzialmente autonomo di taluni sistemi di IA, onde

[2] Consiglio europeo, Riunione straordinaria del Consiglio europeo (1° e 2 ottobre 2020) - Conclusioni, EUCO 13/20, 2020, pag. 7.

[3] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

garantirne la compatibilità con i diritti fondamentali e agevolare l'applicazione delle norme giuridiche[4].

In concordanza con tale prospettiva, anche il Parlamento europeo ha intrapreso una quantità considerevole di attività nel settore dell'IA.

Nell'ottobre del 2020 si sono adottate una serie di risoluzioni concernenti l'IA, anche in relazione ad etica[5], responsabilità[6] e diritti d'autore[7]. Nel 2021 tali risoluzioni sono state seguite da risoluzioni sull'IA in ambito penale[8] nonché nell'istruzione, nella cultura e nel settore audiovisivo[9]. Nella prospettiva concreta di intervento tematico, il parlamento europeo decina quindi un quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate e raccomanda specificamente alla Commissione di proporre una misura legislativa per sfruttare le opportunità e i benefici dell'IA, ma anche per assicurare la tutela dei principi etici.

Tale risoluzione comprende specifiche indicazioni di natura giuridica strumentali per l'elaborazione di misure regolamentari sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'IA, della robotica e delle tecnologie correlate. In tale scenario le linee della Commissione descrivono un quadro normativo sull'intelligenza artificiale con i seguenti **obiettivi specifici**:

assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione;

assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale;

migliorare la governance e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA;

facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato.

---

4 Consiglio dell'Unione Europea, Conclusioni della presidenza – La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale, 11481/20, 2020.

5 Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, 2020/2012(INL).

6 Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 2020/2014(INL).

7 Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, 2020/2015(INI).

8 Progetto di relazione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, 2020/2016(INI).

9 Progetto di relazione del Parlamento europeo sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo, 2020/2017(INI). A tale riguardo, la Commissione ha adottato il piano d'azione per l'istruzione digitale 2021-2027 - Ripensare l'istruzione e la formazione per l'era digitale (comunicazione della Commissione COM(2020) 624 final), che prevede l'elaborazione di orientamenti etici sull'intelligenza artificiale e sull'utilizzo dei dati nell'istruzione.

Al fine di conseguire tali obiettivi è sotteso al legislatore un approccio normativo orizzontale all'IA equilibrato e proporzionato, che si limita ai requisiti minimi necessari per affrontare i rischi e i problemi ad essa collegati, senza limitare od ostacolare indebitamente lo sviluppo tecnologico o altrimenti aumentare in modo sproporzionato il costo dell'immissione sul mercato di soluzioni informatiche. In tale direzione emerge la necessità di completezza in aderenza alle esigenze future per quanto concerne le scelte normative fondamentali, compresi i requisiti basati sui principi che i sistemi di IA dovrebbero soddisfare. In secondo luogo è possibile valutare la messa in atto di un sistema normativo proporzionato incentrato su un approccio normativo ben definito basato sul rischio che non crea restrizioni inutili al commercio, motivo per cui l'intervento legale è adattato alle situazioni concrete nelle quali sussiste un motivo di preoccupazione giustificato o nelle quali tale preoccupazione può essere ragionevolmente prevista nel prossimo futuro. Allo stesso tempo il quadro giuridico concepito può comprendere meccanismi flessibili che fanno sì che esso possa essere adeguato dinamicamente all'evoluzione della tecnologia e all'emergere di nuove situazioni di preoccupazione. In questo scenario di analisi è possibile fissare le regole armonizzate per lo sviluppo, l'immissione sul mercato e l'utilizzo di sistemi di IA nell'Unione seguendo un approccio proporzionato basato sul rischio.

In ambito europeo si propone un'unica definizione di IA adeguata alle esigenze future. Talune pratiche di IA particolarmente dannose sono vietate in quanto in contrasto con i valori dell'Unione, mentre sono proposte restrizioni e tutele specifiche in relazione a determinati usi dei sistemi di identificazione biometrica remota a fini di attività di contrasto. L'attenzione del legislatore, allora, stabilisce una solida metodologia per la gestione dei rischi impiegata per definire i sistemi di IA "ad alto rischio" che pongono rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone. Tali sistemi di IA dovranno rispettare una serie di requisiti obbligatori orizzontali per un'IA affidabile nonché seguire le procedure di valutazione della conformità prima di poter essere immessi sul mercato dell'Unione. Obblighi prevedibili, proporzionati e chiari sono posti in capo anche a fornitori e utenti di tali sistemi con l'obiettivo di assicurare la sicurezza e il rispetto della normativa vigente che tutela i diritti fondamentali durante l'intero ciclo di vita dei sistemi di IA. Per taluni sistemi specifici di IA, vengono proposti soltanto obblighi minimi di trasparenza, in particolare quando vengono utilizzati chatbot. Le regole sviluppate dal legislatore europeo saranno applicate tramite un sistema di governance a livello di Stati membri, sulla base di strutture già esistenti, e un meccanismo di cooperazione a livello dell'Unione con l'istituzione di un comitato europeo per l'intelligenza artificiale. Vengono inoltre declinate misure aggiuntive per sostenere l'innovazione, in particolare attraverso spazi di sperimentazione normativa per l'IA e altre

misure per ridurre gli oneri normativi e sostenere le piccole e medie imprese ("PMI") e le start-up. La natura orizzontale dell' intervento giuridico richiede un'assoluta coerenza con la normativa vigente dell'Unione applicabile ai settori nei quali i sistemi di IA ad alto rischio sono già utilizzati o saranno probabilmente utilizzati in un prossimo futuro. In tale sentiero è assicurata la coerenza con la Carta dei diritti fondamentali dell'Unione europea e il diritto derivato dell'UE in vigore in materia di protezione dei dati, tutela dei consumatori, non discriminazione e parità di genere. Non si pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680) e li integra con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio nonché di restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota. In tale chiave giuridica e operativa si integra inoltre il diritto dell'Unione in vigore in materia di non discriminazione con requisiti specifici che mirano a ridurre al minimo il rischio di discriminazione algoritmica, in particolare in relazione alla progettazione e alla qualità dei set di dati utilizzati per lo sviluppo dei sistemi di IA, integrati con obblighi relativi alle prove, alla gestione dei rischi, alla documentazione e alla sorveglianza umana durante l'intero ciclo di vita dei sistemi di IA. Per quanto concerne i sistemi di IA ad alto rischio che sono componenti di sicurezza dei prodotti, la il quadro normativo di riferimento sarà integrato nella normativa settoriale vigente in materia di sicurezza, al fine di assicurare la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi. In particolare, per quanto concerne i sistemi di IA ad alto rischio collegati a prodotti soggetti al nuovo quadro normativo, i requisiti per i sistemi di IA saranno verificati nel contesto delle procedure di valutazione della conformità esistenti ai sensi della legislazione pertinente di detto nuovo quadro normativo. Per quanto concerne l'interazione dei requisiti, mentre i rischi per la sicurezza specifici dei sistemi di IA sono destinati a essere soggetti ai requisiti generali, la legislazione del nuovo quadro normativo mira a garantire la sicurezza complessiva del prodotto finale e può pertanto contenere requisiti specifici concernenti l'integrazione sicura di un sistema di IA nel prodotto finale. Per quanto concerne i sistemi di IA forniti o utilizzati da enti creditizi regolamentati, le autorità competenti per il controllo sulla normativa dell'Unione in materia di servizi finanziari dovrebbero essere designate come autorità competenti per il controllo sui requisiti previsti dalle norme al fine di assicurare un'applicazione coerente degli obblighi previsti dell'Unione in materia di servizi finanziari laddove i sistemi di IA siano in una certa misura implicitamente regolamentati in relazione al sistema di governance interna degli enti creditizi. Al fine di migliorare ulteriormente la coerenza, la procedura di valutazione della conformità e taluni degli obblighi procedurali dei fornitori sono previste integrazioni nelle procedure ai sensi della direttiva 2013/36/UE sull'accesso all'attività degli enti creditizi e sulla

vigilanza prudenziale[10]. In tale ambito si riscontra la coerenza con la legislazione dell'Unione applicabile ai servizi, compresi i servizi di intermediazione regolati dalla direttiva sul commercio elettronico (direttiva 2000/31/CE)[11] e la recente proposta della Commissione per la legge sui servizi digitali[12].

I problemi posti dallo sviluppo e dall'utilizzo dell'IA

La rilessione normativa in rassegna fa parte di un pacchetto più ampio di misure destinate ad affrontare i problemi posti dallo sviluppo e dall'utilizzo dell'IA, come esaminato nel Libro bianco sull'intelligenza artificiale. Sono pertanto garantite la coerenza e la complementarità rispetto ad altre iniziative in corso o previste della Commissione, volte anch'esse ad affrontare tali problemi, comprese la revisione della normativa settoriale sui prodotti (ad esempio la direttiva macchine, la direttiva sulla sicurezza generale dei prodotti) e le iniziative che affrontano le questioni connesse alla responsabilità in relazione alle nuove tecnologie, compresi i sistemi di IA. Tali iniziative si baseranno sulla presente proposta e la integreranno al fine di apportare chiarezza giuridica e favorire lo sviluppo di un ecosistema di fiducia nei confronti dell'IA in Europa. Nel dettaglio si verifica la coerenza con la strategia digitale globale della Commissione nel contesto del suo contributo alla promozione della tecnologia al servizio delle persone, uno dei tre pilastri principali dell'orientamento politico e degli obiettivi annunciati nella comunicazione "Plasmare il futuro digitale dell'Europa"[13]. Stabilisce un quadro coerente, efficace e proporzionato per assicurare che l'IA si sviluppi secondo modalità che rispettano i diritti delle persone e ne guadagnano la fiducia, rendendo l'Europa adatta all'era digitale e trasformando i prossimi dieci anni nel **decennio digitale**[14]. Inoltre la promozione dell'innovazione basata sull'IA è strettamente legata all'**Atto sulla governance dei dati**[15]**,** alla **direttiva sull'apertura dei dati**[16] e ad altre iniziative nell'ambito della **strategia dell'UE per i dati**[17], che stabiliranno meccanismi e servizi affidabili per il

10 Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

11 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") (GU L 178 del 17.7.2000, pag. 1).

12 Cfr. proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (COM/2020/825 final).

13 Comunicazione della Commissione, Plasmare il futuro digitale dell'Europa (COM(2020) 67 final).

14 Bussola per il digitale 2030: il modello europeo per il decennio digitale.

15 Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati) (COM/2020/767).

16 Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, PE/28/2019/REV/1 (GU L 172 del 26.6.2019, pag. 56).

17 Comunicazione della Commissione, Una strategia europea per i dati (COM/2020/66 final).

riutilizzo, la condivisione e la messa in comune dei dati, essenziali per lo sviluppo di modelli di IA di alta qualità basati sui dati. In tale direzione si rafforza in maniera significativa il ruolo dell'Unione per quanto riguarda il contributo alla definizione di norme e standard globali e la promozione di un'IA in aderenza con i valori e gli interessi dell'Unione. Essa fornisce all'Unione una base solida per impegnarsi ulteriormente con i suoi partner esterni, compresi i paesi terzi, e nei consessi internazionali in merito a questioni relative all'IA. La base giuridica del pensiero del legislatore, sul quale si innesta l'elaborazione delle normative in descrivione, è incentrato sull'114 del trattato sul funzionamento dell'Unione europea (TFUE), che prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno. Infatti con le stesse di costituisce una parte fondamentale della strategia dell'Unione per il mercato unico digitale. L'obiettivo principale è assicurare il buon funzionamento del mercato interno fissando regole armonizzate, in particolare per quanto concerne lo sviluppo, l'immissione sul mercato dell'Unione e l'utilizzo di prodotti e servizi che ricorrono a tecnologie di intelligenza artificiale o forniti come sistemi di IA indipendenti ("stand-alone"). Taluni Stati membri stanno già prendendo in considerazione l'adozione di regole nazionali destinate ad assicurare che l'IA sia sicura e venga sviluppata e utilizzata nel rispetto dei diritti fondamentali. È probabile che ciò determini due problemi principali:

- una frammentazione del mercato interno su elementi essenziali concernenti in particolare i requisiti dei prodotti e dei servizi di IA, la loro commercializzazione, il loro utilizzo, la responsabilità e il controllo da parte delle autorità pubbliche;
- la riduzione sostanziale della certezza del diritto tanto per i fornitori quanto per gli utenti dei sistemi di IA in merito alle modalità secondo cui le regole nuove e quelle esistenti si applicheranno a tali sistemi nell'Unione.

Data l'ampia circolazione di prodotti e servizi a livello transfrontaliero, questi due problemi possono essere risolti al meglio attraverso l'armonizzazione della legislazione a livello UE. Si definiscono infatti dei requisiti obbligatori comuni applicabili alla progettazione e allo sviluppo di alcuni sistemi di IA prima della loro immissione sul mercato, che saranno resi ulteriormente operativi attraverso norme tecniche armonizzate. Sono contemplati altresì la situazione successiva all'immissione sul mercato dei sistemi di IA armonizzando le modalità secondo cui sono eseguiti i controlli ex post. Inoltre, considerando che le norme contengono talune regole specifiche sulla protezione delle persone fisiche per quanto concerne il trattamento di dati personali, in particolare restrizioni sull'utilizzo di sistemi di IA per l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, è

opportuno richiamare, per quanto concerne tali regole specifiche, l'articolo 16 TFUE. La natura dell'IA, che si basa spesso su set di dati di grandi dimensioni e varietà che possono essere integrati in qualsiasi prodotto o servizio che circola liberamente nel mercato interno, implica che gli obiettivi non possano essere conseguiti in maniera efficace dai singoli Stati membri. Il formarsi di un mosaico di regole nazionali potenzialmente divergenti potrebbe inoltre ostacolare la circolazione senza soluzione di continuità di prodotti e servizi collegati ai sistemi di IA in tutta l'UE e potrebbe dimostrarsi inefficace nel garantire la sicurezza e la protezione dei diritti fondamentali e dei valori dell'Unione nei diversi Stati membri. Gli approcci nazionali destinati ad affrontare tali problemi creerebbero soltanto incertezza e ostacoli ulteriori e rallenterebbero l'adozione dell'IA da parte del mercato. Gli obiettivi di fondo possono essere meglio conseguiti a livello dell'Unione per evitare un'ulteriore frammentazione del mercato unico in quadri nazionali potenzialmente contraddittori che impediscono la libera circolazione di beni e servizi in cui è integrata l'IA. Un solido quadro normativo europeo per un'IA affidabile assicurerà altresì parità di condizioni e tutelerà tutte le persone, rafforzando allo stesso tempo la competitività e la base industriale dell'Europa nel settore dell'IA. **Soltanto un'azione comune a livello di Unione può altresì tutelare la sovranità digitale dell'Unione e sfruttare gli strumenti e i poteri di regolamentazione di quest'ultima per plasmare regole e norme di portata globale.**

Percorrendo un ulteriore passo nel sentiero della descrizione è possibile valutare che il quadro normativo sull' IA segue un approccio basato sul rischio e impone oneri normativi soltanto laddove un sistema di intelligenza artificiale possa comportare rischi alti per i diritti fondamentali e la sicurezza. Per altri sistemi di IA non ad alto rischio sono imposti soltanto obblighi di trasparenza molto limitati, ad esempio in termini di fornitura di informazioni per segnalare l'utilizzo di un sistema di IA nelle interazioni con esseri umani. Norme armonizzate e strumenti di sostegno per l'orientamento e la conformità forniranno assistenza a fornitori e utenti ai fini del rispetto dei requisiti stabiliti dalla presente proposta e della riduzione dei costi. In tale ambito lo strumento normativo più adeguato è il regolamento, atto giuridico è giustificata dalla necessità di un'applicazione uniforme delle nuove regole, come la definizione di IA, il divieto di talune pratiche dannose consentite dall'IA e la classificazione di taluni sistemi di IA. L'applicabilità diretta di un regolamento, conformemente all'articolo 288 TFUE, ridurrà la frammentazione giuridica e faciliterà lo sviluppo di un mercato unico per sistemi di IA leciti, sicuri e affidabili. Tale obiettivo sarà conseguito in particolare introducendo una serie armonizzata di requisiti di base per quanto concerne i sistemi di IA classificati come ad alto rischio e di obblighi riguardanti fornitori e utenti di tali sistemi, migliorando la tutela dei diritti fondamentali e garantendo certezza del

diritto tanto per gli operatori quanto per i consumatori. Allo stesso tempo, le disposizioni del regolamento non sono eccessivamente prescrittive e lasciano spazio a diversi livelli di azione da parte degli Stati membri in relazione ad aspetti che non pregiudicano il conseguimento degli obiettivi dell'iniziativa, in particolare l'organizzazione interna del sistema di vigilanza del mercato e l'adozione di misure destinate a promuovere l'innovazione.

La normativa frutto di un processo di consultazione continuo e vivente

La normativa sull' IA in sede europea è il risultato di un'ampia consultazione di tutti i principali portatori di interessi, nel contesto della quale sono stati applicati i principi generali e le norme minime per la consultazione delle parti interessate da parte della Commissione. Una **consultazione pubblica online** è stata avviata il 19 febbraio 2020, unitamente alla pubblicazione del Libro bianco sull'intelligenza artificiale, ed è durata fino al 14 giugno 2020. L'obiettivo di tale consultazione era raccogliere opinioni e pareri sul Libro bianco. Tale consultazione è stata rivolta a tutti i portatori di interessi coinvolti del settore pubblico e di quello privato, compresi governi, autorità locali, organizzazioni commerciali e non, parti sociali, esperti, accademici e cittadini. Dopo aver analizzato tutte le risposte pervenute, la Commissione ha pubblicato una sintesi dei risultati, così come le singole risposte, sul proprio sito web [18][19]. Complessivamente è stato registrato un consenso generale tra i portatori di interessi in merito alla necessità di intervenire. Una grande maggioranza dei portatori di interessi si è detta concorde in merito al fatto che esistano lacune legislative o che sia necessaria una normativa nuova. Tuttavia diversi portatori di interessi hanno avvertito la Commissione di evitare duplicazioni, obblighi contrastanti e una regolamentazione eccessiva. Sono pervenute numerose osservazioni nelle quali è stata sottolineata l'importanza di un quadro normativo proporzionato e neutro dal punto di vista tecnologico. I portatori di interessi hanno richiesto per lo più una definizione restrittiva, chiara e precisa del concetto di intelligenza artificiale. I portatori di interessi hanno altresì sottolineato che, oltre al chiarimento del

[18] Complessivamente sono pervenuti 1 215 contributi, di cui 352 da imprese od organizzazioni/associazioni di imprese, 406 da persone fisiche (92 % persone fisiche dell'UE), 152 a nome di istituzioni accademiche/di ricerca e 73 da autorità pubbliche. I pareri della società civile sono stati rappresentati da 160 partecipanti (tra cui 9 organizzazioni di consumatori, 129 organizzazioni non governative e 22 sindacati); 72 partecipanti hanno invece contribuito classificandosi come "altri". Dei 352 rappresentanti di imprese e dell'industria, 222 sono stati imprese e rappresentanti di imprese, il 41,5 % delle quali apparteneva alla categoria delle micro, piccole e medie imprese. Nel resto dei casi si è trattato di associazioni di imprese. Complessivamente l'84 % delle risposte ricevute da imprese e dall'industria è pervenuto dall'UE-27. A seconda della domanda, tra 81 e 598 partecipanti hanno utilizzato l'opzione di testo libero per inserire osservazioni. Oltre 450 documenti di sintesi sono stati presentati tramite il sito web EUSurvey, in aggiunta alle risposte al questionario (oltre 400) oppure sotto forma di contributi indipendenti (oltre 50).

19 Cfr. tutti i risultati della consultazione.

termine "intelligenza artificiale", è importante definire anche "rischio", "alto rischio", "basso rischio", "identificazione biometrica remota" e "danno". La maggior parte dei partecipanti si è detta esplicitamente a favore dell'approccio basato sul rischio. Il ricorso a un quadro basato sul rischio è stato considerato un'opzione migliore rispetto a una regolamentazione di natura generale applicabile a tutti i sistemi di IA. I tipi di rischi e minacce dovrebbero essere basati su un approccio per singolo settore e per singolo caso. I rischi dovrebbero inoltre essere calcolati tenendo conto del loro impatto su diritti e sicurezza. Disporre di spazi di sperimentazione normativa potrebbe essere molto utile per promuovere l'IA e tale possibilità è stata accolta con favore da taluni portatori di interessi, in particolare le associazioni di imprese. Tra coloro che hanno formulato la loro opinione in merito ai modelli di applicazione, più del 50 %, in particolare appartenenti ad associazioni di imprese, si è detto a favore di una combinazione di un'autovalutazione ex-ante del rischio e un'applicazione ex post per i sistemi di IA ad alto rischio. Inoltre sembra importante evidenziare che il quadro normativo europeo sull' IA si basa su due anni di analisi e uno stretto coinvolgimento dei portatori di interessi, tra i quali figurano accademici, imprese, parti sociali, organizzazioni non governative, Stati membri e cittadini. I lavori preparatori sono iniziati nel 2018 con la creazione di un **gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG)**, avente una configurazione ampia e inclusiva, costituito da 52 esperti di chiara fama incaricati di fornire consulenza alla Commissione in merito all'attuazione della sua strategia sull'intelligenza artificiale. Nell'aprile del 2019 la Commissione ha sostenuto[20] i requisiti fondamentali stabiliti negli orientamenti etici dell'AI HLEG per un'IA affidabile[21], che erano stati rivisti per tenere conto di più di 500 osservazioni formulate da portatori di interessi. I requisiti fondamentali riflettono un approccio diffuso e comune, come evidenziato da una pletora di codici etici e principi sviluppati da numerose organizzazioni private e pubbliche in Europa e al di fuori dei suoi confini, secondo il quale lo sviluppo e l'utilizzo di IA dovrebbero essere guidati da alcuni principi essenziali orientati ai valori. L'elenco di valutazione per un'intelligenza artificiale affidabile (ALTAI, dal titolo inglese della pubblicazione)[22] ha reso operativi tali requisiti nel contesto di un processo pilota che ha coinvolto oltre 350 organizzazioni. È stata inoltre istituita l'**Alleanza per l'IA**[23], costituita da una piattaforma destinata a consentire a circa 4 000 portatori di interessi di discutere le implicazioni tecnologiche e sociali dell'IA, che culmina in un'assemblea annuale sull'IA. Il **Libro bianco** sull'intelligenza artificiale ha sviluppato ulteriormente tale approccio inclusivo, incoraggiando la presentazione di osservazioni da parte di oltre 1 250 portatori di

20 Commissione europea, Creare fiducia nell'intelligenza artificiale antropocentrica, COM(2019) 168 final.
21 Gruppo di esperti ad alto livello sull'intelligenza artificiale, Orientamenti etici per un'IA affidabile, 2019.
22 Gruppo di esperti ad alto livello sull'intelligenza artificiale, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 2020.
23 L'Alleanza per l'IA è un forum che coinvolge più portatori di interessi lanciato nel giugno del 2018. Alleanza per l'IA: https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

interessi, comprese più di 450 prese di posizione aggiuntive. Di conseguenza la Commissione ha pubblicato una valutazione d'impatto iniziale, che ha a sua volta attirato più di 130 osservazioni[24]. Sono stati organizzati anche **seminari ed eventi supplementari dedicati ai portatori di interessi,** i cui risultati hanno sostenuto l'analisi contenuta nella valutazione d'impatto e le scelte politiche effettuate nella presente proposta[25]. È stato altresì commissionato uno **studio esterno** destinato ad alimentare la valutazione d'impatto. In linea con la sua politica "Legiferare meglio", la Commissione ha condotto una valutazione d'impatto in relazione alla nuovo quadro normativo da implementare di natura regolamentare, esaminata dal comitato per il controllo normativo della Commissione. Il 16 dicembre 2020 si è tenuta una riunione con tale comitato, alla quale è seguita la formulazione di un parere negativo. Dopo una revisione sostanziale volta ad affrontare le osservazioni formulate e ripresentare la valutazione d'impatto, il 21 marzo 2021 il comitato per il controllo normativo ha emesso un parere positivo. I pareri del comitato per il controllo normativo, le raccomandazioni e una spiegazione di come queste ultime sono state prese in considerazione sono presentati nell'allegato 1 della valutazione d'impatto.

Il lavoro della Commissione Europea: verso le condizioni di sviluppo dell' IA

La Commissione ha esaminato diverse opzioni strategiche destinate al conseguimento dell'obiettivo generale delle norme sull' IA, ossia quello di **assicurare il buon funzionamento del mercato unico** creando le condizioni per lo sviluppo e l'utilizzo di un'IA affidabile nell'Unione.

Sono state valutate quattro opzioni strategiche che presentano gradi diversi di intervento normativo:

opzione 1: strumento legislativo dell'UE che istituisce un sistema di etichettatura volontario;

opzione 2: approccio settoriale "ad hoc";

opzione 3: strumento legislativo orizzontale dell'UE che segue un approccio proporzionato basato sul rischio;

24 Commissione europea, Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence.
25 Per informazioni dettagliate in merito a tutte le consultazioni svolte si rimanda all'allegato 2 della valutazione d'impatto.

Opzione 3+: strumento legislativo orizzontale dell'UE che segue un approccio proporzionato basato sul rischio + codici di condotta per i sistemi di IA non ad alto rischio;

opzione 4: strumento legislativo orizzontale dell'UE che stabilisce requisiti obbligatori per tutti i sistemi di IA, indipendentemente dal rischio che pongono.

Secondo la metodologia stabilita dalla Commissione, ciascuna opzione strategica è stata valutata rispetto agli impatti economici e sociali, prestando un'attenzione particolare all'impatto sui diritti fondamentali. L'opzione prescelta è l'opzione 3+ che prevede un quadro normativo soltanto per i sistemi di IA ad alto rischio, con la possibilità per tutti i fornitori di sistemi di IA non ad alto rischio di seguire un codice di condotta. I requisiti concernono i dati, la documentazione e la tracciabilità, la fornitura di informazioni e la trasparenza, la sorveglianza umana nonché la robustezza e la precisione. Le imprese che introducessero codici di condotta per altri sistemi di IA lo farebbero su base volontaria. L'opzione prescelta è stata considerata dalla dottrina adeguata per affrontare nel modo più efficace gli obiettivi della presente proposta. Richiedendo una serie limitata ma efficace di interventi da parte di sviluppatori e utenti dell'IA, l'opzione prescelta limita infatti i rischi di violazione dei diritti fondamentali e della sicurezza delle persone e promuove attività efficaci di controllo e applicazione, concentrando i requisiti soltanto sui sistemi che presentano un rischio alto di occorrenza di tali violazioni. Di conseguenza tale opzione mantiene i costi di conformità al minimo, evitando così un inutile rallentamento dell'adozione dovuto a prezzi e costi di conformità più elevati. Al fine di affrontare i possibili svantaggi per le PMI, tale opzione comprende diverse disposizioni destinate a sostenere la loro conformità e ridurre i loro costi, tra le quali la creazione di spazi di sperimentazione normativa e l'obbligo di considerare gli interessi delle PMI quando si fissano le tariffe relative alla valutazione della conformità. Secondo gli esperti della Commissione, l'opzione prescelta aumenterà la fiducia delle persone nei confronti dell'IA, le imprese otterranno vantaggi in termini di certezza del diritto e gli Stati membri non avranno motivo per intraprendere azioni unilaterali che potrebbero frammentare il mercato unico. L'incremento della domanda, in ragione di una fiducia maggiore, e delle offerte disponibili, grazie alla certezza del diritto, nonché l'assenza di ostacoli alla circolazione transfrontaliera dei sistemi di IA faranno probabilmente sì che il mercato unico per l'IA sia fiorente. L'Unione europea continuerà a sviluppare un ecosistema di servizi e prodotti innovativi di IA in rapida crescita che integrano la tecnologia dell'IA o sistemi di IA indipendenti, con conseguente aumento dell'autonomia digitale. Inoltre la letteratura specialista ufficiale della Commisione mette in luce gli obblighi giuridici che si applicheranno a fornitori e utenti di sistemi di IA ad alto rischio. Per i fornitori che sviluppano e immettono tali sistemi sul mercato dell'Unione, si crea certezza del diritto e si assicura l'assenza di ostacoli

alla fornitura transfrontaliera di servizi e prodotti collegati all'IA. Per le imprese che utilizzano l'IA, si promuove la fiducia tra i loro clienti, mentre per le amministrazioni pubbliche nazionali si promuove la fiducia del pubblico nell'utilizzo dell'IA e si rafforzano i meccanismi di applicazione, introducendo un meccanismo di coordinamento europeo, fornendo capacità adeguate e facilitando l'audit dei sistemi di IA con requisiti nuovi per quanto concerne la documentazione, la tracciabilità e la trasparenza. Inoltre il quadro tecnico prevede misure specifiche a sostegno dell'innovazione, tra le quali spazi di sperimentazione normativa e misure specifiche per sostenere utenti e fornitori di piccole dimensioni di sistemi di IA ad alto rischio affinché possano conformarsi alle nuove regole. Le normative mirano inoltre a rafforzare la competitività e la base industriale dell'Europa nel settore dell'IA. È assicurata la piena coerenza con la vigente normativa settoriale dell'Unione applicabile ai sistemi di IA il che apporterà ulteriore chiarezza e semplificherà l'applicazione delle nuove regole.

Le riflessioni nella Commissione in merito all' IA e i diritti fondamentali

L'utilizzo dell'IA con le sue caratteristiche specifiche può però incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea. In tale delicato aspetto, il legislatore mira ad assicurare un livello elevato di protezione di tali diritti fondamentali e ad affrontare varie fonti di rischio attraverso un approccio basato sul rischio chiaramente definito. **Definendo una serie di requisiti per un'IA affidabile e di obblighi proporzionati per tutti i partecipanti alla catena del valore, si vuole migliorare e promuovere la protezione dei diritti tutelati dalla Carta: il diritto alla dignità umana, al rispetto della vita privata e alla protezione dei dati di carattere personale, alla non discriminazione e alla parità tra donne e uomini.** Essa mira a prevenire un effetto dissuasivo sui diritti alla libertà di espressione e alla libertà di riunione nonché ad assicurare la tutela del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa), così come il principio generale di buona amministrazione. Si inciderà inoltre positivamente, secondo quanto applicabile in determinati settori, sui diritti di una serie di gruppi speciali, quali i diritti dei lavoratori a condizioni di lavoro giuste ed eque, un livello elevato di protezione dei consumatori, i diritti del minore e l'inserimento delle persone con disabilità.

Rilevante è anche il diritto a un livello elevato di tutela dell'ambiente e al miglioramento della sua qualità, anche in relazione alla salute e alla sicurezza delle persone. Gli obblighi di prova ex ante, di gestione dei rischi e di sorveglianza umana faciliteranno altresì il rispetto di altri

diritti fondamentali, riducendo al minimo il rischio di decisioni errate o distorte assistite dall'IA in settori critici quali l'istruzione e la formazione, l'occupazione, servizi importanti, le attività di contrasto e il sistema giudiziario. Nel caso in cui si verifichino comunque violazioni dei diritti fondamentali, un ricorso efficace a favore delle persone lese sarà reso possibile assicurando la trasparenza e la tracciabilità dei sistemi di IA unitamente a rigidi controlli ex post. Nell'idea della Commissione c'è la convinzione di imporre alcune restrizioni alla libertà d'impresa e alla libertà delle arti e delle scienze al fine di assicurare il rispetto di motivi imperativi d'interesse pubblico quali la salute, la sicurezza, la tutela dei consumatori e la protezione di altri diritti fondamentali c.d. "innovazione responsabile" nel momento in cui si diffonde e si utilizza una tecnologia di IA. Tali restrizioni sono proporzionate e limitate al minimo necessario per prevenire e attenuare rischi gravi per la sicurezza e probabili violazioni dei diritti fondamentali. Inoltre i maggiori obblighi di trasparenza non incideranno in maniera sproporzionata sul diritto alla protezione della proprietà intellettuale, dato che saranno limitati soltanto alle informazioni minime necessarie affinché le persone possano esercitare il loro diritto a un ricorso effettivo e alla necessaria trasparenza presso le autorità di controllo e di contrasto, in linea con i loro mandati. Qualsiasi divulgazione di informazioni sarà effettuata in conformità alla legislazione pertinente nel settore, compresa la direttiva (UE) 2016/943 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti. Le autorità pubbliche e gli organismi notificati, quando hanno necessità di accedere a informazioni riservate o al codice sorgente per esaminare il rispetto di obblighi sostanziali, sono sottoposti a obblighi di riservatezza vincolanti. Nel redigere il testo del Regolamento, gli analisiti della Commisione hanno avuto un approccio integrale al problema teso ad offrire una normativa armonica. Lo scopo è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale (IA) in conformità ai valori dell'Unione. Il testo persegue una serie di motivi imperativi di interesse pubblico, quali un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, e garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento. In tale direzione, i sistemi di intelligenza artificiale possono essere facilmente impiegati in molteplici settori dell'economia e della società, anche a livello transfrontaliero, e circolare in tutta l'Unione. Alcuni Stati membri hanno già preso in esame l'adozione di regole nazionali per garantire che l'intelligenza artificiale sia sicura e sia sviluppata e utilizzata nel rispetto degli obblighi in materia di diritti fondamentali. Normative nazionali divergenti possono determinare una frammentazione del mercato interno e

diminuire la certezza del diritto per gli operatori che sviluppano o utilizzano sistemi di IA. È pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione 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, sulla base dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE). Nella misura in cui il testo prevede regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, è opportuno basare il dato regolamentare, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE. Alla luce di tali regole specifiche e del ricorso all'articolo 16 TFUE, è opportuna la sinergia con il comitato europeo per la protezione dei dati. Sembra importante rammentare che l'intelligenza artificiale consiste in una famiglia di tecnologie in rapida evoluzione che può contribuire al conseguimento di un'ampia gamma di benefici a livello economico e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale ed ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, istruzione e formazione, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, mitigazione dei cambiamenti climatici e adattamento ad essi.

L'IA nell' analisi swot rischi e oppurtunità

L'intelligenza artificiale può nel contempo, a seconda delle circostanze relative alla sua applicazione e al suo utilizzo specifico, comportare rischi e pregiudicare gli interessi pubblici e i diritti tutelati dalla legislazione dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale. Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di intelligenza artificiale per promuovere lo sviluppo, l'uso e l'adozione dell'intelligenza artificiale 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, come riconosciuti e tutelati dal diritto dell'Unione. Per conseguire tale obiettivo,

è opportuno stabilire regole che disciplinino l'immissione sul mercato e la messa in servizio di determinati sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi. Stabilendo tali regole, si contribuisce all'obiettivo dell'Unione di essere un leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica, come affermato dal Consiglio europeo[26], e garantisce la tutela dei principi etici, come specificamente richiesto dal Parlamento europeo[27]. In tale prospettiva argomentativa, la nozione di sistema di IA dovrebbe essere definita in maniera chiara al fine di garantire la certezza del diritto, prevedendo nel contempo la flessibilità necessaria per agevolare i futuri sviluppi tecnologici. La definizione dovrebbe essere basata sulle principali caratteristiche funzionali del software, in particolare sulla capacità, per una determinata serie di obiettivi definiti dall'uomo, di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano l'ambiente con cui il sistema interagisce, tanto in una dimensione fisica quanto in una dimensione digitale. I sistemi di IA possono essere progettati per funzionare con livelli di autonomia variabili e per essere utilizzati come elementi indipendenti o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto o assista la funzionalità del prodotto senza esservi incorporato. La definizione di sistema di IA dovrebbe essere completata da un elenco di tecniche e approcci specifici utilizzati per il suo sviluppo, che dovrebbe essere tenuto aggiornato alla luce degli sviluppi di mercato e tecnologici mediante l'adozione da parte della Commissione di atti delegati volti a modificare tale elenco. La refilessione tecnica può essere arricchita dalla nozione di dati biometrici interpretata in modo coerente con la nozione di dati biometrici di cui all'articolo 4, punto 14), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[28], all'articolo 3, punto 18), del regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio[29] e all'articolo 3, punto 13), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[30]. Altro aspetto di particolare interesse giuridico è la nozione di sistema di identificazione biometrica remota utilizzata nell'idea regolamentare, quale sistema di IA destinato all'identificazione a distanza

---

[26] Consiglio europeo, riunione straordinaria del Consiglio europeo (1 e 2 ottobre 2020) – Conclusioni, EUCO 13/20, 2020, pag. 6.

[27] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

[28] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

[29] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

[30] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie) *(GU L 119 del 4.5.2016, pag. 89)*.

di persone fisiche mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, e senza sapere in anticipo se la persona interessata sarà presente e può essere identificata, a prescindere dalla tecnologia, dai processi o dai tipi specifici di dati biometrici utilizzati. Tenuto conto delle loro diverse caratteristiche e modalità di utilizzo, nonché dei diversi rischi connessi, è opportuno operare una distinzione tra sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori". Nel caso dei sistemi "in tempo reale", il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono tutti istantaneamente, quasi istantaneamente o in ogni caso senza ritardi significativi. A tale riguardo, non dovrebbe essere possibile eludere le regole per quanto attiene all'uso "in tempo reale" dei sistemi di IA in questione prevedendo ritardi minimi. I sistemi "in tempo reale" comportano l'uso di materiale "dal vivo" o "quasi dal vivo" (ad esempio filmati) generato da una telecamera o da un altro dispositivo con funzionalità analoghe. Nel caso dei sistemi di identificazione "a posteriori", invece, i dati biometrici sono già stati rilevati e il confronto e l'identificazione avvengono solo con un ritardo significativo. Altro delicato aspetto giuridico concerne la nozione di spazio accessibile al pubblico intesa come riferita a qualsiasi luogo fisico accessibile al pubblico, a prescindere dal fatto che il luogo in questione sia di proprietà pubblica o privata. La nozione non contempla pertanto i luoghi di natura privata, quali abitazioni, circoli privati, uffici, magazzini e fabbriche, che non sono di norma accessibili a terzi, comprese le autorità di contrasto, a meno che tali soggetti non siano stati specificamente invitati o autorizzati. Non sono del pari contemplati gli spazi online, dato che non sono luoghi fisici. Il semplice fatto che possano applicarsi determinate condizioni di accesso a uno spazio specifico, quali biglietti d'ingresso o limiti di età, non significa tuttavia che lo spazio non sia accessibile al pubblico ai sensi del presente regolamento. Di conseguenza, oltre agli spazi pubblici come le strade, le parti pertinenti degli edifici governativi e la maggior parte delle infrastrutture di trasporto, sono di norma accessibili al pubblico anche spazi quali cinema, teatri, negozi e centri commerciali. L'accessibilità di un determinato spazio al pubblico dovrebbe tuttavia essere determinata caso per caso, tenendo conto delle specificità della singola situazione presa in esame. Nella complessità dell' analisi giuridica è possibile considerare il c.d. diritto di libertà legato all' IA. Al fine di garantire condizioni di parità e una protezione efficace dei diritti e delle libertà delle persone in tutta l'Unione, è opportuno che le regole stabilite nell' argomento de quo si applichino ai fornitori di sistemi di IA in modo non discriminatorio, a prescindere dal fatto che siano stabiliti nell'Unione o in un paese terzo, e agli utenti dei sistemi di IA stabiliti nell'Unione. Alla luce della loro natura di sistemi digitali, è opportuno che determinati sistemi di IA rientrino nell'ambito di applicazione del presente regolamento anche quando non sono immessi sul mercato, né messi in servizio, né utilizzati nell'Unione. È il caso, ad esempio, di un operatore stabilito nell'Unione che appalta alcuni servizi a un operatore stabilito al di fuori

dell'Unione in relazione a un'attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio e i cui effetti avrebbero un impatto sulle persone fisiche che si trovano nell'Unione. In tali circostanze il sistema di IA utilizzato dall'operatore al di fuori dell'Unione potrebbe trattare dati raccolti nell'Unione e da lì trasferiti, nel rispetto della legge, e fornire all'operatore appaltante nell'Unione l'output di tale sistema di IA risultante da tale trattamento, senza che tale sistema di IA sia immesso sul mercato, messo in servizio o utilizzato nell'Unione. Al fine di impedire l'elusione del presente regolamento e di garantire una protezione efficace delle persone fisiche che si trovano nell'Unione, è opportuno che il presente regolamento si applichi anche ai fornitori e agli utenti di sistemi di IA stabiliti in un paese terzo, nella misura in cui l'output prodotto da tali sistemi è utilizzato nell'Unione. Cionondimeno, per tener conto degli accordi vigenti e delle esigenze particolari per la cooperazione con partner stranieri con cui sono scambiate informazioni e elementi probatori, il testo della nroamtiva non dovrebbe applicarsi alle autorità pubbliche di un paese terzo e alle organizzazioni internazionali che agiscono nel quadro di accordi internazionali conclusi a livello nazionale o europeo per la cooperazione delle autorità giudiziarie e di contrasto con l'Unione o con i suoi Stati membri. Tali accordi sono stati conclusi bilateralmente tra Stati membri e paesi terzi o tra l'Unione europea, Europol e altre agenzie dell'UE e paesi terzi e organizzazioni internazionali. Gli analisiti della Commisione evidenziano l'opportunità che tali normative si applichino alle istituzioni, agli uffici, agli organismi e alle agenzie dell'Unione quando agiscono in qualità di fornitori o utenti di un sistema di IA. I sistemi di IA sviluppati o utilizzati esclusivamente per scopi militari dovrebbero essere esclusi dall'ambito di applicazione nel caso in cui tale uso rientri nell'ambito di competenza esclusiva della politica estera e di sicurezza comune disciplinata dal titolo V del trattato sull'Unione europea (TUE). In particolare non si dovrebbero pregiudicare le disposizioni relative alla responsabilità dei prestatori intermediari di cui alla direttiva 2000/31/CE del Parlamento europeo e del Consiglio. Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno a giudizio dei giuristi della Commissione, stabilire norme legislative comuni per tutti i sistemi di IA ad alto rischio. Tali norme dovrebbero essere coerenti con la Carta dei diritti fondamentali dell'Unione europea, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di intelligenza artificiale, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA. Infatti, l'intelligenza

artificiale presenta, accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e dovrebbero essere vietate poiché contraddicono i valori dell'Unione relativi al rispetto della dignità umana, della libertà, dell'uguaglianza, della democrazia e dello Stato di diritto e dei diritti fondamentali dell'Unione, compresi il diritto alla non discriminazione, alla protezione dei dati e della vita privata e i diritti dei minori. In tale direzione, è opportuno vietare l'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA intesi a distorcere il comportamento umano e che possono provocare danni fisici o psicologici. Tali sistemi di IA impiegano componenti subliminali che i singoli individui non sono in grado di percepire, oppure sfruttano le vulnerabilità di bambini e persone, dovute all'età o a incapacità fisiche o mentali. Si tratta di azioni compiute con l'intento di distorcere materialmente il comportamento di una persona, in un modo che provoca o può provocare un danno a tale persona o a un'altra. Tale intento non può essere presunto se la distorsione del comportamento umano è determinata da fattori esterni al sistema di IA, che sfuggono al controllo del fornitore o dell'utente. Tale divieto non dovrebbe ostacolare la ricerca per scopi legittimi in relazione a tali sistemi di IA, se tale ricerca non equivale a un uso del sistema di IA nelle relazioni uomo-macchina che espone le persone fisiche a danni e se tale ricerca è condotta conformemente a norme etiche riconosciute per la ricerca scientifica. Nelle riflessioni della Commissione emerge che i sistemi di IA che forniscono un punteggio sociale delle persone fisiche per finalità generali delle autorità pubbliche o di loro rappresentanti possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano l'affidabilità delle persone fisiche sulla base del loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note o previste. Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. **È pertanto opportuno vietare secondo la Commisione tali sistemi di IA.**

Il caso dell' identificazione biometrica

Particolarmente delicato è anche l'uso di sistemi di IA di identificazione biometrica remota "in tempo reale" delle persone fisiche in spazi accessibili al pubblico. Nel merito, il legislatore europeo a fini di attività di contrasto ritiene particolarmente invasivo dei diritti e delle libertà delle persone interessate, nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali. L'immediatezza dell'impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all'uso di tali sistemi che operano "in tempo reale" comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone oggetto di attività di contrasto. L'uso di tali sistemi a fini di attività di contrasto dovrebbe pertanto essere vietato, eccezion fatta **per tre situazioni elencate in modo esaustivo e definite rigorosamente, nelle quali l'uso è strettamente necessario per perseguire un interesse pubblico rilevante, la cui importanza prevale sui rischi**. Tali situazioni comprendono la ricerca di potenziali vittime di reato, compresi i minori scomparsi, determinate minacce per la vita o l'incolumità fisica delle persone fisiche o un attacco terroristico nonché il rilevamento, la localizzazione e l'identificazione degli autori o dei sospettati di reati di cui nella decisione quadro 2002/584/GAI del Consiglio[31] o l'azione penale nei loro confronti, se tali reati, quali definiti dalla legge dello Stato membro interessato, sono punibili in tale Stato membro con una pena o una misura di sicurezza privativa della libertà personale della durata massima di almeno tre anni. Tale soglia per la pena o la misura di sicurezza privativa della libertà personale in conformità al diritto nazionale contribuisce a garantire che il reato sia sufficientemente grave da giustificare potenzialmente l'uso di sistemi di identificazione biometrica remota "in tempo reale". Inoltre è probabile che, a livello pratico, alcuni dei 32 reati elencati della decisione quadro 2002/584/GAI del Consiglio risultino più pertinenti di altri, poiché il grado di necessità e proporzionalità del ricorso all'identificazione biometrica remota "in tempo reale" sarà prevedibilmente molto variabile per quanto concerne il perseguimento pratico del rilevamento, della localizzazione, dell'identificazione o dell'azione penale nei confronti di un autore o un sospettato dei vari reati elencati e con riguardo alle possibili differenze in termini di gravità, probabilità e portata del danno o delle eventuali conseguenze negative. Inoltre, al fine di garantire che tali sistemi siano utilizzati in modo responsabile e proporzionato, è altresì importante stabilire che, in ciascuna delle tre situazioni

[31] Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

elencate in modo esaustivo e definite rigorosamente, è opportuno tener conto di taluni elementi, in particolare per quanto riguarda la natura della situazione all'origine della richiesta e le conseguenze dell'uso per i diritti e le libertà di tutte le persone interessate, nonché le tutele e le condizioni previste per l'uso. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto dovrebbe inoltre essere subordinato a limiti di tempo e di spazio adeguati, con particolare riguardo a indicazioni o elementi probatori relativi a minacce, vittime o autori di reati. La banca dati di riferimento delle persone dovrebbe risultare adeguata per ogni caso d'uso in ciascuna delle tre situazioni di cui sopra. Specificamente, in tale dinamica di trattazione, è opportuno subordinare ogni uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a un'autorizzazione esplicita e specifica da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente di uno Stato membro. Tale autorizzazione dovrebbe, in linea di principio, essere ottenuta prima dell'uso, tranne in situazioni di urgenza debitamente giustificate, vale a dire le situazioni in cui la necessità di utilizzare i sistemi in questione è tale da far sì che sia effettivamente e oggettivamente impossibile ottenere un'autorizzazione prima di iniziare a utilizzare il sistema. In tali situazioni di urgenza, è opportuno limitare l'uso al minimo indispensabile e subordinarlo a tutele e condizioni adeguate, come stabilito dal diritto nazionale e specificato nel contesto di ogni singolo caso d'uso urgente dall'autorità di contrasto stessa. L'autorità di contrasto dovrebbe inoltre in tali situazioni tentare di ottenere nel minor tempo possibile un'autorizzazione, indicando contestualmente i motivi per cui non ha potuto richiederla prima. È altresì opportuno prevedere, nell'ambito del quadro esaustivo stabilito dal presente regolamento, che tale uso nel territorio di uno Stato membro in conformità al presente regolamento sia possibile solo nel caso e nella misura in cui lo Stato membro in questione abbia deciso di prevedere espressamente la possibilità di autorizzare tale uso nelle regole dettagliate del proprio diritto nazionale. Gli Stati membri restano di conseguenza liberi, a norma del presente regolamento, di non prevedere affatto tale possibilità o di prevederla soltanto per alcuni degli obiettivi idonei a giustificare l'uso autorizzato di cui nel presente regolamento.

Altro punto cruciale per delicatezza e rispetto dei diritti fondamentali della persona umana riguarda il c.d. trattamento dei dati biometrici. L'uso di sistemi di IA per l'identificazione biometrica remota "in tempo reale" di persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto comporta necessariamente il trattamento di tale tipologia di dati. Le regole vergate dai giuristi della Commissione che, fatte salve alcune eccezioni, vietano tale uso, e che sono basate sull'articolo 16 TFUE, **dovrebbero applicarsi come *lex specialis* rispetto alle regole sul trattamento dei dati biometrici di cui all'articolo 10 della direttiva**

(UE) 2016/680, disciplinando quindi in modo esaustivo tale uso e il trattamento dei dati biometrici interessati. L'uso e il trattamento di cui sopra dovrebbero pertanto essere possibili solo nella misura in cui siano compatibili con il quadro stabilito dal presente regolamento, senza che al di fuori di tale quadro sia prevista la possibilità, per le autorità competenti, quando agiscono a fini di attività di contrasto, di utilizzare tali sistemi e trattare tali dati in connessione con tali attività per i motivi di cui all'articolo 10 della direttiva (UE) 2016/680. In tale contesto, l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini diversi dalle attività di contrasto, anche da parte delle autorità competenti, non dovrebbe rientrare nel quadro specifico stabilito dalla normativa in rassegna in relazione a tale uso a fini di attività di contrasto. Qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica, diverso da quello connesso all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto disciplinato dal presente regolamento, compresi i casi in cui tali sistemi sono utilizzati dalle autorità competenti in spazi accessibili al pubblico per fini diversi dalle attività di contrasto, dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, dall'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 e dall'articolo 10 della direttiva (UE) 2016/680, a seconda dei casi.

La complessa interazione nelle aree merceologiche dell' IA: il mercato dei prodotti, l'offerta di servizi e e la tutela dei diritti

È opportuno che i sistemi di IA ad alto rischio siano immessi sul mercato dell'Unione o messi in servizio solo se soddisfano determinati requisiti obbligatori. Tali requisiti dovrebbero garantire che i sistemi di IA ad alto rischio disponibili nell'Unione o i cui output sono altrimenti utilizzati nell'Unione non presentino rischi inaccettabili per interessi pubblici importanti dell'Unione, come riconosciuti e tutelati dal diritto dell'Unione. È opportuno limitare i sistemi di IA identificati come ad alto rischio a quelli che hanno un impatto nocivo significativo sulla salute, la sicurezza e i diritti fondamentali delle persone nell'Unione, e tale limitazione riduce al minimo eventuali potenziali restrizioni al commercio internazionale. I sistemi di IA potrebbero avere ripercussioni negative per la salute e la sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei

prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati. **La portata dell'impatto negativo del sistema di IA sui diritti fondamentali protetti dalla Carta è di particolare rilevanza ai fini della classificazione di un sistema di IA tra quelli ad alto rischio. Tali diritti comprendono il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e la non discriminazione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione. Oltre a tali diritti, è importante sottolineare che i minori godono di diritti specifici sanciti dall'articolo 24 della Carta dell'UE e dalla Convenzione delle Nazioni Unite sui diritti del fanciullo (ulteriormente elaborati nell'osservazione generale n. 25 della Convenzione delle Nazioni Unite sui diritti del fanciullo per quanto riguarda l'ambiente digitale), che prevedono la necessità di tenere conto delle loro vulnerabilità e di fornire la protezione e l'assistenza necessarie al loro benessere. È altresì opportuno tenere in considerazione, nel valutare la gravità del danno che un sistema di IA può provocare, anche in relazione alla salute e alla sicurezza delle persone, il diritto fondamentale a un livello elevato di protezione dell'ambiente sancito dalla Carta e attuato nelle politiche dell'Unione.**

Per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto in questione è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, macchine, giocattoli, ascensori, apparecchi e sistemi di protezione destinati a

essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici e dispositivi medico-diagnostici in vitro. La classificazione di un sistema di IA come ad alto rischio a norma del presente regolamento non dovrebbe necessariamente significare che il prodotto il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia considerato "ad alto rischio" in base ai criteri stabiliti nella pertinente normativa di armonizzazione dell'Unione che si applica al prodotto. Ciò vale in particolare per il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio[32] e per il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio[33], in cui è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio. Per quanto riguarda i sistemi di IA indipendenti, ossia i sistemi di IA ad alto rischio diversi da quelli che sono componenti di sicurezza di prodotti o che sono essi stessi prodotti, è opportuno classificarli come ad alto rischio se, alla luce della loro finalità prevista, presentano un alto rischio di pregiudicare la salute e la sicurezza o i diritti fondamentali delle persone, tenendo conto sia della gravità del possibile danno sia della probabilità che si verifichi, e sono utilizzati in una serie di settori specificamente predefiniti. L'identificazione di tali sistemi si basa sulla stessa metodologia e sui medesimi criteri previsti anche per eventuali future modifiche dell'elenco dei sistemi di IA ad alto rischio. Le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori. Ciò diviene particolarmente importante quando si trattano aspetti quali età, etnia, sesso o disabilità. È pertanto opportuno classificare i sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori" come sistemi ad alto rischio. Alla luce dei rischi che comportano, entrambi i tipi di sistemi di identificazione biometrica remota dovrebbero essere soggetti a requisiti specifici in materia di capacità di registrazione e sorveglianza umana. Per quanto riguarda la gestione e il funzionamento delle infrastrutture critiche, è opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati come componenti di sicurezza ai fini della gestione del traffico stradale nonché della fornitura di acqua, gas, riscaldamento ed elettricità, in quanto un loro guasto o malfunzionamento può mettere a rischio la vita e la salute di un grande numero di persone e provocare perturbazioni significative del normale svolgimento delle attività sociali ed economiche. Diversamente, i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'assegnazione di persone agli istituti

[32] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

[33] Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

di istruzione e formazione professionale o per valutare le persone che svolgono prove come parte o presupposto della loro istruzione, dovrebbero essere considerati ad alto rischio in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione. Anche i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo, in particolare per l'assunzione e la selezione delle persone, per l'adozione di decisioni in materia di promozione e cessazione del rapporto di lavoro, nonché per l'assegnazione dei compiti, per il monitoraggio o la valutazione delle persone nei rapporti contrattuali legati al lavoro, dovrebbero essere classificati come sistemi ad alto rischio, in quanto tali sistemi possono avere un impatto significativo sul futuro di tali persone in termini di future prospettive di carriera e sostentamento. I pertinenti rapporti contrattuali legati al lavoro dovrebbero coinvolgere i dipendenti e le persone che forniscono servizi tramite piattaforme, come indicato nel programma di lavoro annuale della Commissione per il 2021. In linea di principio, tali persone non dovrebbero essere considerate utenti ai sensi del presente regolamento. **Durante tutto il processo di assunzione, nonché ai fini della valutazione e della promozione delle persone o del proseguimento dei rapporti contrattuali legati al lavoro, tali sistemi possono perpetuare modelli storici di discriminazione**, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale. **I sistemi di IA utilizzati per monitorare le prestazioni e il comportamento di tali persone possono inoltre incidere sui loro diritti in materia di protezione dei dati e vita privata.** Un altro settore in cui l'utilizzo dei sistemi di IA merita particolare attenzione è l'accesso ad alcuni prestazioni e servizi pubblici e servizi privati essenziali, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi. È in particolare opportuno classificare i sistemi di IA utilizzati per valutare il merito di credito o l'affidabilità creditizia delle persone fisiche come sistemi di IA ad alto rischio, in quanto determinano l'accesso di tali persone alle risorse finanziarie o a servizi essenziali quali l'alloggio, l'elettricità e i servizi di telecomunicazione. I sistemi di IA utilizzati a tal fine possono portare alla discriminazione di persone o gruppi e perpetuare modelli storici di discriminazione, ad esempio in base all'origine razziale o etnica, alle disabilità, all'età o all'orientamento sessuale, o dar vita a nuove forme di effetti discriminatori. In considerazione della portata molto limitata dell'impatto e delle alternative disponibili sul mercato, è opportuno esentare i sistemi di IA destinati alla valutazione dell'affidabilità creditizia e del

merito creditizio nei casi in cui sono messi in servizio da fornitori di piccole dimensioni per uso proprio. Le persone fisiche che chiedono o ricevono prestazioni e servizi di assistenza pubblica dalle autorità pubbliche sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità competenti. I sistemi di IA, se utilizzati per determinare se tali prestazioni e servizi dovrebbero essere negati, ridotti, revocati o recuperati dalle autorità, possono avere un impatto significativo sul sostentamento delle persone e violare i loro diritti fondamentali, quali il diritto alla protezione sociale, alla non discriminazione, alla dignità umana o a un ricorso effettivo. È pertanto opportuno classificare tali sistemi come sistemi ad alto rischio. In tale proiezione argomentativa il dato normativo in rassegna non dovrebbe ostacolare lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche. Infine, è opportuno classificare come ad alto rischio anche i sistemi di IA utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, in quanto prendono decisioni in situazioni molto critiche per la vita e la salute delle persone e per i loro beni. Le azioni delle autorità di contrasto che prevedono determinati usi dei sistemi di IA sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali garantiti nella Carta. In particolare, il sistema di IA, se non è addestrato con dati di elevata qualità, se non soddisfa requisiti adeguati in termini di accuratezza o robustezza, o se non è adeguatamente progettato e sottoposto a prova prima di essere immesso sul mercato o altrimenti messo in servizio, può individuare le persone in modo discriminatorio o altrimenti errato o ingiusto. Potrebbe inoltre essere ostacolato l'esercizio di importanti diritti procedurali fondamentali, quali il diritto a un ricorso effettivo e a un giudice imparziale, nonché i diritti della difesa e la presunzione di innocenza, in particolare nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati. È pertanto opportuno classificare come ad alto rischio una serie di sistemi di IA destinati a essere utilizzati nel contesto delle attività di contrasto, in cui l'accuratezza, l'affidabilità e la trasparenza risultano particolarmente importanti per evitare impatti negativi, mantenere la fiducia dei cittadini e garantire la responsabilità e mezzi di ricorso efficaci. In considerazione della natura delle attività in questione e dei rischi a esse connessi, tra tali sistemi di IA ad alto rischio è opportuno includere, in particolare, i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per valutazioni dei rischi individuali, come poligrafi e strumenti analoghi, oppure per rilevare lo stato emotivo delle persone fisiche, individuare "deep fake", valutare l'affidabilità degli elementi probatori nei procedimenti penali, prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle

persone fisiche, o valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso delle persone fisiche o dei gruppi, nonché ai fini della profilazione nel corso dell'indagine, dell'accertamento e del perseguimento di reati e dell'analisi criminale nei riguardi delle persone fisiche. I sistemi di IA specificamente destinati a essere utilizzati per procedimenti amministrativi dalle autorità fiscali e doganali non dovrebbero essere considerati sistemi di IA ad alto rischio utilizzati dalle autorità di contrasto a fini di prevenzione, accertamento, indagine e perseguimento di reati. I sistemi di IA utilizzati nella gestione della migrazione, dell'asilo e del controllo delle frontiere hanno effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dall'esito delle azioni delle autorità pubbliche competenti. L'accuratezza, la natura non discriminatoria e la trasparenza dei sistemi di IA utilizzati in tali contesti sono pertanto particolarmente importanti per garantire il rispetto dei diritti fondamentali delle persone interessate, in particolare i loro diritti alla libera circolazione, alla non discriminazione, alla protezione della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione. È pertanto opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti incaricate di compiti in materia di gestione della migrazione, dell'asilo e del controllo delle frontiere, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica, per valutare taluni rischi presentati da persone fisiche che entrano nel territorio di uno Stato membro o presentano domanda di visto o di asilo, per verificare l'autenticità dei pertinenti documenti delle persone fisiche, nonché per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami in relazione all'obiettivo di determinare l'ammissibilità delle persone fisiche che richiedono tale status. I sistemi di IA nel settore della gestione della migrazione, dell'asilo e dei controlli di frontiera dovrebbero essere conformi ai pertinenti requisiti procedurali stabiliti dalla direttiva 2013/32/UE del Parlamento europeo e del Consiglio[34], dal regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio[35] e da altre normative pertinenti. Appare importante considerare che alcuni sistemi di IA destinati all'amministrazione della giustizia e ai processi democratici dovrebbero essere classificati come sistemi ad alto rischio, in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale. È in particolare opportuno, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, classificare come ad alto rischio i sistemi di IA destinati ad

34 Direttiva 2013/32/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale (GU L 180 del 29.6.2013, pag. 60).

35 Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un Codice comunitario dei visti (codice dei visti) (GU L 243 del 15.9.2009, pag. 1).

assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti. Non è tuttavia opportuno estendere tale classificazione ai sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi o l'assegnazione delle risorse. Come sottolinea la Commissione, il fatto che un sistema di IA sia classificato come ad alto rischio non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia necessariamente lecito a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, ad esempio in materia di protezione dei dati personali, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità ai requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale. Il presente regolamento non dovrebbe essere inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali. Al fine di attenuare, per gli utenti e per le persone interessate, i rischi derivanti dai sistemi di IA ad alto rischio immessi o altrimenti messi in servizio sul mercato dell'Unione, è opportuno applicare determinati requisiti obbligatori, tenendo conto della finalità prevista dell'uso del sistema e conformemente al sistema di gestione dei rischi che deve essere stabilito dal fornitore. Tali requisiti dovrebbero applicarsi ai sistemi di IA ad alto rischio per quanto concerne la qualità dei set di dati utilizzati, la documentazione tecnica e la conservazione delle registrazioni, la trasparenza e la fornitura di informazioni agli utenti, la sorveglianza umana e la robustezza, l'accuratezza e la cibersicurezza. Tali requisiti sono necessari per attenuare efficacemente i rischi per la salute, la sicurezza e i diritti fondamentali, come applicabile alla luce della finalità prevista del sistema, e, non essendo ragionevolmente disponibili altre misure meno restrittive degli scambi, sono così evitate limitazioni ingiustificate del commercio.

Le delicate valutazioni della Commissione nella logica della sicurezza dei dati nell'UE

Un'elevata qualità dei dati è essenziale per le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come

previsto e in maniera sicura e che non diventi fonte di una discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessaria l'attuazione di adeguate pratiche di governance e gestione dei dati. I set di dati di addestramento, convalida e prova dovrebbero essere sufficientemente pertinenti, rappresentativi e privi di errori, nonché completi alla luce della finalità prevista del sistema. Dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. In particolare, i set di dati di addestramento, convalida e prova dovrebbero tenere conto, nella misura necessaria alla luce della finalità prevista, delle caratteristiche o degli elementi peculiari dello specifico contesto o ambito geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato. Al fine di proteggere i diritti di terzi dalla discriminazione che potrebbe derivare dalla distorsione nei sistemi di IA, è opportuno che i fornitori siano in grado di trattare anche categorie particolari di dati personali, come questione di rilevante interesse pubblico, al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio. Ai fini dello sviluppo di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli dell'innovazione digitale, le strutture di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei rispettivi settori di attività connessi al presente regolamento. Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA. Ad esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di intelligenza artificiale su tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale. Le autorità competenti interessate, comprese quelle settoriali, che forniscono o sostengono l'accesso ai dati, possono anche sostenere la fornitura di dati di alta qualità a fini di addestramento, convalida e prova dei sistemi di IA. Altro aspetto di analisi concerne la necessità di disporre di informazioni sulle modalità di sviluppo dei sistemi di IA ad alto rischio e sulle loro modalità di funzionamento durante tutto il ciclo di vita. Ciò è essenziale per verificare la conformità ai requisiti normativi. Occorre a tal fine conservare le registrazioni e disporre di una documentazione tecnica contenente le informazioni necessarie per valutare la conformità del sistema di IA ai requisiti pertinenti. Tali informazioni dovrebbero includere le caratteristiche, le capacità e i limiti generali del sistema, gli algoritmi,

i dati, l'addestramento, i processi di prova e di convalida utilizzati, nonché la documentazione sul pertinente sistema di gestione dei rischi. Certamenente è opportuno tenere aggiornata la documentazione tecnica. Per ovviare all'opacità che può rendere alcuni sistemi di IA incomprensibili o troppo complessi per le persone fisiche, è opportuno imporre un certo grado di trasparenza per i sistemi di IA ad alto rischio. Gli utenti dovrebbero poter interpretare gli output del sistema e utilizzarlo in modo adeguato. I sistemi di IA ad alto rischio dovrebbero pertanto essere corredati di documentazione e istruzioni per l'uso pertinenti, nonché di informazioni concise e chiare, anche in relazione, se del caso, ai possibili rischi in termini di diritti fondamentali e discriminazione. Inoltre, i sistemi di IA ad alto rischio dovrebbero essere progettati e sviluppati in modo da consentire alle persone fisiche di sorvegliarne il funzionamento. Il fornitore del sistema dovrebbe a tal fine individuare misure di sorveglianza umana adeguate prima dell'immissione del sistema sul mercato o della sua messa in servizio. Tali misure dovrebbero in particolare garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo. Le prestazioni dei sistemi di IA ad alto rischio dovrebbero essere coerenti durante tutto il loro ciclo di vita e tali sistemi dovrebbero garantire un livello adeguato di accuratezza, robustezza e cibersicurezza, conformemente allo stato dell'arte generalmente riconosciuto. È opportuno che i livelli di precisione e le pertinenti metriche di accuratezza siano comunicati agli utenti. La robustezza tecnica è un requisito fondamentale dei sistemi di IA ad alto rischio. Tali sistemi dovrebbero essere resilienti rispetto sia ai rischi connessi alle limitazioni del sistema sia alle azioni dolose che possono compromettere la sicurezza del sistema di IA e comportare comportamenti dannosi o altrimenti indesiderati. La mancata protezione da tali rischi potrebbe avere ripercussioni sulla sicurezza o incidere negativamente sui diritti fondamentali, ad esempio a causa della generazione da parte del sistema di IA di decisioni errate o di output sbagliati o distorti. In una valutazione integrale delle problematiche sottese all'elaborazione normativa del legislatore europeo è cruciale approfondire il macro tema della sicurezza informatica. La cibersicurezza svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza. Gli attacchi informatici contro i sistemi di IA possono far leva sulle risorse specifiche dell'IA, quali i set di dati di addestramento (ad esempio "avvelenamento dei dati", *data poisoning*) o i modelli addestrati (ad esempio "attacchi antagonisti", *adversarial attacks*), o sfruttare le vulnerabilità delle risorse digitali del sistema di IA o dell'infrastruttura TIC sottostante. Al fine di garantire un livello di cibersicurezza adeguato ai rischi, è pertanto

opportuno che i fornitori di sistemi di IA ad alto rischio adottino misure adeguate, anche tenendo debitamente conto dell'infrastruttura TIC sottostante. Dettagliatamente, nell'ambito della normativa di armonizzazione dell'Unione, è opportuno che le regole applicabili all'immissione sul mercato, alla messa in servizio e all'uso di sistemi di IA ad alto rischio siano stabilite conformemente al regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio[36] che pone norme in materia di accreditamento e vigilanza del mercato dei prodotti, alla decisione n. 768/2008/CE del Parlamento europeo e del Consiglio[37] relativa a un quadro comune per la commercializzazione dei prodotti e al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio[38] sulla vigilanza del mercato e sulla conformità dei prodotti ("nuovo quadro legislativo per la commercializzazione dei prodotti"). Nel merito, è opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema. È quindi opportuno che il fornitore istituisca un solido sistema di gestione della qualità, garantisca l'espletamento della procedura di valutazione della conformità richiesta, rediga la documentazione pertinente e istituisca un sistema robusto per il monitoraggio successivo all'immissione sul mercato. Le autorità pubbliche che mettono in servizio sistemi di IA ad alto rischio per uso proprio possono adottare e attuare le regole per il sistema di gestione della qualità nell'ambito del sistema di gestione della qualità adottato a livello nazionale o regionale, a seconda dei casi, tenendo conto delle specificità del settore come pure delle competenze e dell'organizzazione dell'autorità pubblica in questione. Qualora un sistema di IA ad alto rischio che è un componente di sicurezza di un prodotto disciplinato da una pertinente normativa settoriale del nuovo quadro legislativo non fosse immesso sul mercato o messo in servizio separatamente dal prodotto, il fabbricante del prodotto finale quale definito nella pertinente normativa del nuovo quadro legislativo dovrebbe adempiere gli obblighi del fornitore stabiliti nel presente regolamento e, in particolare, garantire che il sistema di IA integrato nel prodotto finale soddisfi i requisiti del legislatore europeo. Inoltre, al fine di consentire l'applicazione del presente regolamento e di creare condizioni di parità per gli operatori, e tenendo conto delle diverse forme di messa a disposizione di prodotti digitali, è importante garantire che, in qualsiasi circostanza, una persona stabilita nell'Unione possa fornire alle autorità tutte le informazioni necessarie sulla conformità di un sistema di IA.

[36] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

[37] Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

[38] Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011 (GU L 169 del 25.6.2019, pag. 1).

Pertanto, prima di mettere a disposizione i propri sistemi di IA nell'Unione, nel caso in cui non possa essere identificato un importatore, i fornitori stabiliti al di fuori dell'Unione dovrebbero nominare, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

In linea con i principi del nuovo quadro legislativo, è opportuno stabilire obblighi specifici per gli operatori economici pertinenti, quali importatori e distributori, al fine di garantire la certezza del diritto e facilitare il rispetto della normativa da parte di tali operatori. Nel merito, in considerazione della natura dei sistemi di IA e dei possibili rischi per la sicurezza e i diritti fondamentali associati al loro utilizzo, anche per quanto riguarda la necessità di garantire un adeguato monitoraggio delle prestazioni di un sistema di IA in un contesto reale, è opportuno stabilire responsabilità specifiche per gli utenti. È in particolare opportuno che gli utenti usino i sistemi di IA ad alto rischio conformemente alle istruzioni per l'uso e che siano previsti alcuni altri obblighi in materia di monitoraggio del funzionamento dei sistemi di IA e conservazione delle registrazioni, a seconda dei casi. Specificamente, è opportuno prevedere che l'utente del sistema di IA sia la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo sotto la cui autorità è utilizzato il sistema di IA, salvo nel caso in cui il sistema sia utilizzato nel corso di un'attività personale non professionale. Alla luce della complessità della catena del valore dell'intelligenza artificiale, i terzi pertinenti, in particolare quelli coinvolti nella vendita e nella fornitura di software, strumenti e componenti software, modelli preaddestrati e dati, o i fornitori di servizi di rete, dovrebbero cooperare, a seconda dei casi, con i fornitori e con gli utenti per consentire loro di rispettare gli obblighi previsti dal presente regolamento e con le autorità competenti istituite a norma del presente regolamento. La conformità alle norme armonizzate quali definite nel regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio[39] dovrebbe essere un modo per i fornitori di dimostrare la conformità ai requisiti del presente regolamento. La Commissione potrebbe tuttavia adottare specifiche tecniche comuni nei settori in cui le norme armonizzate non esistono oppure sono insufficienti. Al fine di garantire un elevato livello di affidabilità dei sistemi di IA ad alto rischio, è opportuno sottoporre tali sistemi a una valutazione della conformità prima della loro immissione sul mercato o messa in servizio. Ai fini della valutazione della conformità da parte di terzi dei sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota delle persone, è opportuno che le autorità nazionali competenti designino organismi notificati a norma del presente regolamento, a condizione che tali organismi soddisfino una serie di requisiti, in particolare in materia di indipendenza, competenza e assenza di conflitti di interesse. In linea

[39] Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

con la nozione generalmente riconosciuta di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, è opportuno che un sistema di IA sia sottoposto a una nuova valutazione della conformità ogniqualvolta intervenga una modifica che possa incidere sulla conformità del sistema al presente regolamento oppure quando viene modificata la finalità prevista del sistema. È inoltre necessario, per quanto riguarda i sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio (ossia adattano automaticamente le modalità di svolgimento delle funzioni), prevedere regole atte a stabilire che le modifiche apportate all'algoritmo e alle sue prestazioni, predeterminate dal fornitore e valutate al momento della valutazione della conformità, non costituiscano una modifica sostanziale. I sistemi di IA ad alto rischio dovrebbero recare la marcatura CE per indicare la loro conformità al presente regolamento, in modo da poter circolare liberamente nel mercato interno. Gli Stati membri non dovrebbero ostacolare in maniera ingiustificata l'immissione sul mercato o la messa in servizio di sistemi di IA ad alto rischio che soddisfano i requisiti stabiliti nel presente regolamento e recano la marcatura CE. In tale scia descrittiva si palesa la disponibilità in tempi rapidi di tecnologie innovative che può, a determinate condizioni, essere fondamentale per la salute e la sicurezza delle persone e per la società nel suo insieme. È pertanto opportuno che, per motivi eccezionali di pubblica sicurezza o di tutela della vita e della salute delle persone fisiche nonché della proprietà industriale e commerciale, gli Stati membri possano autorizzare l'immissione sul mercato o la messa in servizio di sistemi di IA che non sono stati sottoposti a una valutazione della conformità. Nel dettaglio, al fine di agevolare il lavoro della Commissione e degli Stati membri nel settore dell'intelligenza artificiale e di aumentare la trasparenza nei confronti del pubblico, **è opportuno che i fornitori di sistemi di IA ad alto rischio diversi da quelli collegati a prodotti che rientrano nell'ambito di applicazione della pertinente normativa di armonizzazione dell'Unione vigente siano tenuti a registrare il loro sistema di IA ad alto rischio in una banca dati dell'UE, che sarà istituita e gestita dalla Commissione**. **È opportuno che la Commissione sia la titolare del trattamento di tale banca dati conformemente al regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio**[40]. Al fine di garantire la piena funzionalità della banca dati, è opportuno che, al momento dell'attivazione, la procedura per l'istituzione della banca dati preveda l'elaborazione di specifiche funzionali da parte della Commissione e una relazione di audit indipendente. Alcuni sistemi di IA destinati all'interazione con persone fisiche o alla generazione di contenuti possono comportare rischi specifici di impersonificazione o inganno,

[40] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

a prescindere dal fatto che siano considerati ad alto rischio o no. L'uso di tali sistemi dovrebbe pertanto essere, in determinate circostanze, soggetto a specifici obblighi di trasparenza, fatti salvi i requisiti e gli obblighi per i sistemi di IA ad alto rischio. Le persone fisiche dovrebbero in particolare ricevere una notifica nel momento in cui interagiscono con un sistema di IA, a meno che tale interazione non risulti evidente dalle circostanze e dal contesto di utilizzo. È inoltre opportuno che le persone fisiche ricevano una notifica quando sono esposte a un sistema di riconoscimento delle emozioni o a un sistema di categorizzazione biometrica. Tali informazioni e notifiche dovrebbero essere fornite in formati accessibili alle persone con disabilità. Inoltre, gli utenti che utilizzano un sistema di IA per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a persone, luoghi o eventi esistenti e che potrebbero apparire falsamente autentici, dovrebbero rendere noto che il contenuto è stato creato o manipolato artificialmente etichettando come tali gli output dell'intelligenza artificiale e rivelandone l'origine artificiale.

L'IA nella dinamica vievente tra normazione e innoazione: verso il comitato europeo per l'intelligenza artificiale

L'intelligenza artificiale appartiene una famiglia di tecnologie in rapida evoluzione che richiede nuove forme di sorveglianza regolamentare e uno spazio sicuro per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi. Al fine di garantire un quadro giuridico favorevole all'innovazione, adeguato alle esigenze future e resiliente alle perturbazioni, **è opportuno incoraggiare le autorità nazionali competenti di uno o più Stati membri a istituire spazi di sperimentazione normativa in materia di intelligenza artificiale per agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio.** Nel merito, gli obiettivi degli spazi di sperimentazione normativa dovrebbero essere la promozione dell'innovazione in materia di IA, mediante la creazione di un ambiente controllato di sperimentazione e prova nella fase di sviluppo e pre-commercializzazione al fine di garantire la conformità dei sistemi di IA innovativi al presente regolamento e ad altre normative pertinenti dell'Unione e degli Stati membri, e il rafforzamento della certezza del diritto per gli innovatori e della sorveglianza e della comprensione da parte delle autorità competenti delle opportunità, dei rischi emergenti e degli

impatti dell'uso dell'IA, nonché l'accelerazione dell'accesso ai mercati, anche mediante l'eliminazione degli ostacoli per le piccole e medie imprese (PMI) e le start-up. Al fine di garantire un'attuazione uniforme in tutta l'Unione ed economie di scala, è opportuno stabilire regole comuni per l'attuazione degli spazi di sperimentazione normativa e un quadro per la cooperazione tra le autorità competenti coinvolte nel controllo degli spazi di sperimentazione. Il dato normativo sviluppato dalla Commissione è quindi la base giuridica per l'utilizzo dei dati personali raccolti per altre finalità ai fini dello sviluppo di determinati sistemi di IA di interesse pubblico nell'ambito dello spazio di sperimentazione normativa per l'IA, in linea con l'articolo 6, paragrafo 4, del regolamento (UE) 2016/679, e con l'articolo 6 del regolamento (UE) 2018/1725, e fatto salvo l'articolo 4, paragrafo 2, della direttiva (UE) 2016/680. I partecipanti allo spazio di sperimentazione dovrebbero fornire garanzie adeguate e cooperare con le autorità competenti, anche seguendo i loro orientamenti e agendo rapidamente e in buona fede per attenuare eventuali rischi elevati per la sicurezza e i diritti fondamentali che possono emergere durante lo sviluppo e la sperimentazione nello spazio sopraindicato. È opportuno che le autorità competenti, nel decidere se infliggere una sanzione amministrativa pecuniaria a norma dell'articolo 83, paragrafo 2, del regolamento 2016/679 e dell'articolo 57 della direttiva 2016/680, tengano conto della condotta dei partecipanti allo spazio di sperimentazione. Al fine di promuovere e proteggere l'innovazione, è importante che siano tenuti in particolare considerazione gli interessi dei fornitori di piccole dimensioni e degli utenti di sistemi di IA. È a tal fine opportuno che gli Stati membri sviluppino iniziative destinate a tali operatori, anche in materia di sensibilizzazione e comunicazione delle informazioni. È inoltre opportuno che gli organismi notificati, nel fissare le tariffe per la valutazione della conformità, tengano in considerazione gli interessi e le esigenze specifici dei fornitori di piccole dimensioni. Le spese di traduzione connesse alla documentazione obbligatoria e alla comunicazione con le autorità possono rappresentare un costo significativo per i fornitori e gli altri operatori, in particolare quelli di dimensioni ridotte. Gli Stati membri dovrebbero garantire, se possibile, che una delle lingue da essi indicate e accettate per la documentazione dei fornitori pertinenti e per la comunicazione con gli operatori sia una lingua ampiamente compresa dal maggior numero possibile di utenti transfrontalieri. Al fine di ridurre al minimo i rischi per l'attuazione derivanti dalla mancanza di conoscenze e competenze sul mercato, nonché per agevolare il rispetto, da parte dei fornitori e degli organismi notificati, degli obblighi loro imposti dal presente regolamento, è opportuno che la piattaforma di IA on demand, i poli europei dell'innovazione digitale e le strutture di prova e sperimentazione istituiti dalla Commissione e dagli Stati membri a livello nazionale o dell'UE contribuiscano, se possibile, all'attuazione del presente regolamento. Nell'ambito delle rispettive missioni e dei rispettivi settori di competenza essi possono fornire, in particolare,

sostegno tecnico e scientifico ai fornitori e agli organismi notificati. È opportuno che la Commissione agevoli, nella misura del possibile, l'accesso alle strutture di prova e sperimentazione di organismi, gruppi o laboratori istituiti o accreditati a norma di qualsiasi pertinente normativa di armonizzazione dell'Unione che assolvano compiti nel contesto della valutazione della conformità di prodotti o dispositivi contemplati da tale normativa di armonizzazione dell'Unione. Ciò vale in particolare per i gruppi di esperti, i laboratori specializzati e i laboratori di riferimento nel settore dei dispositivi medici a norma del regolamento (UE) 2017/745 e del regolamento (UE) 2017/746. **In tale ambito i tecnici della commissione aupicano l'istituzione di un comitato europeo per l'intelligenza artificiale**. **Il comitato dovrebbe essere responsabile di una serie di compiti consultivi, tra cui l'emanazione di pareri, raccomandazioni, consulenze o orientamenti su questioni relative all'attuazione di tutte le indicazioni normative rispostate in tale documento di introduzione, comprese le specifiche tecniche o le norme esistenti per quanto riguarda i requisiti stabiliti nel dato regolamentare e la fornitura di consulenza e assistenza alla Commissione su questioni specifiche connesse all'intelligenza artificiale.** Gli Stati membri svolgono un ruolo chiave nell'applicare del norme vigenti e nel garantirne il rispetto. A tale riguardo, è opportuno che ciascuno Stato membro designi una o più autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione deldato regolamentare. Al fine di incrementare l'efficienza organizzativa da parte degli Stati membri e di istituire un punto di contatto ufficiale nei confronti del pubblico e di altre controparti sia a livello di Stati membri sia a livello di Unione, è opportuno che in ciascuno Stato membro sia designata come autorità nazionale di controllo un'autorità nazionale. Al fine di garantire che i fornitori di sistemi di IA ad alto rischio possano tenere in considerazione l'esperienza sull'uso di sistemi di IA ad alto rischio per migliorare i loro sistemi e il processo di progettazione e sviluppo o possano adottare tempestivamente eventuali misure correttive, è opportuno che tutti i fornitori dispongano di un sistema di monitoraggio successivo all'immissione sul mercato. Tale sistema è altresì fondamentale per garantire che i possibili rischi derivanti dai sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio possano essere affrontati in modo più efficiente e tempestivo. I fornitori dovrebbero anche essere tenuti, in tale contesto, a predisporre un sistema per segnalare alle autorità competenti eventuali incidenti gravi o violazioni della normativa nazionale e dell'Unione che tutela i diritti fondamentali derivanti dall'uso dei loro sistemi di IA. Inoltre, al fine di garantire un'applicazione adeguata ed efficace dei requisiti e degli obblighi stabiliti dalla normativa europea vigente è opportuno che si applichi nella sua interezza il sistema di vigilanza del mercato e di conformità dei prodotti istituito dal regolamento (UE) 2019/1020. Ove necessario

per il loro mandato, è opportuno che le autorità o gli organismi pubblici nazionali che controllano l'applicazione della normativa dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità, abbiano altresì accesso alla documentazione creata a norma del presente regolamento. Appare importante evidenziare che la legislazione dell'Unione in materia di servizi finanziari comprende regole e requisiti in materia di governance interna e di gestione dei rischi che sono applicabili agli istituti finanziari regolamentati durante la fornitura di tali servizi, anche quando si avvalgono di sistemi di IA. Al fine di garantire la coerenza dell'applicazione e dell'attuazione degli obblighi previsti dalla normativa vigente e delle regole e dei requisiti pertinenti della normativa dell'Unione in materia di servizi finanziari, è opportuno che le autorità responsabili del controllo e dell'applicazione della normativa in materia di servizi finanziari, compresa, se del caso, la Banca centrale europea, siano designate come autorità competenti ai fini del controllo dell'attuazione del presente regolamento, anche in relazione alle attività di vigilanza del mercato, per quanto riguarda i sistemi di IA forniti o utilizzati da istituti finanziari regolamentati e sottoposti a vigilanza. Per migliorare ulteriormente la coerenza tra il presente regolamento e le regole applicabili agli enti creditizi disciplinati dalla direttiva 2013/36/UE del Parlamento europeo e del Consiglio[41], è altresì opportuno integrare negli obblighi e nelle procedure esistenti a norma di tale direttiva la procedura di valutazione della conformità e alcuni degli obblighi procedurali dei fornitori in materia di gestione dei rischi, monitoraggio successivo alla commercializzazione e documentazione. Al fine di evitare sovrapposizioni, è opportuno prevedere deroghe limitate anche in relazione al sistema di gestione della qualità dei fornitori e all'obbligo di monitoraggio imposto agli utenti dei sistemi di IA ad alto rischio nella misura in cui si applicano agli enti creditizi disciplinati dalla direttiva 2013/36/UE. Lo sviluppo di sistemi di IA diversi dai sistemi di IA ad alto rischio può portare a una più ampia adozione nell'Unione dell'intelligenza artificiale affidabile. I fornitori di sistemi di IA non ad alto rischio dovrebbero essere incoraggiati a creare codici di condotta volti a promuovere l'applicazione volontaria dei requisiti obbligatori applicabili ai sistemi di IA ad alto rischio. **I fornitori dovrebbero inoltre essere incoraggiati ad applicare su base volontaria requisiti supplementari relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità per le persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo di sistemi di IA e alla diversità dei gruppi che si occupano dello sviluppo.** La Commissione può elaborare iniziative, anche di natura settoriale, per agevolare la riduzione degli ostacoli tecnici che ostruiscono lo scambio

[41] Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

transfrontaliero di dati per lo sviluppo dell'IA, anche per quanto riguarda l'infrastruttura di accesso ai dati e l'interoperabilità semantica e tecnica dei diversi tipi di dati. Nel merito, nel pensiero del legislare europeo, i sistemi di IA collegati a prodotti che non sono ad alto rischio in conformità al presente regolamento e che pertanto non sono tenuti a rispettare i requisiti ivi stabiliti debbono comunque essere sicuri al momento dell'immissione sul mercato o della messa in servizio. Per contribuire a tale obiettivo, sarebbe opportuno applicare come rete di sicurezza la direttiva 2001/95/CE del Parlamento europeo e del Consiglio[42]. **Al fine di garantire una cooperazione affidabile e costruttiva delle autorità competenti a livello nazionale e dell'Unione, è opportuno che tutte le parti coinvolte nell'applicazione della normativa rispettino la riservatezza delle informazioni e dei dati ottenuti nell'assolvimento dei loro compiti**. Gli Stati membri dovrebbero adottare tutte le misure necessarie per assicurare l'attuazione delle disposizioni normative, anche stabilendo sanzioni effettive, proporzionate e dissuasive in caso di violazione. Per talune violazioni specifiche, è opportuno che gli Stati membri tengano conto dei margini e dei criteri stabiliti. Il Garante europeo della protezione dei dati dovrebbe disporre del potere di infliggere sanzioni pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento. Al fine di garantire che il quadro normativo possa essere adeguato ove necessario, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per modificare le tecniche e gli approcci di cui all'allegato I per definire i sistemi di IA, la normativa di armonizzazione dell'Unione elencata nell'allegato II, i sistemi di IA ad alto rischio elencati nell'allegato III, le disposizioni relative alla documentazione tecnica di cui all'allegato IV, il contenuto della dichiarazione di conformità UE di cui all'allegato V, le disposizioni relative alle procedure di valutazione della conformità di cui agli allegati VI e VII e le disposizioni che stabiliscono i sistemi di IA ad alto rischio cui dovrebbe applicarsi la procedura di valutazione della conformità sulla base della valutazione del sistema di gestione della qualità e della valutazione della documentazione tecnica. **È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016**[43]**. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle**

[42] Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti (GU L 11 del 15.1.2002, pag. 4).

[43] GU L 123 del 12.5.2016, pag. 1.

riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.