COMMISSIONE
EUROPEA

Bruxelles, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

1.1. Motivi e obiettivi della proposta

La presente relazione accompagna la proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale). Con il termine intelligenza artificiale (IA) 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. Tale azione 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.

Con la presente proposta si tiene fede all'impegno politico della presidente von der Leyen che, nei suoi orientamenti politici per la Commissione 2019-2024 "Un'Unione più ambiziosa"[1], ha annunciato che la Commissione avrebbe presentato una normativa per un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale. A seguito di tale annuncio la Commissione ha pubblicato il 19 febbraio 2020 il Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia[2]. 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. La presente proposta mira ad attuare il secondo obiettivo al fine di sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile. La proposta si basa sui valori e sui diritti 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 da un gran numero di questi ultimi, che ha espresso il proprio favore a un intervento normativo volto ad affrontare le sfide e le preoccupazioni sollevate dal crescente utilizzo dell'IA.

---

[1] https://op.europa.eu/it/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1.

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

La presente proposta risponde altresì alle richieste 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 ("sistemi di IA"), nel contesto del quale tanto i benefici quanto i rischi legati all'intelligenza artificiale siano adeguatamente affrontati a livello dell'Unione. Essa contribuisce all'obiettivo dell'Unione di essere un leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica, come dichiarato dal Consiglio europeo[3], e garantisce la tutela dei principi etici, come richiesto specificamente dal Parlamento europeo[4].

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"[5]. Nelle sue conclusioni del 2019 sul piano coordinato sullo sviluppo e l'utilizzo dell'intelligenza artificiale "Made in Europe"[6], il Consiglio ha inoltre posto l'accento sull'importanza di garantire il pieno rispetto dei diritti dei cittadini europei e ha esortato a rivedere la normativa pertinente in vigore con l'obiettivo di garantire che essa sia idonea allo scopo alla luce delle 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[7].

Nelle conclusioni più recenti del 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 garantirne la compatibilità con i diritti fondamentali e agevolare l'applicazione delle norme giuridiche[8].

Anche il Parlamento europeo ha intrapreso una quantità considerevole di attività nel settore dell'IA. Nell'ottobre del 2020 ha adottato una serie di risoluzioni concernenti l'IA, anche in relazione ad etica[9], responsabilità[10] e diritti d'autore[11]. Nel 2021 tali risoluzioni sono state seguite da risoluzioni sull'IA in ambito penale[12] nonché nell'istruzione, nella cultura e nel settore audiovisivo[13]. La risoluzione del Parlamento europeo concernente un quadro relativo

---

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

4 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)).

5 Consiglio europeo, *Riunione del Consiglio europeo (19 ottobre 2017) – Conclusioni* EUCO 14/17, 2017, pag. 8.

6 Consiglio dell'Unione Europea, *Intelligenza artificiale b) Conclusioni relative al piano coordinato sull'intelligenza artificiale - Adozione* 6177/19, 2019.

7 Consiglio europeo, *Riunione speciale del Consiglio europeo (1° e 2 ottobre 2020) – Conclusioni* EUCO 13/20, 2020.

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

9 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).

10 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).

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

12 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).

13 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

agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate 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 il testo di una proposta legislativa di regolamento sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'IA, della robotica e delle tecnologie correlate. Conformemente all'impegno politico assunto dalla presidente von der Leyen nei suoi orientamenti politici per quanto concerne le risoluzioni adottate dal Parlamento europeo ai sensi dell'articolo 225 TFUE, la presente proposta tiene conto della summenzionata risoluzione del Parlamento europeo nel pieno rispetto dei principi di proporzionalità e sussidiarietà, nonché di quelli dell'accordo "Legiferare meglio".

In tale contesto politico, la Commissione presenta il quadro normativo proposto 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.

Al fine di conseguire tali obiettivi la presente proposta presenta 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 di IA. La proposta definisce un quadro giuridico solido e flessibile. Da un lato, è completa e adeguata alle esigenze future per quanto concerne le sue scelte normative fondamentali, compresi i requisiti basati sui principi che i sistemi di IA dovrebbero soddisfare. Dall'altro, mette in atto 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 comprende meccanismi flessibili che fanno sì che esso possa essere adeguato dinamicamente all'evoluzione della tecnologia e all'emergere di nuove situazioni di preoccupazione.

La proposta fissa 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. Essa 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. La proposta 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

---

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.

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 o "deep fake".

Le regole proposte 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 proposte 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.

1.2. Coerenza con le disposizioni vigenti nel settore normativo interessato

La natura orizzontale della proposta 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.

È inoltre 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. La proposta non 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. La presente proposta 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. La presente proposta non pregiudica l'applicazione del diritto dell'Unione in materia di concorrenza.

Per quanto concerne i sistemi di IA ad alto rischio che sono componenti di sicurezza dei prodotti, la presente proposta sarà integrata 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 (ad esempio macchine, dispositivi medici, giocattoli), i requisiti per i sistemi di IA stabiliti nella presente proposta 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 della presente proposta, 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. La proposta di regolamento sulle macchine, adottata nella medesima data della presente proposta, riflette pienamente questo approccio. Per quanto concerne i sistemi di IA ad alto rischio collegati a prodotti soggetti all'applicazione della pertinente normativa del "vecchio approccio" (ad esempio aviazione, autovetture), la presente proposta non si applicherebbe direttamente.

Tuttavia i requisiti essenziali ex ante per i sistemi di IA ad alto rischio stabiliti nella presente proposta dovranno essere presi in considerazione al momento dell'adozione della pertinente normativa di esecuzione o delegata ai sensi di tali atti.

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 della presente proposta al fine di assicurare un'applicazione coerente degli obblighi previsti dalla presente proposta e dalla normativa 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 a norma della presente proposta sono integrati nelle procedure ai sensi della direttiva 2013/36/UE sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale[14].

La presente proposta è altresì coerente con la legislazione dell'Unione applicabile ai servizi, compresi i servizi di intermediazione regolati dalla direttiva sul commercio elettronico (direttiva 2000/31/CE)[15] e la recente proposta della Commissione per la legge sui servizi digitali[16].

In relazione ai sistemi di IA che sono componenti di sistemi informatici su larga scala nello spazio di libertà, sicurezza e giustizia gestiti dall'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), la proposta non si applicherà ai sistemi di IA immessi sul mercato o messi in servizio prima che sia trascorso un anno dalla data di applicazione del presente regolamento, fatto salvo il caso in cui la sostituzione o la modifica di tali atti giuridici comporti una modifica significativa della progettazione o della finalità prevista del sistema di IA o dei sistemi di IA interessati.

1.3. Coerenza con le altre normative dell'Unione

La proposta 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.

La proposta è inoltre coerente 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"[17]. Stabilisce un quadro coerente, efficace e

---

[14] 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).

[15] 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).

[16] 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).

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

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**[18].

Inoltre la promozione dell'innovazione basata sull'IA è strettamente legata all'**Atto sulla governance dei dati**[19]**,** alla **direttiva sull'apertura dei dati**[20] e ad altre iniziative nell'ambito della **strategia dell'UE per i dati**[21], che stabiliranno meccanismi e servizi affidabili per il riutilizzo, la condivisione e la messa in comune dei dati, essenziali per lo sviluppo di modelli di IA di alta qualità basati sui dati.

La proposta rafforza inoltre 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 affidabile che sia coerente 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.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

2.1. Base giuridica

La base giuridica della proposta è costituita innanzitutto dall'articolo 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.

La presente proposta costituisce una parte fondamentale della strategia dell'Unione per il mercato unico digitale. L'obiettivo principale della presente proposta 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: i) 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; ii) 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.

La presente proposta definisce 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. La presente

---

18 *Bussola per il digitale 2030: il modello europeo per il decennio digitale*.

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

20 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).

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

proposta contempla 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 la presente proposta contiene 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 basare il presente regolamento, per quanto concerne tali regole specifiche, sull'articolo 16 TFUE.

2.2. Sussidiarietà (per la competenza non esclusiva)

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 della presente proposta 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 della presente proposta 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.

2.3. Proporzionalità

La proposta si basa sui quadri giuridici esistenti ed è proporzionata e necessaria per il conseguimento dei suoi obiettivi dato che segue un approccio basato sul rischio e impone oneri normativi soltanto laddove un sistema di IA 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. Per i sistemi di IA ad alto rischio i requisiti di qualità elevata dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, precisione e robustezza sono strettamente necessari per attenuare i rischi per i diritti fondamentali e la sicurezza posti dall'IA e che non sono oggetto di altri quadri giuridici in vigore. 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. I costi sostenuti dagli operatori sono proporzionati agli obiettivi conseguiti e ai benefici economici e reputazionali che gli operatori possono aspettarsi dalla presente proposta.

2.4. Scelta dell'atto giuridico

La scelta di un regolamento come 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.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

3.1. Consultazione dei portatori di interessi

La presente proposta 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[22].

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).

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.

[22] Cfr. tutti i risultati della consultazione.

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 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.

3.2. Assunzione e uso di perizie

La proposta 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[23] i requisiti fondamentali stabiliti negli orientamenti etici dell'AI HLEG per un'IA affidabile[24], 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)[25] 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**[26], 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.

---

23 Commissione europea, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final.

24 Gruppo di esperti ad alto livello sull'intelligenza artificiale, *Orientamenti etici per un'IA affidabile*, 2019.

25 Gruppo di esperti ad alto livello sull'intelligenza artificiale, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 2020.

26 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.

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 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[27]. 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[28]. È stato altresì commissionato uno **studio esterno** destinato ad alimentare la valutazione d'impatto.

3.3. Valutazione d'impatto

In linea con la sua politica "Legiferare meglio", la Commissione ha condotto una valutazione d'impatto in relazione alla presente proposta, 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.

La Commissione ha esaminato diverse opzioni strategiche destinate al conseguimento dell'obiettivo generale della presente proposta, 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;
- **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 riguarderanno i dati, la documentazione e la tracciabilità, la fornitura di informazioni e la trasparenza, la

[27] 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*.

[28] Per informazioni dettagliate in merito a tutte le consultazioni svolte si rimanda all'allegato 2 della valutazione d'impatto.

sorveglianza umana nonché la robustezza e la precisione e saranno obbligatori per i sistemi di IA ad alto rischio. Le imprese che introducessero codici di condotta per altri sistemi di IA lo farebbero su base volontaria.

L'opzione prescelta è stata considerata 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 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.

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.

Imprese o autorità pubbliche che sviluppano o utilizzano applicazioni di IA che rappresentano un rischio alto per la sicurezza o i diritti fondamentali dei cittadini dovrebbero rispettare requisiti e obblighi specifici. Entro il 2025 il rispetto di tali requisiti comporterebbe costi compresi, circa, tra 6 000 EUR e 7 000 EUR per la fornitura di un sistema di IA medio ad alto rischio del valore di circa 170 000 EUR. Per gli utenti di IA andrebbe altresì considerato il costo annuale del tempo impiegato per assicurare la sorveglianza umana, ove opportuno, a seconda del caso d'uso. Secondo le stime, tale costo tale costo sarebbe compreso, circa, tra 5 000 EUR e 8 000 EUR l'anno. I costi di verifica potrebbero ammontare a ulteriori 3 000 EUR - 7 500 EUR per i fornitori di IA ad alto rischio. Le imprese o le autorità pubbliche che sviluppano o utilizzano una qualsiasi applicazione di IA non classificata come ad alto rischio sarebbero soggette soltanto ad obblighi minimi di informazione. Potrebbero tuttavia scegliere di riunirsi ad altri soggetti e adottare congiuntamente un codice di condotta per seguire requisiti adeguati e per assicurare che i loro sistemi di IA siano affidabili. In tal caso i costi sarebbero al massimo pari a quelli dei sistemi di IA ad alto rischio, ma molto probabilmente inferiori.

Gli impatti delle opzioni strategiche su diverse categorie di portatori di interessi (operatori economici/imprese; organismi di valutazione della conformità, organismi di normazione e altri enti pubblici; persone fisiche/cittadini; ricercatori) sono spiegati in dettaglio nell'allegato 3 della valutazione d'impatto a sostegno della presente proposta.

3.4. Efficienza normativa e semplificazione

La presente proposta stabilisce gli obblighi 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, la presente proposta creerà certezza del diritto e assicurerà l'assenza di ostacoli alla fornitura transfrontaliera di servizi e prodotti collegati all'IA. Per le imprese che utilizzano l'IA, promuoverà la fiducia tra i loro clienti, mentre per le amministrazioni

pubbliche nazionali la presente proposta promuoverà la fiducia del pubblico nell'utilizzo dell'IA e rafforzerà 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 prevedrà 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.

La presente proposta mira inoltre specificamente 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 (ad esempio su prodotti e servizi), il che apporterà ulteriore chiarezza e semplificherà l'applicazione delle nuove regole.

3.5. Diritti fondamentali

L'utilizzo dell'IA con le sue caratteristiche specifiche (ad esempio opacità, complessità, dipendenza dai dati, comportamento autonomo) può incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("la Carta"). La presente proposta 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, la presente proposta migliorerà e promuoverà la protezione dei diritti tutelati dalla Carta: il diritto alla dignità umana (articolo 1), al rispetto della vita privata e alla protezione dei dati di carattere personale (articoli 7 e 8), alla non discriminazione (articolo 21) e alla parità tra donne e uomini (articolo 23). Essa mira a prevenire un effetto dissuasivo sui diritti alla libertà di espressione (articolo 11) e alla libertà di riunione (articolo 12), 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 (articoli 47 e 48), così come il principio generale di buona amministrazione. La presente proposta 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 (articolo 31), un livello elevato di protezione dei consumatori (articolo 38), i diritti del minore (articolo 24) e l'inserimento delle persone con disabilità (articolo 26). Rilevante è anche il diritto a un livello elevato di tutela dell'ambiente e al miglioramento della sua qualità (articolo 37), 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.

La presente proposta impone alcune restrizioni alla libertà d'impresa (articolo 16) e alla libertà delle arti e delle scienze (articolo 13) 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 ("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 (articolo 17, paragrafo 2), 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.

4. INCIDENZA SUL BILANCIO

Gli Stati membri dovranno designare autorità di controllo incaricate di attuare i requisiti legislativi. La loro funzione di controllo potrebbe basarsi su accordi esistenti, ad esempio per quanto riguarda gli organismi di valutazione della conformità o la vigilanza del mercato, ma richiederebbe competenze tecnologiche e risorse umane e finanziarie sufficienti. A seconda della struttura preesistente in ciascuno Stato membro, ciò potrebbe rappresentare da 1 a 25 equivalenti a tempo pieno per Stato membro.

Una panoramica dettagliata dei costi in questione è riportata nella "scheda finanziaria" collegata alla presente proposta.

5. ALTRI ELEMENTI

5.1. Piani attuativi e modalità di monitoraggio, valutazione e informazione

Prevedere un solido meccanismo di monitoraggio e valutazione è fondamentale per assicurare che la presente proposta sia efficace nel conseguire i suoi obiettivi specifici. La Commissione sarà incaricata di monitorare gli effetti della proposta. Stabilirà un sistema di registrazione delle applicazioni di IA ad alto rischio indipendenti in una banca dati pubblica a livello dell'UE. Tale registrazione consentirà altresì alle autorità competenti, agli utenti e ad altre persone interessate di verificare se il sistema di IA ad alto rischio è conforme ai requisiti stabiliti nella presente proposta nonché di esercitare una sorveglianza rafforzata sui sistemi di IA che presentano un alto rischio per i diritti fondamentali. Al fine di alimentare tale banca dati, i fornitori di IA saranno tenuti a fornire informazioni significative sui loro sistemi e sulla valutazione della conformità condotta su tali sistemi.

I fornitori di IA saranno inoltre tenuti a informare le autorità nazionali competenti in merito a incidenti gravi o malfunzionamenti che costituiscono una violazione degli obblighi in materia di diritti fondamentali non appena ne vengono a conoscenza, nonché in merito a qualsiasi richiamo o ritiro di sistemi di IA dal mercato. Le autorità nazionali competenti indagheranno quindi sugli incidenti o sui malfunzionamenti, raccoglieranno tutte le informazioni necessarie e le trasmetteranno periodicamente alla Commissione con metadati adeguati. La Commissione integrerà tali informazioni sugli incidenti con un'analisi completa del mercato globale per l'IA.

La Commissione pubblicherà una relazione di valutazione e sul riesame del quadro proposto per l'IA cinque anni dopo la data in cui quest'ultimo diventa applicabile.

5.2. Illustrazione dettagliata delle singole disposizioni della proposta

5.2.1. AMBITO DI APPLICAZIONE E DEFINIZIONI (TITOLO I)

Il **titolo I** definisce l'oggetto del regolamento e l'ambito di applicazione delle nuove regole concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA. Stabilisce inoltre le definizioni utilizzate in tutto l'atto. La definizione di sistema di IA nel quadro giuridico mira ad essere il più possibile neutrale dal punto di vista tecnologico e

adeguata alle esigenze future, tenendo conto dei rapidi sviluppi tecnologici e di mercato relativi all'IA. Al fine di fornire la necessaria certezza del diritto, il titolo I è integrato dall'allegato I, contenente un elenco dettagliato di approcci e tecniche per lo sviluppo dell'IA che deve essere adattato dalla Commissione in linea con i nuovi sviluppi tecnologici. Anche i partecipanti chiave lungo l'intera catena del valore dell'IA sono chiaramente definiti, quali i fornitori e gli utenti di sistemi di IA, considerando tanto gli operatori pubblici quanto quelli privati in maniera da assicurare parità di condizioni.

5.2.2. PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE (TITOLO II)

Il **titolo II** stabilisce un elenco di pratiche di IA vietate. Il regolamento segue un approccio basato sul rischio, differenziando tra gli usi dell'IA che creano: i) un rischio inaccettabile; ii) un rischio alto; iii) un rischio basso o minimo. L'elenco delle pratiche vietate di cui al titolo II comprende tutti i sistemi di IA il cui uso è considerato inaccettabile in quanto contrario ai valori dell'Unione, ad esempio perché viola i diritti fondamentali. I divieti riguardano pratiche che presentano un elevato potenziale in termini di manipolazione delle persone attraverso tecniche subliminali, senza che tali persone ne siano consapevoli, oppure di sfruttamento delle vulnerabilità di specifici gruppi vulnerabili, quali i minori o le persone con disabilità, al fine di distorcerne materialmente il comportamento in maniera tale da provocare loro o a un'altra persona un danno psicologico o fisico. Altre pratiche manipolative o di sfruttamento che interessano gli adulti che potrebbero essere facilitate dai sistemi di IA potrebbero essere soggette alla normativa vigente in materia di protezione dei dati, tutela dei consumatori e servizi digitali, che garantisce che le persone fisiche siano adeguatamente informate e dispongano della libera scelta di non essere soggette a profilazione o ad altre pratiche che potrebbero influire sul loro comportamento. La proposta vieta altresì l'attribuzione di un punteggio sociale basato sull'IA per finalità generali da parte di autorità pubbliche. È infine vietato anche il ricorso a sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, fatta salva l'applicazione di talune eccezioni limitate.

5.2.3. SISTEMI DI IA AD ALTO RISCHIO (TITOLO III)

Il **titolo III** contiene regole specifiche per i sistemi di IA che creano un rischio alto per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche. In linea con un approccio basato sul rischio, tali sistemi di IA ad alto rischio sono consentiti sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e ad una valutazione della conformità ex ante. La classificazione di un sistema di IA come ad alto rischio si basa sulla sua finalità prevista, in linea con la normativa vigente dell'UE in materia di sicurezza dei prodotti. Di conseguenza la classificazione come ad alto rischio non dipende solo dalla funzione svolta dal sistema di IA, ma anche dalle finalità e modalità specifiche di utilizzo di tale sistema.

Il capo 1 del titolo III fissa le regole di classificazione e individua due categorie principali di sistemi di IA ad alto rischio:

- i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti a valutazione della conformità ex ante da parte di terzi;
- altri sistemi di IA indipendenti che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'allegato III.

Tale elenco di sistemi di IA ad alto rischio di cui all'allegato III contiene un numero limitato di sistemi di IA i cui rischi si sono già concretizzati o potrebbero concretizzarsi nel prossimo futuro. Al fine di assicurare che il regolamento possa essere adattato agli usi e alle applicazioni emergenti dell'intelligenza artificiale, la Commissione può ampliare l'elenco dei

sistemi di IA ad alto rischio utilizzati all'interno di alcuni settori predefiniti, applicando una serie di criteri e una metodologia di valutazione dei rischi.

Il capo 2 definisce i requisiti giuridici per i sistemi di IA ad alto rischio in relazione a dati e governance dei dati, documentazione e conservazione delle registrazioni, trasparenza e fornitura di informazioni agli utenti, sorveglianza umana, robustezza, accuratezza e sicurezza. I requisiti minimi proposti costituiscono già lo stato dell'arte per numerosi operatori diligenti e rappresentano il risultato di due anni di lavoro preparatorio, derivato dagli orientamenti etici del gruppo di esperti ad alto livello sull'intelligenza artificiale[29], guidato da più di 350 organizzazioni[30]. Tali requisiti sono altresì in gran parte coerenti con altre raccomandazioni e altri principi internazionali, circostanza questa che assicura che il quadro dell'IA proposto sia compatibile con quelli adottati dai partner commerciali internazionali dell'UE. Le soluzioni tecniche precise atte a conseguire la conformità a tali requisiti possono essere previste mediante norme o altre specifiche tecniche o altrimenti essere sviluppate in conformità alle conoscenze ingegneristiche o scientifiche generali, a discrezione del fornitore del sistema di IA. Tale flessibilità è particolarmente importante in quanto consente ai fornitori di sistemi di IA di scegliere il modo in cui soddisfare i requisiti che li riguardano, tenendo conto dello stato dell'arte e del progresso tecnologico e scientifico nel settore.

Il capo 3 definisce una serie chiara di obblighi orizzontali per i fornitori di sistemi di IA ad alto rischio. Obblighi proporzionati sono imposti anche a utenti e altri partecipanti lungo la catena del valore dell'IA (ad esempio importatori, distributori, rappresentanti autorizzati).

Il capo 4 definisce il quadro per gli organismi notificati che saranno coinvolti come terze parti indipendenti nelle procedure di valutazione della conformità, mentre il capo 5 spiega in dettaglio le procedure di valutazione della conformità da seguire per ciascun tipo di sistema di IA ad alto rischio. L'approccio di valutazione della conformità mira a ridurre al minimo l'onere per gli operatori economici e per gli organismi notificati, la cui capacità deve essere aumentata progressivamente nel corso del tempo. I sistemi di IA destinati a essere utilizzati come componenti di sicurezza di prodotti disciplinati conformemente al nuovo quadro normativo (ad esempio macchine, giocattoli, dispositivi medici, ecc.) saranno soggetti agli stessi meccanismi di conformità e applicazione ex ante ed ex post dei prodotti di cui sono un componente. La differenza fondamentale consiste nel fatto che i meccanismi ex ante ed ex post assicureranno la conformità non soltanto ai requisiti stabiliti dalla normativa settoriale, ma anche a quelli fissati dal presente regolamento.

Per quanto riguarda i sistemi di IA ad alto rischio indipendenti di cui all'allegato III, sarà istituito un nuovo sistema di conformità e applicazione. Tale scelta segue il modello della legislazione del nuovo quadro normativo attuata mediante verifiche di controllo interno da parte di fornitori, fatta eccezione per i sistemi di identificazione biometrica remota che sarebbero soggetti a una valutazione della conformità da parte di terzi. Una valutazione completa della conformità ex ante attraverso controlli interni, combinata con una forte applicazione ex post, potrebbe costituire una soluzione efficace e ragionevole per tali sistemi, considerato che l'intervento normativo è in fase iniziale e che il settore dell'IA è molto innovativo e soltanto ora si stanno maturando le competenze di audit. Una valutazione attraverso controlli interni per sistemi di IA ad alto rischio indipendenti richiederebbe una conformità ex ante piena, effettiva e adeguatamente documentata a tutti i requisiti del

[29] Gruppo di esperti ad alto livello sull'intelligenza artificiale, *Orientamenti etici per un'IA affidabile*, 2019.

[30] I requisiti sono stati inoltre approvati dalla Commissione nella sua comunicazione del 2019 sull'approccio antropocentrico all'IA.

regolamento e ai sistemi solidi di gestione della qualità e dei rischi e a un monitoraggio successivo all'immissione sul mercato. Dopo aver effettuato la pertinente valutazione della conformità, il fornitore dovrebbe registrare tali sistemi di IA ad alto rischio indipendenti in una banca dati dell'UE che sarà gestita dalla Commissione al fine di aumentare la trasparenza nei confronti del pubblico e la sorveglianza, nonché di rafforzare il controllo ex post da parte delle autorità competenti. Al contrario, per motivi di coerenza con la normativa vigente in materia di sicurezza dei prodotti, le valutazioni della conformità dei sistemi di IA che sono componenti di sicurezza di prodotti seguiranno un sistema che prevede procedure di valutazione della conformità ad opera di terzi già stabilito dalla normativa settoriale pertinente in materia di sicurezza dei prodotti. Saranno necessarie nuove rivalutazioni ex ante della conformità in caso di modifiche sostanziali ai sistemi di IA (e in particolare modifiche che vanno oltre quanto predeterminato dal fornitore nella sua documentazione tecnica e verificato al momento della valutazione della conformità ex ante).

5.2.4. OBBLIGHI DI TRASPARENZA PER DETERMINATI SISTEMI DI IA (TITOLO IV)

Il **titolo IV** si concentra su determinati sistemi di IA al fine di tenere conto dei rischi specifici di manipolazione che essi comportano. Gli obblighi di trasparenza si applicheranno ai sistemi che: i) interagiscono con gli esseri umani; ii) sono utilizzati per rilevare emozioni o stabilire un'associazione con categorie (sociali) sulla base di dati biometrici; oppure iii) generano o manipolano contenuti (*"deep fake"*). Quando interagiscono con un sistema di IA o le loro emozioni o caratteristiche vengono riconosciute attraverso mezzi automatizzati, le persone devono esserne informate. Se un sistema di IA viene utilizzato per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a contenuti autentici, dovrebbe essere previsto l'obbligo di rivelare che tali contenuti sono generati ricorrendo a mezzi automatizzati, fatte salve le eccezioni per finalità legittime (attività di contrasto, libertà di espressione). Ciò consente alle persone di compiere scelte informate o di compiere un passo indietro rispetto a una determinata situazione.

5.2.5. MISURE A SOSTEGNO DELL'INNOVAZIONE (TITOLO V)

Il **titolo V** contribuisce all'obiettivo di creare un quadro giuridico favorevole all'innovazione, adeguato alle esigenze future e resiliente alle perturbazioni. Di conseguenza incoraggia le autorità nazionali competenti a creare spazi di sperimentazione normativa e definisce un quadro di base in termini di governance, controllo e responsabilità. Gli spazi di sperimentazione normativa per l'IA creano un ambiente controllato per sottoporre a prova tecnologie innovative per un periodo di tempo limitato sulla base di un piano di prova concordato con le autorità competenti. Il titolo V contiene altresì misure per ridurre gli oneri normativi per le PMI e le start-up.

5.2.6. GOVERNANCE E ATTUAZIONE (TITOLI VI, VII E VII)

Il **titolo VI** istituisce i sistemi di governance a livello di Unione e nazionale. A livello di Unione, la proposta istituisce un comitato europeo per l'intelligenza artificiale (il "comitato"), costituito da rappresentanti degli Stati membri e della Commissione. Tale comitato faciliterà un'attuazione agevole, efficace e armonizzata del presente regolamento contribuendo all'efficacia della cooperazione tra le autorità nazionali di controllo e la Commissione nonché fornendo consulenza e competenze alla Commissione. Raccoglierà e condividerà inoltre le migliori pratiche tra gli Stati membri.

A livello nazionale, gli Stati membri dovranno designare una o più autorità nazionali competenti e, tra queste, l'autorità nazionale di controllo, al fine di controllare l'applicazione e l'attuazione del regolamento. Il Garante europeo della protezione dei dati agirà in qualità di

autorità competente per la vigilanza delle istituzioni, delle agenzie e degli organismi dell'Unione nei casi in cui essi rientrano nell'ambito di applicazione del presente regolamento.

Il **titolo VII** mira a facilitare il lavoro di monitoraggio della Commissione e delle autorità nazionali attraverso la creazione di una banca dati a livello dell'UE per sistemi di IA ad alto rischio indipendenti che presentano principalmente implicazioni in relazione ai diritti fondamentali. La banca dati sarà gestita dalla Commissione e alimentata con i dati messi a disposizione dai fornitori dei sistemi di IA, che saranno tenuti a registrare i propri sistemi prima di immetterli sul mercato o altrimenti metterli in servizio.

Il **titolo VIII** stabilisce gli obblighi in materia di monitoraggio e segnalazione per i fornitori di sistemi di IA per quanto riguarda il monitoraggio successivo all'immissione sul mercato e la segnalazione di incidenti e malfunzionamenti correlati all'IA nonché le indagini in merito. Le autorità di vigilanza del mercato controllerebbero anche il mercato e indagherebbero in merito al rispetto degli obblighi e dei requisiti per tutti i sistemi di IA ad alto rischio già immessi sul mercato. Le autorità di vigilanza del mercato avrebbero tutti i poteri di cui al regolamento (UE) 2019/1020 sulla vigilanza del mercato. L'applicazione ex post dovrebbe assicurare che, una volta che il sistema di IA è stato immesso sul mercato, le autorità pubbliche dispongano dei poteri e delle risorse per intervenire nel caso in cui i sistemi di IA generino rischi imprevisti, che richiedono un intervento rapido. Tali autorità monitoreranno inoltre il rispetto da parte degli operatori dei loro obblighi pertinenti a norma del presente regolamento. La proposta non prevede la creazione automatica di ulteriori organismi o autorità a livello di Stato membro. Gli Stati membri possono quindi nominare autorità settoriali esistenti (avvalendosi delle loro competenze) e a tali autorità sarebbero affidati anche i poteri per monitorare e applicare le disposizioni del presente regolamento.

Tutto ciò non pregiudica il sistema esistente e l'attribuzione di poteri di applicazione ex post degli obblighi in materia di diritti fondamentali negli Stati membri. Se necessario per il loro mandato, le autorità di controllo e contrasto esistenti avranno altresì il potere di richiedere tutta la documentazione conservata ai sensi del presente regolamento e di accedervi, nonché, ove necessario, di richiedere alle autorità di vigilanza del mercato di organizzare prove del sistema di IA ad alto rischio mediante mezzi tecnici.

5.2.7. CODICI DI CONDOTTA (TITOLO IX)

Il **titolo IX** istituisce un quadro per la creazione di codici di condotta che mira a incoraggiare i fornitori di sistemi di IA non ad alto rischio ad applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio (come stabilito nel titolo III). I fornitori di sistemi di IA non ad alto rischio possono creare e attuare i codici di condotta autonomamente. Tali codici possono altresì comprendere impegni volontari relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità da parte delle persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di IA, nonché alla diversità dei gruppi che si occupano dello sviluppo.

5.2.8. DISPOSIZIONI FINALI (TITOLI X, XI E XII)

Il **titolo X** sottolinea l'obbligo per tutte le parti di rispettare la riservatezza delle informazioni e dei dati e stabilisce le regole per lo scambio delle informazioni ottenute durante l'attuazione del regolamento. Il titolo X comprende altresì misure per assicurare l'efficace attuazione del regolamento mediante sanzioni efficaci, proporzionate e dissuasive in caso di violazione delle disposizioni.

Il **titolo XI** stabilisce le regole per l'esercizio della delega e delle competenze di esecuzione. La proposta conferisce alla Commissione la facoltà di adottare, se del caso, atti di esecuzione

con l'obiettivo di assicurare l'applicazione uniforme del regolamento o atti delegati per aggiornare o integrare gli elenchi di cui agli allegati da I a VII.

Il **titolo XII** contiene l'obbligo per la Commissione di valutare periodicamente la necessità di un aggiornamento dell'allegato III e di preparare relazioni periodiche di valutazione e sul riesame del regolamento. Stabilisce inoltre disposizioni finali, compreso un periodo transitorio differenziato per la data iniziale di applicabilità del regolamento al fine di facilitare la corretta attuazione da parte di tutte le parti interessate.

2021/0106 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare gli articoli 16 e 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[31],

visto il parere del Comitato delle regioni[32],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Lo scopo del presente regolamento 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 presente regolamento 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.

(2) I sistemi di intelligenza artificiale (sistemi di IA) 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 presente regolamento prevede regole specifiche sulla

[31] GU C […] del […], pag. […].
[32] GU C […] del […], pag. […].

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 presente regolamento, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE. Alla luce di tali regole specifiche e del ricorso all'articolo 16 TFUE, è opportuno consultare il comitato europeo per la protezione dei dati.

(3) 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.

(4) L'intelligenza artificiale può nel contempo, a seconda delle circostanze relative alla sua applicazione e al suo utilizzo specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti tutelati dalla legislazione dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale.

(5) 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, il presente regolamento 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[33], e garantisce la tutela dei principi etici, come specificamente richiesto dal Parlamento europeo[34].

(6) 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 (stand-alone) o come componenti di un

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

[34] 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)).

prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato). 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.

(7) La nozione di dati biometrici utilizzata nel presente regolamento è in linea e dovrebbe essere 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[35], all'articolo 3, punto 18), del regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio[36] e all'articolo 3, punto 13), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[37].

(8) È opportuno definire a livello funzionale la nozione di sistema di identificazione biometrica remota utilizzata nel presente regolamento, quale sistema di IA destinato all'identificazione a distanza 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 del presente regolamento 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. Si tratta di materiale, come immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati, che è stato generato prima che il sistema fosse usato in relazione alle persone fisiche interessate.

(9) Ai fini del presente regolamento la nozione di spazio accessibile al pubblico dovrebbe essere 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

---

35 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).

36 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).

37 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).

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.

(10) 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 dal presente regolamento 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.

(11) 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. Ciononostante, 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 presente regolamento 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.

(12) È altresì opportuno che il presente regolamento si applichi 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 del presente regolamento 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). Il presente regolamento non dovrebbe pregiudicare le disposizioni

relative alla responsabilità dei prestatori intermediari di cui alla direttiva 2000/31/CE del Parlamento europeo e del Consiglio [come modificata dalla legge sui servizi digitali].

(13) Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno 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 (la Carta), non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione.

(14) 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.

(15) 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.

(16) 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.

(17) 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 tali sistemi di IA.

(18) L'uso di sistemi di IA di identificazione biometrica remota "in tempo reale" delle persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto è ritenuto 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.

(19) 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[38] 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.

(20) Al fine di garantire che tali sistemi siano utilizzati in modo responsabile e proporzionato, è altresì importante stabilire che, in ciascuna delle tre situazioni 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.

(21) 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

[38] 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).

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.

(22) 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.

(23) 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 dati biometrici. Le regole del presente regolamento 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, il presente regolamento non è inteso a fornire la base giuridica per il trattamento dei dati personali a norma dell'articolo 8 della direttiva 2016/680. Tuttavia, 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 dal presente regolamento in relazione a tale uso a fini di attività di contrasto. Tale uso a fini diversi dalle attività di contrasto non dovrebbe pertanto essere subordinato all'obbligo di un'autorizzazione a norma del presente regolamento e delle regole dettagliate applicabili del diritto nazionale che possono darvi attuazione.

(24) 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.

(25) A norma dell'articolo 6 bis del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, l'Irlanda non è vincolata dalle regole stabilite all'articolo 5, paragrafo 1, lettera d), e paragrafi 2 e 3, del presente regolamento, adottate in base all'articolo 16 TFUE, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE, laddove l'Irlanda non sia vincolata da regole che disciplinano forme di cooperazione giudiziaria in materia penale o di cooperazione di polizia nell'ambito delle quali devono essere rispettate le disposizioni stabilite in base all'articolo 16 TFUE.

(26) A norma degli articoli 2 e 2 bis del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al TFUE, la Danimarca non è vincolata dalle regole stabilite all'articolo 5, paragrafo 1, lettera d), e paragrafi 2 e 3, del presente regolamento, adottate in base all'articolo 16 TFUE, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE, né è soggetta alla loro applicazione.

(27) 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.

(28) 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.

(29) Per quanto riguarda i sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti o sistemi o che sono essi stessi prodotti o sistemi che rientrano nell'ambito di applicazione del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio[39], del regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio[40], del regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio[41], della direttiva 2014/90/UE del Parlamento europeo e del Consiglio[42], della direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio[43], del regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio[44], del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio[45], e del regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio[46], è opportuno modificare i suddetti atti per garantire che, nell'adottare qualsiasi futuro atto delegato o di esecuzione pertinente sulla base di tali atti, la Commissione tenga conto, sulla base

---

39 Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

40 Regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1).

41 Regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio, del 15 gennaio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli (GU L 60 del 2.3.2013, pag. 52).

42 Direttiva 2014/90/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sull'equipaggiamento marittimo e che abroga la direttiva 96/98/CE del Consiglio (GU L 257 del 28.8.2014, pag. 146).

43 Direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, relativa all'interoperabilità del sistema ferroviario dell'Unione europea (GU L 138 del 26.5.2016, pag. 44).

44 Regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE (GU L 151 del 14.6.2018, pag. 1).

45 Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).

46 Regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010,(UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011,(UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012,(UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione (GU L 325 del 16.12.2019, pag. 1).

delle specificità tecniche e normative di ciascun settore e senza interferire con i vigenti meccanismi di governance, valutazione della conformità e applicazione e con le autorità da essi stabilite, dei requisiti obbligatori sanciti dal presente regolamento.

(30) 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.

(31) 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[47] e per il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio[48], in cui è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio.

(32) 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 indicati nel regolamento. 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.

(33) 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.

---

47 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).

48 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).

(34) 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.

(35) I sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'assegnazione di persone agli istituti 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.

(36) 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.

(37) 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. Cionondimeno, il presente regolamento 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.

(38) 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.

(39) 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 di cui al presente regolamento dovrebbero essere conformi ai pertinenti requisiti procedurali stabiliti dalla direttiva 2013/32/UE del Parlamento europeo e del Consiglio[49], dal regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio[50] e da altre normative pertinenti.

(40) 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 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.

(41) Il fatto che un sistema di IA sia classificato come ad alto rischio a norma del presente regolamento 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.

---

49 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).

50 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).

(42) 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.

(43) 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.

(44) 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.

(45) 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.

(46) 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 è essenziale per verificare la conformità ai requisiti di cui al presente regolamento. 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. È opportuno tenere aggiornata la documentazione tecnica.

(47) 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.

(48) 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.

(49) 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.

(50) 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 (ad esempio errori, guasti, incoerenze, situazioni impreviste) 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.

(51) 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.

(52) 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[51] 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[52] relativa a un quadro comune per la commercializzazione dei prodotti e al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio[53] sulla vigilanza del mercato e sulla conformità dei prodotti ("nuovo quadro legislativo per la commercializzazione dei prodotti").

(53) 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.

(54) È 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.

(55) 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 presente regolamento.

(56) 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. 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.

---

51 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).

52 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).

53 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).

(57) 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.

(58) 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.

(59) 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.

(60) 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.

(61) La normazione dovrebbe svolgere un ruolo fondamentale nel fornire soluzioni tecniche ai fornitori per garantire la conformità al presente regolamento. La conformità alle norme armonizzate quali definite nel regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio[54] 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.

(62) 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.

(63) Al fine di ridurre al minimo l'onere per gli operatori ed evitare eventuali duplicazioni, la conformità ai requisiti del presente regolamento dei sistemi di IA ad alto rischio collegati a prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione secondo l'approccio del nuovo quadro legislativo dovrebbe essere valutata nell'ambito della valutazione della conformità già prevista da tale normativa. L'applicabilità dei requisiti del presente regolamento non dovrebbe pertanto incidere sulla logica specifica, la metodologia o la struttura generale della valutazione della conformità a norma della pertinente normativa specifica del nuovo quadro legislativo. Tale approccio si riflette pienamente nell'interazione tra il presente regolamento e il

[54] 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).

[regolamento macchine]. Mentre i requisiti del presente regolamento fanno fronte ai rischi per la sicurezza dei sistemi di IA che assolvono funzioni di sicurezza nelle macchine, alcuni requisiti specifici del [regolamento macchine] garantiranno l'integrazione sicura del sistema di IA nella macchina nel suo complesso, in modo da non compromettere la sicurezza di quest'ultima. Il [regolamento macchine] applica la stessa definizione di sistema di IA di cui al presente regolamento.

(64) In considerazione della più ampia esperienza dei certificatori professionali pre-commercializzazione nel settore della sicurezza dei prodotti e della diversa natura dei rischi connessi, è opportuno limitare, almeno in una fase iniziale di applicazione del presente regolamento, l'ambito di applicazione della valutazione della conformità da parte di terzi ai sistemi di IA ad alto rischio diversi da quelli collegati ai prodotti. È pertanto opportuno che la valutazione della conformità di tali sistemi sia di norma effettuata dal fornitore sotto la propria responsabilità, con la sola eccezione dei sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota di persone, per i quali è opportuno prevedere il coinvolgimento di un organismo notificato nella valutazione della conformità, nella misura in cui tali sistemi non siano vietati.

(65) 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.

(66) In linea 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.

(67) 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.

(68) La disponibilità in tempi rapidi di tecnologie innovative 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.

(69) 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[55]. 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.

(70) Alcuni sistemi di IA destinati all'interazione con persone fisiche o alla generazione di contenuti possono comportare rischi specifici di impersonificazione o inganno, 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.

(71) L'intelligenza artificiale è 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.

(72) 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

[55] 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).

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 presente regolamento dovrebbe fornire 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.

(73) 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.

(74) 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.

(75) 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.

(76) Al fine di facilitare un'attuazione agevole, efficace e armonizzata del presente regolamento, è opportuno istituire 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 del presente regolamento, comprese le specifiche tecniche o le norme esistenti per quanto riguarda i requisiti stabiliti nel presente regolamento, e la fornitura di consulenza e assistenza alla Commissione su questioni specifiche connesse all'intelligenza artificiale.

(77) Gli Stati membri svolgono un ruolo chiave nell'applicare il presente regolamento 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 del presente regolamento. 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.

(78) 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.

(79) Al fine di garantire un'applicazione adeguata ed efficace dei requisiti e degli obblighi stabiliti dal presente regolamento, che costituisce la normativa di armonizzazione dell'Unione, 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.

(80) 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 dal presente regolamento 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[56], 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.

(81) Lo sviluppo di sistemi di IA diversi dai sistemi di IA ad alto rischio in conformità ai requisiti del presente regolamento 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 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.

(82) È importante che 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 siano comunque 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[57].

(83) 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 del presente regolamento rispettino la riservatezza delle informazioni e dei dati ottenuti nell'assolvimento dei loro compiti.

(84) Gli Stati membri dovrebbero adottare tutte le misure necessarie per assicurare l'attuazione delle disposizioni di cui al presente regolamento, 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 nel presente regolamento. 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.

---

[56] 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).

[57] 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).

(85) 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[58]. 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 riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(86) È opportuno attribuire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di esecuzione del presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[59].

(87) Poiché l'obiettivo del presente regolamento non può essere conseguito in misura sufficiente dagli Stati membri e, a motivo della portata o degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 TUE. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(88) Il presente regolamento dovrebbe applicarsi a decorrere dal... [*OP: inserire la data stabilita all'articolo 85*]. È tuttavia opportuno che l'infrastruttura relativa alla governance e al sistema di valutazione della conformità sia operativa prima di tale data, pertanto le disposizioni sugli organismi notificati e sulla struttura di governance dovrebbero applicarsi a decorrere dal... [*OP: inserire la data corrispondente a tre mesi dopo l'entrata in vigore del presente regolamento*]. Gli Stati membri dovrebbero inoltre stabilire e notificare alla Commissione la normativa relativa alle sanzioni, comprese le sanzioni amministrative pecuniarie, e garantire che essa sia attuata in modo corretto ed efficace entro la data di applicazione del presente regolamento. Le disposizioni relative alle sanzioni dovrebbero pertanto applicarsi a decorrere dal [*OP: inserire la data corrispondente a dodici mesi dopo l'entrata in vigore del presente regolamento*].

(89) Conformemente all'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati e hanno formulato il loro parere il [...],

---

58 GU L 123 del 12.5.2016, pag. 1.

59 Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I

DISPOSIZIONI GENERALI

Articolo 1
Oggetto

Il presente regolamento stabilisce:

a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale ("sistemi di IA") nell'Unione;

a) il divieto di determinate pratiche di intelligenza artificiale;

b) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi;

c) regole di trasparenza armonizzate per i sistemi di IA destinati a interagire con le persone fisiche, i sistemi di riconoscimento delle emozioni, i sistemi di categorizzazione biometrica e i sistemi di IA utilizzati per generare o manipolare immagini o contenuti audio o video;

d) regole in materia di monitoraggio e vigilanza del mercato.

Articolo 2
Ambito di applicazione

1. Il presente regolamento si applica:

a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un paese terzo;

b) agli utenti dei sistemi di IA situati nell'Unione;

c) ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, laddove l'output prodotto dal sistema sia utilizzato nell'Unione.

2. Solo l'articolo 84 del presente regolamento si applica ai sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti o sistemi, o che sono essi stessi prodotti o sistemi, che rientrano nell'ambito di applicazione dei seguenti atti:

a) regolamento (CE) n. 300/2008;

b) regolamento (UE) n. 167/2013;

c) regolamento (UE) n. 168/2013;

d) direttiva 2014/90/UE;

e) direttiva (UE) 2016/797;

f) regolamento (UE) 2018/858;

g) regolamento (UE) 2018/1139;

h) regolamento (UE) 2019/2144.

3. Il presente regolamento non si applica ai sistemi di IA sviluppati o usati per scopi esclusivamente militari.

4. Il presente regolamento non si applica alle autorità pubbliche di un paese terzo né alle organizzazioni internazionali che rientrano nell'ambito di applicazione del presente regolamento a norma del paragrafo 1, laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri.

5. Il presente regolamento non pregiudica l'applicazione delle disposizioni sulla responsabilità dei prestatori intermediari di cui al capo II, sezione IV, della direttiva 2000/31/CE del Parlamento europeo e del Consiglio[60] [*da sostituire con le corrispondenti disposizioni della legge sui servizi digitali*].

Articolo 3
Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) "sistema di intelligenza artificiale" (sistema di IA): un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono;

2) "fornitore": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o che fa sviluppare un sistema di IA al fine di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio, a titolo oneroso o gratuito;

3) "fornitore di piccole dimensioni": un fornitore che è una microimpresa o una piccola impresa ai sensi della raccomandazione 2003/361/CE della Commissione[61];

4) "utente": qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;

5) "rappresentante autorizzato": qualsiasi persona fisica o giuridica stabilita nell'Unione che ha ricevuto un mandato scritto da un fornitore di un sistema di IA al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento;

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

7) "distributore": qualsiasi persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione senza modificarne le proprietà;

---

60 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).

61 Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

8) "operatore": il fornitore, l'utente, il rappresentante autorizzato, l'importatore e il distributore;

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

10) "messa a disposizione sul mercato": qualsiasi fornitura di un sistema di IA per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito;

11) "messa in servizio": la fornitura di un sistema di IA direttamente all'utente per il primo uso o per uso proprio sul mercato dell'Unione per la finalità prevista;

12) "finalità prevista": l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;

13) "uso improprio ragionevolmente prevedibile": l'uso di un sistema di IA in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi ragionevolmente prevedibile;

14) "componente di sicurezza di un prodotto o di un sistema": un componente di un prodotto o di un sistema che svolge una funzione di sicurezza per tale prodotto o sistema o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni;

15) "istruzioni per l'uso": le informazioni comunicate dal fornitore per informare l'utente in particolare della finalità prevista e dell'uso corretto di un sistema di IA, compreso lo specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere utilizzato;

16) "richiamo di un sistema di IA": qualsiasi misura volta a ottenere la restituzione al fornitore di un sistema di IA messo a disposizione degli utenti;

17) "ritiro di un sistema di IA": qualsiasi misura volta a impedire la distribuzione, l'esposizione e l'offerta di un sistema di IA;

18) "prestazioni di un sistema di IA": la capacità di un sistema di IA di conseguire la finalità prevista;

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

20) "valutazione della conformità": la procedura atta a verificare se i requisiti di cui al titolo III, capo 2, del presente regolamento relativi a un sistema di IA sono stati soddisfatti;

21) "organismo di valutazione della conformità": un organismo che svolge per conto di terzi attività di valutazione della conformità, incluse prove, certificazioni e ispezioni;

22) "organismo notificato": un organismo di valutazione della conformità designato in conformità al presente regolamento e ad altre pertinenti normative di armonizzazione dell'Unione;

23) "modifica sostanziale": una modifica del sistema di IA a seguito della sua immissione sul mercato o messa in servizio che incide sulla conformità del sistema di

IA ai requisiti di cui al titolo III, capo 2, del presente regolamento o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato;

24) "marcatura CE di conformità" (marcatura CE): una marcatura mediante la quale un fornitore indica che un sistema di IA è conforme ai requisiti stabiliti al titolo III, capo 2, del presente regolamento e in altre normative applicabili dell'Unione che armonizzano le condizioni per la commercializzazione dei prodotti ("normativa di armonizzazione dell'Unione") e che ne prevedono l'apposizione;

25) "monitoraggio successivo all'immissione sul mercato": tutte le attività svolte dai fornitori di sistemi di IA al fine di raccogliere e analizzare in modo proattivo l'esperienza maturata tramite l'uso dei sistemi di IA che immettono sul mercato o che mettono in servizio, al fine di individuare eventuali necessità di immediate azioni correttive o preventive;

26) "autorità di vigilanza del mercato": l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2019/1020;

27) "norma armonizzata": la norma europea di cui all'articolo 2, punto 1, lettera c), del regolamento (UE) n. 1025/2012;

28) "specifiche comuni": un documento, diverso da una norma, contenente soluzioni tecniche che forniscono i mezzi per soddisfare determinati requisiti e obblighi stabiliti a norma del presente regolamento;

29) "dati di addestramento": i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere, compresi i pesi di una rete neurale;

30) "dati di convalida": i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine di evitare l'eccessivo adattamento ai dati di addestramento (*overfitting*), considerando che il set di dati di convalida può essere un set di dati distinto o essere costituito da una partizione fissa o variabile del set di dati di addestramento;

31) "dati di prova": i dati utilizzati per fornire una valutazione indipendente del sistema di IA addestrato e convalidato al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;

32) "dati di input": i dati forniti a un sistema di IA o direttamente acquisiti dallo stesso, in base ai quali il sistema produce un output;

33) "dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

34) "sistema di riconoscimento delle emozioni": un sistema di IA finalizzato all'identificazione o alla deduzione di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;

35) "sistema di categorizzazione biometrica": un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, quali quelle basate sul sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, l'origine etnica o l'orientamento sessuale o politico;

36) "sistema di identificazione biometrica remota": un sistema di IA finalizzato all'identificazione a distanza 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 che l'utente del sistema di IA sappia in anticipo se la persona sarà presente e può essere identificata;

37) "sistema di identificazione biometrica remota "in tempo reale"": un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi. Sono incluse non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione della normativa;

38) "sistema di identificazione biometrica remota "a posteriori"": un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota "in tempo reale";

39) "spazio accessibile al pubblico": qualsiasi luogo fisico accessibile al pubblico, indipendentemente dall'applicabilità di determinate condizioni di accesso;

40) "autorità di contrasto":

   a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; o

   b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;

41) "attività di contrasto": le attività svolte dalle autorità di contrasto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;

42) "autorità nazionale di controllo": l'autorità alla quale uno Stato membro attribuisce la responsabilità di attuare e applicare il presente regolamento, di coordinare le attività affidate a tale Stato membro, di fungere da punto di contatto unico per la Commissione e di rappresentare lo Stato membro in seno al comitato europeo per l'intelligenza artificiale;

43) "autorità nazionale competente": l'autorità nazionale di controllo, l'autorità di notifica e l'autorità di vigilanza del mercato;

44) "incidente grave": qualsiasi incidente che, direttamente o indirettamente, causa, può aver causato o può causare una delle seguenti conseguenze:

   a) il decesso di una persona o gravi danni alla salute di una persona, alle cose o all'ambiente,

   b) una perturbazione grave e irreversibile della gestione e del funzionamento delle infrastrutture critiche.

Articolo 4
Modifiche dell'allegato I

Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di modificare l'elenco delle tecniche e degli approcci di cui all'allegato I, per

aggiornare tale elenco agli sviluppi tecnologici e di mercato sulla base di caratteristiche simili alle tecniche e agli approcci ivi elencati.

TITOLO II

PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE

Articolo 5

1. Sono vietate le pratiche di intelligenza artificiale seguenti:

   a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

   b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

   c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari:

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

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

   d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

      i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;

      ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;

      iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio[62],

[62] 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).

punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

2. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), tiene conto dei seguenti elementi:

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

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

   L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali.

3. Per quanto riguarda il paragrafo 1, lettera d), e il paragrafo 2, ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo durante o dopo l'uso.

   L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2.

4. Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, lettera d), e ai paragrafi 2 e 3. Tale Stato membro stabilisce nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, lettera d), compresi i reati di cui al punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto.

TITOLO III

SISTEMI DI IA AD ALTO RISCHIO

CAPO 1

CLASSIFICAZIONE DEI SISTEMI DI IA COME "AD ALTO RISCHIO"

Articolo 6
Regole di classificazione per i sistemi di IA ad alto rischio

1. A prescindere dal fatto che sia immesso sul mercato o messo in servizio in modo indipendente rispetto ai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

   a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;

   b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.

2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.

Articolo 7
Modifiche dell'allegato III

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di aggiornare l'elenco di cui all'allegato III aggiungendo sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

   a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati ai punti da 1 a 8 dell'allegato III;

   b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali, che è, in relazione alla sua gravità e alla probabilità che si verifichi, equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.

2. Nel valutare, ai fini del paragrafo 1, se un sistema di IA presenti un rischio di danno per la salute e la sicurezza o un rischio di impatto negativo sui diritti fondamentali equivalente o superiore al rischio di danno presentato dai sistemi di IA ad alto rischio di cui all'allegato III, la Commissione tiene conto dei criteri seguenti:

   a) la finalità prevista del sistema di IA;

   b) la misura in cui un sistema di IA è stato usato o è probabile che sarà usato;

   c) la misura in cui l'uso di un sistema di IA ha già causato un danno alla salute e alla sicurezza o un impatto negativo sui diritti fondamentali o ha suscitato gravi

preoccupazioni in relazione al verificarsi di tale danno o impatto negativo, come dimostrato da relazioni o da prove documentate presentate alle autorità nazionali competenti;

d) la portata potenziale di tale danno o di tale impatto negativo, in particolare in termini di intensità e capacità di incidere su una pluralità di persone;

e) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo dipendono dal risultato prodotto da un sistema di IA, in particolare perché per motivi pratici o giuridici non è ragionevolmente possibile sottrarsi a tale risultato;

f) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto all'utente di un sistema di IA, in particolare a causa di uno squilibrio di potere, conoscenza, situazione economica o sociale o età;

g) la misura in cui il risultato prodotto con un sistema di IA è facilmente reversibile, considerando non facilmente reversibili i risultati che hanno un impatto sulla salute o sulla sicurezza delle persone;

h) la misura in cui la legislazione vigente dell'Unione prevede:

i) misure di ricorso efficaci in relazione ai rischi presentati da un sistema di IA, ad esclusione delle richieste di risarcimento del danno;

ii) misure efficaci per prevenire o ridurre sostanzialmente tali rischi.

CAPO 2

REQUISITI PER I SISTEMI DI IA AD ALTO RISCHIO

Articolo 8
Conformità ai requisiti

1. I sistemi di IA ad alto rischio rispettano i requisiti stabiliti nel presente capo.

2. Nel garantire conformità a tali requisiti si tiene conto della finalità prevista del sistema di IA ad alto rischio e del sistema di gestione dei rischi di cui all'articolo 9.

Articolo 9
Sistema di gestione dei rischi

1. In relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi.

2. Il sistema di gestione dei rischi è costituito da un processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un aggiornamento costante e sistematico. Esso comprende le fasi seguenti:

a) identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema di IA ad alto rischio;

b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile;

c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 61;

d) adozione di adeguate misure di gestione dei rischi conformemente alle disposizioni dei paragrafi seguenti.

3. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), tengono in debita considerazione gli effetti e le possibili interazioni derivanti dall'applicazione combinata dei requisiti di cui al presente capo 2. Esse tengono conto dello stato dell'arte generalmente riconosciuto, anche come indicato nelle pertinenti norme armonizzate o specifiche comuni.

4. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che qualsiasi rischio residuo associato a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili, a condizione che il sistema di IA ad alto rischio sia usato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile. Tali rischi residui sono comunicati all'utente.

Nell'individuare le misure di gestione dei rischi più appropriate, occorre garantire quanto segue:

a) l'eliminazione o la riduzione dei rischi per quanto possibile attraverso un'adeguata progettazione e fabbricazione;

b) ove opportuno, l'attuazione di adeguate misure di attenuazione e di controllo in relazione ai rischi che non possono essere eliminati;

c) la fornitura di informazioni adeguate a norma dell'articolo 13, in particolare per quanto riguarda i rischi di cui al paragrafo 2, lettera b), del presente articolo e, ove opportuno, la formazione degli utenti.

Nell'eliminare o ridurre i rischi connessi all'uso del sistema di IA ad alto rischio, si tengono debitamente in considerazione le conoscenze tecniche, l'esperienza, l'istruzione e la formazione che ci si può aspettare dall'utente e l'ambiente in cui il sistema è destinato ad essere usato.

5. I sistemi di IA ad alto rischio sono sottoposti a prova al fine di individuare le misure di gestione dei rischi più appropriate. Le prove garantiscono che i sistemi di IA ad alto rischio funzionino in modo coerente per la finalità prevista e che siano conformi ai requisiti di cui al presente capo.

6. Le procedure di prova sono idonee a conseguire la finalità prevista del sistema di IA e non devono andare al di là di quanto necessario per conseguire tale finalità.

7. Le prove dei sistemi di IA ad alto rischio sono effettuate, a seconda dei casi, in un qualsiasi momento dell'intero processo di sviluppo e, in ogni caso, prima dell'immissione sul mercato o della messa in servizio. Le prove sono effettuate sulla base di metriche e soglie probabilistiche definite in via preliminare e adeguate alla finalità prevista perseguita dal sistema di IA ad alto rischio.

8. Nell'attuare il sistema di gestione dei rischi di cui ai paragrafi da 1 a 7, è prestata particolare attenzione all'eventualità che il sistema di IA ad alto rischio sia accessibile ai minori o abbia un impatto su di essi.

9. Per gli enti creditizi disciplinati dalla direttiva 2013/36/UE, gli aspetti descritti ai paragrafi da 1 a 8 fanno parte delle procedure di gestione dei rischi stabilite da tali enti a norma dell'articolo 74 di tale direttiva.

Articolo 10
Dati e governance dei dati

1. I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5.

2. I set di dati di addestramento, convalida e prova sono soggetti ad adeguate pratiche di governance e gestione dei dati. Tali pratiche riguardano in particolare:

   a) le scelte progettuali pertinenti;

   b) la raccolta dei dati;

   c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione;

   d) la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino;

   e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari;

   f) un esame atto a valutare le possibili distorsioni;

   g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o di una combinazione degli stessi.

4. I set di dati di addestramento, convalida e prova tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

5. Nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

6. Per lo sviluppo di sistemi di IA ad alto rischio diversi da quelli che utilizzano tecniche che prevedono l'addestramento di modelli si applicano adeguate pratiche di

gestione e governance dei dati, al fine di garantire che tali sistemi di IA ad alto rischio siano conformi al paragrafo 2.

Articolo 11
Documentazione tecnica

1. La documentazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio di tale sistema ed è tenuta aggiornata.

   La documentazione tecnica è redatta in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti di cui al presente capo e fornisce alle autorità nazionali competenti e agli organismi notificati tutte le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. Essa contiene almeno gli elementi di cui all'allegato IV.

2. Se è immesso sul mercato o messo in servizio un sistema di IA ad alto rischio connesso a un prodotto al quale si applicano gli atti giuridici elencati nell'allegato II, sezione A, si redige un'unica documentazione tecnica contenente tutte le informazioni di cui all'allegato IV e le informazioni necessarie a norma di tali atti giuridici.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di modificare l'allegato IV ove necessario per garantire che, alla luce del progresso tecnico, la documentazione tecnica fornisca tutte le informazioni necessarie per valutare la conformità del sistema ai requisiti di cui al presente capo.

Articolo 12
Conservazione delle registrazioni

1. I sistemi di IA ad alto rischio sono progettati e sviluppati con capacità che consentono la registrazione automatica degli eventi ("log") durante il loro funzionamento. Tali capacità di registrazione sono conformi a norme riconosciute o a specifiche comuni.

2. Le capacità di registrazione garantiscono un livello di tracciabilità del funzionamento del sistema di IA durante tutto il suo ciclo di vita adeguato alla finalità prevista del sistema.

3. Le capacità di registrazione consentono in particolare di monitorare il funzionamento del sistema di IA ad alto rischio per quanto riguarda il verificarsi di situazioni che possono far sì che il sistema di IA presenti un rischio ai sensi dell'articolo 65, paragrafo 1, o comportare una modifica sostanziale, e agevolano il monitoraggio successivo all'immissione sul mercato di cui all'articolo 61.

4. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le capacità di registrazione comprendono almeno i seguenti dati:

   a) la registrazione del periodo di ciascun utilizzo del sistema (data e ora di inizio e di fine di ciascun utilizzo);

   b) la banca dati di riferimento con cui il sistema ha verificato i dati di input;

   c) i dati di input per i quali la ricerca ha portato a una corrispondenza;

   d) l'identificativo delle persone fisiche che partecipano alla verifica dei risultati di cui all'articolo 14, paragrafo 5.

Articolo 13
Trasparenza e fornitura di informazioni agli utenti

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi dell'utente e del fornitore di cui al capo 3 del presente titolo.

2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso in un formato digitale o non digitale appropriato, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per gli utenti.

3. Le informazioni di cui al paragrafo 2 specificano:

   a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato;

   b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:

      i) la finalità prevista;

      ii) il livello di accuratezza, robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato e che ci si può attendere, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza;

      iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali;

      iv) le sue prestazioni per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato;

      v) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA;

   c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità;

   d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti;

   e) la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software.

Articolo 14
Sorveglianza umana

1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso.

2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare quando tali rischi persistono nonostante l'applicazione di altri requisiti di cui al presente capo.

3. La sorveglianza umana è garantita mediante almeno una delle seguenti misure:

   a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile;

   b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dall'utente.

4. Le misure di cui al paragrafo 3 consentono le seguenti azioni, a seconda delle circostanze, alle persone alle quali è affidata la sorveglianza umana:

   a) comprendere appieno le capacità e i limiti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, in modo che i segnali di anomalie, disfunzioni e prestazioni inattese possano essere individuati e affrontati quanto prima;

   b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare per i sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche;

   c) essere in grado di interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto in particolare delle caratteristiche del sistema e degli strumenti e dei metodi di interpretazione disponibili;

   d) essere in grado di decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio;

   e) essere in grado di intervenire sul funzionamento del sistema di IA ad alto rischio o di interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga.

5. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 sono tali da garantire che, inoltre, l'utente non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che essa non sia stata verificata e confermata da almeno due persone fisiche.

Articolo 15
Accuratezza, robustezza e cibersicurezza

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire, alla luce della loro finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.

2. I livelli di accuratezza e le pertinenti metriche di accuratezza dei sistemi di IA ad alto rischio sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema.

3. I sistemi di IA ad alto rischio sono resilienti per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi.

   La robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe.

   I sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da garantire che gli output potenzialmente distorti a causa dell'utilizzo di output come input per operazioni future ("circuiti di feedback", *feedback loops*) siano oggetto di adeguate misure di attenuazione.

4. I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso o le prestazioni sfruttando le vulnerabilità del sistema.

   Le soluzioni tecniche volte a garantire la cibersicurezza dei sistemi di IA ad alto rischio sono adeguate alle circostanze e ai rischi pertinenti.

   Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA includono, ove opportuno, misure volte a prevenire e controllare gli attacchi che cercano di manipolare il set di dati di addestramento ("avvelenamento dei dati", *data poisoning*), gli input progettati in modo da far sì che il modello commetta un errore ("esempi antagonistici", *adversarial examples*) o i difetti del modello.

CAPO 3

OBBLIGHI DEI FORNITORI E DEGLI UTENTI DEI SISTEMI DI IA AD ALTO RISCHIO E DI ALTRE PARTI

Articolo 16
Obblighi dei fornitori dei sistemi di IA ad alto rischio

I fornitori dei sistemi di IA ad alto rischio:

a) garantiscono che i loro sistemi di IA ad alto rischio siano conformi ai requisiti di cui al capo 2 del presente titolo;

b) dispongono di un sistema di gestione della qualità conforme all'articolo 17;

c) redigono la documentazione tecnica del sistema di IA ad alto rischio;

d) quando sono sotto il loro controllo, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio;

e) garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità prima della sua immissione sul mercato o messa in servizio;

f) rispettano gli obblighi di registrazione di cui all'articolo 51;

g) adottano le necessarie misure correttive, se il sistema di IA ad alto rischio non è conforme ai requisiti di cui al capo 2 del presente titolo;

h) informano le autorità nazionali competenti degli Stati membri in cui hanno messo a disposizione o messo in servizio il sistema di IA e, ove applicabile, l'organismo notificato in merito alla non conformità e alle eventuali misure correttive adottate;

i) appongono la marcatura CE sui loro sistemi di IA ad alto rischio per indicare la conformità al presente regolamento a norma dell'articolo 49;

j) su richiesta di un'autorità nazionale competente, dimostrano la conformità del sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo.

Articolo 17
Sistema di gestione della qualità

1. I fornitori di sistemi di IA ad alto rischio istituiscono di un sistema di gestione della qualità che garantisce la conformità al presente regolamento. Tale sistema è documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende almeno i seguenti aspetti:

   a) una strategia per la conformità normativa, compresa la conformità alle procedure di valutazione della conformità e alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio;

   b) le tecniche, le procedure e gli interventi sistematici da utilizzare per la progettazione, il controllo della progettazione e la verifica della progettazione del sistema di IA ad alto rischio;

   c) le tecniche, le procedure e gli interventi sistematici da utilizzare per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio;

   d) le procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA ad alto rischio e la frequenza con cui devono essere effettuate;

   e) le specifiche tecniche, comprese le norme, da applicare e, qualora le pertinenti norme armonizzate non siano applicate integralmente, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme ai requisiti di cui al capo 2 del presente titolo;

   f) i sistemi e le procedure per la gestione dei dati, compresa la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio;

   g) il sistema di gestione dei rischi di cui all'articolo 9;

   h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato a norma dell'articolo 61;

i) le procedure relative alla segnalazione di incidenti gravi e di malfunzionamenti a norma dell'articolo 62;

j) la gestione della comunicazione con le autorità nazionali competenti, le autorità competenti, comprese quelle settoriali, che forniscono o sostengono l'accesso ai dati, gli organismi notificati, altri operatori, clienti o altre parti interessate;

k) i sistemi e le procedure per la conservazione delle registrazioni e di tutte le informazioni e la documentazione pertinenti;

l) la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento;

m) un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale per quanto riguarda tutti gli aspetti elencati nel presente paragrafo.

2. L'attuazione degli aspetti di cui al paragrafo 1 è proporzionata alle dimensioni dell'organizzazione del fornitore.

3. Per i fornitori che sono enti creditizi disciplinati dalla direttiva 2013/36/UE, l'obbligo di istituire un sistema di gestione della qualità si considera soddisfatto se sono rispettate le regole sui dispositivi, i processi e i meccanismi di governance interna di cui all'articolo 74 di tale direttiva. In tale contesto, si tiene conto delle norme armonizzate di cui all'articolo 40 del presente regolamento.

Articolo 18
Obbligo di redigere la documentazione tecnica

1. I fornitori di sistemi di IA ad alto rischio redigono la documentazione tecnica di cui all'articolo 11 in conformità all'allegato IV.

2. I fornitori che sono enti creditizi disciplinati dalla direttiva 2013/36/UE mantengono la documentazione tecnica nell'ambito della documentazione riguardante i dispositivi, i processi e i meccanismi di governance interna di cui all'articolo 74 di tale direttiva.

Articolo 19
Valutazione della conformità

1. I fornitori dei sistemi di IA ad alto rischio garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità di cui all'articolo 43 prima della sua immissione sul mercato o messa in servizio. Se in seguito a tale valutazione i sistemi di IA risultano conformi ai requisiti di cui al capo 2 del presente titolo, i fornitori redigono una dichiarazione di conformità UE a norma dell'articolo 48 e appongono la marcatura CE di conformità a norma dell'articolo 49.

2. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettera b), immessi sul mercato o messi in servizio da fornitori che sono enti creditizi disciplinati dalla direttiva 2013/36/UE, la valutazione della conformità è effettuata nell'ambito della procedura di cui agli articoli da 97 a 101 di tale direttiva.

Articolo 20
Log generati automaticamente

1. I fornitori di sistemi di IA ad alto rischio conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo in virtù di un accordo contrattuale con l'utente o in forza di legge. I log sono conservati per un periodo adeguato alla luce della finalità prevista del sistema di IA ad alto rischio e degli obblighi giuridici applicabili a norma del diritto dell'Unione o nazionale.
2. I fornitori che sono enti creditizi disciplinati dalla direttiva 2013/36/UE mantengono i log generati automaticamente dai loro sistemi di IA ad alto rischio nell'ambito della documentazione di cui all'articolo 74 di tale direttiva.

Articolo 21
Misure correttive

I fornitori di sistemi di IA ad alto rischio che ritengono o hanno motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio non sia conforme al presente regolamento adottano immediatamente le misure correttive necessarie per rendere conforme tale dispositivo, ritirarlo o richiamarlo, a seconda dei casi. Essi informano di conseguenza i distributori del sistema di IA ad alto rischio in questione e, ove applicabile, il rappresentante autorizzato e gli importatori.

Articolo 22
Dovere di informazione

Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 65, paragrafo 1, e tale rischio sia noto al fornitore del sistema, tale fornitore informa immediatamente le autorità nazionali competenti degli Stati membri in cui ha messo a disposizione il sistema e, ove applicabile, l'organismo notificato che ha rilasciato un certificato per il sistema di IA ad alto rischio, in particolare in merito alla non conformità e alle eventuali misure correttive adottate.

Articolo 23
Cooperazione con le autorità competenti

I fornitori di sistemi di IA ad alto rischio, su richiesta di un'autorità nazionale competente, forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, in una lingua ufficiale dell'Unione stabilita dallo Stato membro interessato. Su richiesta motivata di un'autorità nazionale competente, i fornitori forniscono a tale autorità l'accesso ai log generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo in virtù di un accordo contrattuale con l'utente o in forza di legge.

Articolo 24
Obblighi dei fabbricanti di prodotti

Qualora un sistema di IA ad alto rischio collegato a prodotti ai quali si applicano gli atti giuridici elencati nell'allegato II, sezione A, sia immesso sul mercato o messo in servizio insieme al prodotto fabbricato conformemente a tali atti giuridici e con il nome del fabbricante del prodotto, quest'ultimo si assume la responsabilità della conformità del sistema

di IA al presente regolamento e ha, per quanto riguarda il sistema di IA, gli stessi obblighi imposti dal presente regolamento al fornitore.

Articolo 25
Rappresentanti autorizzati

1. Prima di mettere a disposizione i propri sistemi sul mercato dell'Unione, qualora non possa essere identificato un importatore, i fornitori stabiliti al di fuori dell'Unione nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

2. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fabbricante. Il mandato consente al rappresentante autorizzato di eseguire i seguenti compiti:

   a) tenere una copia della dichiarazione di conformità UE e della documentazione tecnica a disposizione delle autorità nazionali competenti e delle autorità nazionali di cui all'articolo 63, paragrafo 7;

   b) fornire all'autorità nazionale competente, su richiesta motivata, tutte le informazioni e la documentazione necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, compreso l'accesso ai log generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore in virtù di un accordo contrattuale con l'utente o in forza di legge;

   c) cooperare con le autorità nazionali competenti, su richiesta motivata, in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio.

Articolo 26
Obblighi degli importatori

1. Prima di immettere sul mercato un sistema di IA ad alto rischio, gli importatori di tale sistema garantiscono che:

   a) il fornitore di tale sistema di IA abbia eseguito l'appropriata procedura di valutazione della conformità;

   b) il fornitore abbia redatto la documentazione tecnica conformemente all'allegato IV;

   c) il sistema rechi la necessaria marcatura di conformità e sia accompagnato dalla documentazione e dalle istruzioni per l'uso necessarie.

2. Qualora ritenga o abbia motivo di ritenere che un sistema di IA ad alto rischio non sia conforme al presente regolamento, un importatore non lo immette sul mercato fino a quando tale sistema di IA non sia stato reso conforme. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 65, paragrafo 1, l'importatore ne informa il fornitore del sistema di IA e le autorità di vigilanza del mercato.

3. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o in un documento di accompagnamento.

4. Gli importatori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità ai requisiti di cui al capo 2 del presente titolo.

5. Gli importatori forniscono all'autorità nazionale competente, su richiesta motivata, tutte le informazioni e la documentazione necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo in una lingua che può essere compresa facilmente da tale autorità nazionale competente, compreso l'accesso ai log generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore in virtù di un accordo contrattuale con l'utente o in forza di legge. Essi cooperano inoltre con tali autorità in merito a qualsiasi azione intrapresa dall'autorità nazionale competente in relazione a tale sistema.

Articolo 27
Obblighi dei distributori

1. Prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che il sistema di IA ad alto rischio rechi la necessaria marcatura CE di conformità, che sia accompagnato dalla documentazione e dalle istruzioni per l'uso necessarie e che il fornitore e l'importatore del sistema, a seconda dei casi, abbiano rispettato gli obblighi di cui al presente regolamento.

2. Qualora ritenga o abbia motivo di ritenere che un sistema di IA ad alto rischio non sia conforme ai requisiti di cui al capo 2 del presente titolo, un distributore non lo mette a disposizione sul mercato fino a quando tale sistema di IA ad alto rischio non sia stato reso conforme a tali requisiti. Inoltre, qualora il sistema presenti un rischio ai sensi dell'articolo 65, paragrafo 1, il distributore ne informa il fornitore o l'importatore del sistema, a seconda dei casi.

3. I distributori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità del sistema ai requisiti di cui al capo 2 del presente titolo.

4. Un distributore che ritiene o ha motivo di ritenere che un sistema di IA ad alto rischio che ha messo a disposizione sul mercato non sia conforme ai requisiti di cui al capo 2 del presente titolo adotta le misure correttive necessarie per rendere tale sistema conforme a tali requisiti, ritirarlo o richiamarlo o garantisce che il fornitore, l'importatore o qualsiasi operatore pertinente, a seconda dei casi, adotti tali misure correttive. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 65, paragrafo 1, il distributore ne informa immediatamente le autorità nazionali competenti degli Stati membri in cui ha messo il prodotto a disposizione, fornendo in particolare informazioni precise sulla non conformità e sulle eventuali misure correttive adottate.

5. Su richiesta motivata di un'autorità nazionale competente, i distributori di sistemi di IA ad alto rischio forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità di un sistema ad alto rischio ai requisiti di cui al capo 2 del presente titolo. I distributori cooperano inoltre con tale autorità nazionale competente in merito a qualsiasi misura adottata da tale autorità.

Articolo 28
Obblighi di distributori, importatori, utenti e altri terzi

1. Qualsiasi distributore, importatore, utente o altro terzo è considerato un fornitore ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti:

   a) se immette sul mercato o mette in servizio un sistema di IA ad alto rischio con il loro nome o marchio;

   b) se modifica la finalità prevista di un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio;

   c) se apporta una modifica sostanziale al sistema di IA ad alto rischio.

2. Qualora si verifichino le circostanze di cui al paragrafo 1, lettera b) o c), il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA ad alto rischio non è più considerato un fornitore ai fini del presente regolamento.

Articolo 29
Obblighi degli utenti dei sistemi di IA ad alto rischio

1. Gli utenti di sistemi di IA ad alto rischio usano tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 2 e 5.

2. Gli obblighi di cui al paragrafo 1 lasciano impregiudicati gli altri obblighi degli utenti previsti dal diritto dell'Unione o nazionale e la discrezionalità dell'utente nell'organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore.

3. Fatto salvo il paragrafo 1, nella misura in cui esercita il controllo sui dati di input, l'utente garantisce che tali dati di input siano pertinenti alla luce della finalità prevista del sistema di IA ad alto rischio.

4. Gli utenti monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso. Se hanno motivo di ritenere che l'uso in conformità alle istruzioni per l'uso possa far sì che il sistema di IA presenti un rischio ai sensi dell'articolo 65, paragrafo 1, ne informano il fornitore o il distributore e sospendono l'uso del sistema. Essi informano inoltre il fornitore o il distributore qualora abbiano individuato un incidente grave o un malfunzionamento ai sensi dell'articolo 62 e interrompono l'uso del sistema di IA. Nel caso in cui l'utente non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 62.

   Per gli utenti che sono enti creditizi disciplinati dalla direttiva 2013/36/UE, l'obbligo di cui al primo comma si considera soddisfatto se sono rispettate le regole sui dispositivi, i processi e i meccanismi di governance interna di cui all'articolo 74 di tale direttiva.

5. Gli utenti di sistemi di IA ad alto rischio conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo. I log sono conservati per un periodo adeguato alla luce della finalità prevista del sistema di IA ad alto rischio e degli obblighi giuridici applicabili a norma del diritto dell'Unione o nazionale.

   Gli utenti che sono enti creditizi disciplinati dalla direttiva 2013/36/UE mantengono i log nell'ambito della documentazione riguardante i dispositivi, i processi e i meccanismi di governance interna di cui all'articolo 74 di tale direttiva.

6. Gli utenti di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, ove applicabile.

CAPO 4

AUTORITÀ DI NOTIFICA E ORGANISMI NOTIFICATI

Articolo 30
Autorità di notifica

1. Ciascuno Stato membro designa o istituisce un'autorità di notifica responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio.
2. Gli Stati membri possono designare come autorità di notifica un organismo nazionale di accreditamento di cui al regolamento (CE) n. 765/2008.
3. Le autorità di notifica sono istituite, organizzate e gestite in modo tale che non sorgano conflitti di interesse con gli organismi di valutazione della conformità e che siano salvaguardate l'obiettività e l'imparzialità delle loro attività.
4. Le autorità di notifica sono organizzate in modo che le decisioni relative alla notifica di un organismo di valutazione della conformità siano prese da persone competenti, diverse da quelle che hanno effettuato la valutazione.
5. Le autorità di notifica non offrono né svolgono attività eseguite dagli organismi di valutazione della conformità o servizi di consulenza su base commerciale o concorrenziale.
6. Le autorità di notifica salvaguardano la riservatezza delle informazioni ottenute.
7. Le autorità di notifica dispongono di un numero sufficiente di dipendenti competenti per l'adeguata esecuzione dei relativi compiti.
8. Le autorità di notifica si accertano che le valutazioni della conformità siano effettuate in modo proporzionato, evitando oneri inutili per i fornitori, e che gli organismi notificati svolgano le loro attività tenendo debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA in questione.

Articolo 31
Domanda di notifica presentata dagli organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità presentano una domanda di notifica all'autorità di notifica dello Stato membro in cui sono stabiliti.
2. La domanda di notifica è accompagnata da una descrizione delle attività di valutazione della conformità, del modulo o dei moduli di valutazione della conformità e delle tecnologie di intelligenza artificiale per le quali tale organismo di valutazione della conformità dichiara di essere competente, nonché da un certificato di accreditamento, se disponibile, rilasciato da un organismo nazionale di accreditamento che attesti che l'organismo di valutazione della conformità è conforme ai requisiti di cui all'articolo 33. Sono aggiunti documenti validi relativi

alle designazioni esistenti dell'organismo notificato richiedente ai sensi di qualsiasi altra normativa di armonizzazione dell'Unione.

3. Qualora non possa fornire un certificato di accreditamento, l'organismo di valutazione della conformità interessato fornisce all'autorità di notifica le prove documentali necessarie per la verifica, il riconoscimento e il controllo periodico della sua conformità ai requisiti di cui all'articolo 33. Per gli organismi notificati designati ai sensi di qualsiasi altra normativa di armonizzazione dell'Unione, tutti i documenti e i certificati connessi a tali designazioni possono essere utilizzati a sostegno della loro procedura di designazione a norma del presente regolamento, a seconda dei casi.

Articolo 32
Procedura di notifica

1. Le autorità di notifica possono notificare solo gli organismi di valutazione della conformità che soddisfino i requisiti di cui all'articolo 33.

2. Le autorità di notifica notificano la Commissione e gli altri Stati membri utilizzando lo strumento elettronico di notifica elaborato e gestito dalla Commissione.

3. La notifica include tutti i dettagli delle attività di valutazione della conformità, del modulo o dei moduli di valutazione della conformità e delle tecnologie di intelligenza artificiale interessate.

4. L'organismo di valutazione della conformità interessato può eseguire le attività di un organismo notificato solo se non sono sollevate obiezioni da parte della Commissione o degli altri Stati membri entro un mese dalla notifica.

5. Le autorità di notifica informano la Commissione e gli altri Stati membri di eventuali successive modifiche di rilievo apportate alla notifica.

Articolo 33
Organismi notificati

1. Gli organismi notificati verificano la conformità del sistema di IA ad alto rischio secondo le procedure di valutazione della conformità di cui all'articolo 43.

2. Gli organismi notificati soddisfano i requisiti organizzativi, di gestione della qualità e relativi alle risorse e ai processi necessari all'assolvimento dei loro compiti.

3. La struttura organizzativa, l'assegnazione delle responsabilità, le linee di riporto e il funzionamento degli organismi notificati sono tali da garantire la fiducia nelle prestazioni degli organismi notificati e nei risultati delle attività di valutazione della conformità che essi effettuano.

4. Gli organismi notificati sono indipendenti dal fornitore di un sistema di IA ad alto rischio in relazione al quale svolgono attività di valutazione della conformità. Gli organismi notificati sono inoltre indipendenti da qualsiasi altro operatore avente un interesse economico nel sistema di IA ad alto rischio oggetto della valutazione, nonché da eventuali concorrenti del fornitore.

5. Gli organismi notificati sono organizzati e gestiti in modo da salvaguardare l'indipendenza, l'obiettività e l'imparzialità delle loro attività. Gli organismi notificati documentano e attuano una struttura e procedure per salvaguardare l'imparzialità e per promuovere e applicare i principi di imparzialità in tutta l'organizzazione, tra il personale e nelle attività di valutazione.

6. Gli organismi notificati dispongono di procedure documentate per garantire che il loro personale, i loro comitati, affiliate, subappaltatori e qualsiasi altra organizzazione associata o il personale di organismi esterni rispettino la riservatezza delle informazioni di cui vengono in possesso nello svolgimento delle attività di valutazione della conformità, salvo quando la legge ne prescriva la divulgazione. Il personale degli organismi notificati è tenuto a osservare il segreto professionale riguardo a tutte le informazioni ottenute nello svolgimento dei suoi compiti a norma del presente regolamento, tranne che nei confronti delle autorità di notifica dello Stato membro in cui svolge le sue attività.

7. Gli organismi notificati dispongono di procedure per svolgere le attività che tengono debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA in questione.

8. Gli organismi notificati sottoscrivono un'adeguata assicurazione di responsabilità per le loro attività di valutazione della conformità, a meno che lo Stato membro interessato non si assuma tale responsabilità a norma del diritto interno o non sia direttamente responsabile della valutazione della conformità.

9. Gli organismi notificati sono in grado di eseguire tutti i compiti assegnati loro in forza del presente regolamento con il più elevato grado di integrità professionale e di competenza richiesta nel settore specifico, indipendentemente dal fatto che tali compiti siano eseguiti dagli organismi notificati stessi o per loro conto e sotto la loro responsabilità.

10. Gli organismi notificati dispongono di sufficienti competenze interne per poter valutare efficacemente i compiti svolti da parti esterne per loro conto. A tal fine, in ogni circostanza e per ogni procedura di valutazione della conformità e ogni tipo di sistema di IA ad alto rischio in relazione al quale sono stati designati, gli organismi notificati dispongono permanentemente di sufficiente personale amministrativo, tecnico e scientifico dotato di esperienza e conoscenze relative alle tecnologie, ai dati e al calcolo dei dati di intelligenza artificiale pertinenti, nonché ai requisiti di cui al capo 2 del presente titolo.

11. Gli organismi notificati partecipano alle attività di coordinamento di cui all'articolo 38. Inoltre essi partecipano direttamente o sono rappresentati in seno alle organizzazioni europee di normazione o garantiscono di essere informati e di mantenersi aggiornati in merito alle norme pertinenti.

12. Gli organismi notificati mettono a disposizione e trasmettono su richiesta tutta la documentazione pertinente, inclusa la documentazione del fornitore, all'autorità di notifica di cui all'articolo 30 per consentirle di svolgere le proprie attività di valutazione, designazione, notifica, monitoraggio e vigilanza e per agevolare la valutazione di cui al presente capo.

Articolo 34
Affiliate e subappaltatori degli organismi notificati

1. L'organismo notificato, qualora subappalti compiti specifici connessi alla valutazione della conformità oppure ricorra a un'affiliata, garantisce che il subappaltatore o l'affiliata soddisfino i requisiti di cui all'articolo 33 e ne informa l'autorità di notifica.

2. Gli organismi notificati si assumono la completa responsabilità dei compiti eseguiti da subappaltatori o affiliate, ovunque questi siano stabiliti.

3. Le attività possono essere subappaltate o eseguite da un'affiliata solo con il consenso del fornitore.

4. Gli organismi notificati tengono a disposizione dell'autorità di notifica i documenti pertinenti riguardanti la valutazione delle qualifiche del subappaltatore o dell'affiliata e il lavoro da essi eseguito a norma del presente regolamento.

Articolo 35
Numeri di identificazione e liste di organismi notificati designati a norma del presente regolamento

1. La Commissione assegna un numero di identificazione agli organismi notificati. Essa assegna un numero unico anche se un organismo è notificato a norma di diversi atti dell'Unione.

2. La Commissione mette pubblicamente a disposizione l'elenco degli organismi notificati a norma del presente regolamento, inclusi i numeri di identificazione loro assegnati e le attività per le quali sono stati notificati. La Commissione garantisce che l'elenco sia tenuto aggiornato.

Articolo 36
Modifiche delle notifiche

1. Qualora un'autorità di notifica sospetti o sia stata informata del fatto che un organismo notificato non soddisfa più i requisiti di cui all'articolo 33 o non adempie i suoi obblighi, tale autorità indaga senza ritardo sulla questione con la massima diligenza. In tale contesto, essa informa l'organismo notificato interessato in merito alle obiezioni sollevate e gli dà la possibilità di esprimere il suo punto di vista. Se l'autorità di notifica conclude che l'organismo notificato su cui ha condotto le indagini non soddisfa più i requisiti di cui all'articolo 33 o non adempie i suoi obblighi, tale autorità limita, sospende o ritira la notifica, a seconda dei casi, in funzione della gravità dell'inadempimento. Essa inoltre ne informa immediatamente la Commissione e gli altri Stati membri.

2. Nei casi di limitazione, sospensione o ritiro della notifica, oppure di cessazione dell'attività dell'organismo notificato, l'autorità di notifica adotta le misure appropriate per garantire che le pratiche di tale organismo notificato siano evase da un altro organismo notificato o siano tenute a disposizione delle autorità di notifica responsabili, su loro richiesta.

Articolo 37
Contestazione della competenza degli organismi notificati

1. Ove necessario, la Commissione indaga su tutti i casi in cui vi siano motivi di dubitare della conformità di un organismo notificato ai requisiti di cui all'articolo 33.

2. L'autorità di notifica fornisce alla Commissione, su richiesta, tutte le informazioni relative alla notifica dell'organismo notificato interessato.

3. La Commissione provvede affinché tutte le informazioni riservate ottenute nel corso delle sue indagini a norma del presente articolo siano trattate in maniera riservata.

4. La Commissione, qualora accerti che un organismo notificato non soddisfa o non soddisfa più i requisiti di cui all'articolo 33, adotta una decisione motivata con cui chiede allo Stato membro notificante di adottare le misure correttive necessarie,

compreso il ritiro della notifica. Tale atto di esecuzione è adottato in conformità alla procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 38
Coordinamento degli organismi notificati

1. La Commissione garantisce che, per quanto riguarda i settori disciplinati dal presente regolamento, siano istituiti e funzionino correttamente, sotto forma di un gruppo settoriale di organismi notificati, un coordinamento e una cooperazione adeguati tra gli organismi notificati che partecipano alle procedure di valutazione della conformità dei sistemi di IA a norma del presente regolamento.
2. Gli Stati membri garantiscono che gli organismi da essi notificati partecipino al lavoro di tale gruppo, direttamente o mediante rappresentanti designati.

Articolo 39
Organismi di valutazione della conformità di paesi terzi

Gli organismi di valutazione della conformità istituiti a norma del diritto di un paese terzo con il quale l'Unione ha concluso un accordo possono essere autorizzati a svolgere le attività degli organismi notificati a norma del presente regolamento.

CAPO 5

NORME, VALUTAZIONE DELLA CONFORMITÀ, CERTIFICATI, REGISTRAZIONE

Articolo 40
Norme armonizzate

I sistemi di IA ad alto rischio che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* si presumono conformi ai requisiti essenziali, di cui al capo 2 del presente titolo, nella misura in cui tali requisiti sono contemplati da tali norme.

Articolo 41
Specifiche comuni

1. Qualora non esistano norme armonizzate di cui all'articolo 40 o la Commissione ritenga che le norme armonizzate pertinenti siano insufficienti o che vi sia la necessità di rispondere a specifiche preoccupazioni in materia di sicurezza o di diritti fondamentali, la Commissione può, mediante atti di esecuzione, adottare specifiche comuni in relazione ai requisiti di cui al capo 2 del presente titolo. Tali atti di esecuzione sono adottati in conformità alla procedura d'esame di cui all'articolo 74, paragrafo 2.
2. Nel preparare le specifiche comuni di cui al paragrafo 1, la Commissione raccoglie i pareri dei pertinenti organismi o gruppi di esperti istituiti a norma del pertinente diritto settoriale dell'Unione.
3. I sistemi di IA ad alto rischio conformi alle specifiche comuni di cui al paragrafo 1 si presumono conformi ai requisiti di cui al capo 2 del presente titolo, nella misura in cui tali requisiti sono contemplati da tali specifiche comuni.

4. Qualora non rispettino le specifiche comuni di cui al paragrafo 1, i fornitori adottano soluzioni tecniche debitamente motivate che sono almeno equivalenti.

Articolo 42
Presunzione di conformità a determinati requisiti

1. Tenendo conto della loro finalità prevista, i sistemi di IA ad alto rischio che sono stati addestrati e sottoposti a prova con dati concernenti il contesto geografico, comportamentale e funzionale specifico all'interno del quale sono destinati a essere usati si presumono conformi al requisito di cui all'articolo 10, paragrafo 4.

2. I sistemi di IA ad alto rischio che sono stati certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersicurezza a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[63] e i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* si presumono conformi ai requisiti di cibersicurezza di cui all'articolo 15 del presente regolamento, nella misura in cui tali requisiti siano contemplati nel certificato di cibersicurezza o nella dichiarazione di conformità o in parti di essi.

Articolo 43
Valutazione della conformità

1. Per i sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, se ha applicato le norme armonizzate di cui all'articolo 40 o, ove applicabile, le specifiche comuni di cui all'articolo 41 nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, il fornitore segue una delle procedure seguenti:

   a) la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI;

   b) la procedura di valutazione della conformità basata sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica, con il coinvolgimento di un organismo notificato, di cui all'allegato VII.

   Se non ha applicato o ha applicato solo in parte le norme armonizzate di cui all'articolo 40 nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, o se tali norme armonizzate non esistono e non sono disponibili le specifiche comuni di cui all'articolo 41, il fornitore segue la procedura di valutazione della conformità di cui all'allegato VII.

   Ai fini della procedura di valutazione della conformità di cui all'allegato VII, il fornitore può scegliere uno qualsiasi degli organismi notificati. Tuttavia, quando il sistema è destinato ad essere messo in servizio dalle autorità di contrasto, dalle autorità competenti in materia di immigrazione o di asilo, nonché da istituzioni, organismi o agenzie dell'UE, l'autorità di vigilanza del mercato di cui all'articolo 63, paragrafo 5 o 6, a seconda dei casi, agisce in qualità di organismo notificato.

---

63 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

2. Per i sistemi di IA ad alto rischio di cui all'allegato III, punti da 2 a 8, i fornitori seguono la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI, che non prevede il coinvolgimento di un organismo notificato. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettera b), immessi sul mercato o messi in servizio da enti creditizi disciplinati dalla direttiva 2013/36/UE, la valutazione della conformità è effettuata nell'ambito della procedura di cui agli articoli da 97 a 101 di tale direttiva.

3. Per i sistemi di IA ad alto rischio ai quali si applicano gli atti giuridici elencati nell'allegato II, sezione A, il fornitore segue la pertinente valutazione della conformità prevista da tali atti giuridici. I requisiti di cui al capo 2 del presente titolo si applicano a tali sistemi di IA ad alto rischio e fanno parte di tale valutazione. Si applicano anche i punti 4.3, 4.4, 4.5 e il punto 4.6, quinto comma, dell'allegato VII.

   Ai fini di tale valutazione, gli organismi notificati che sono stati notificati a norma di tali atti giuridici hanno la facoltà di controllare la conformità dei sistemi di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 33, paragrafi 4, 9 e 10, sia stata valutata nel contesto della procedura di notifica a norma di tali atti giuridici.

   Qualora gli atti giuridici elencati nell'allegato II, sezione A, consentano al fabbricante del prodotto di sottrarsi a una valutazione della conformità da parte di terzi, purché abbia applicato tutte le norme armonizzate che contemplano tutti i requisiti pertinenti, tale fabbricante può avvalersi di tale facoltà solo se ha applicato anche le norme armonizzate o, ove applicabili, le specifiche comuni di cui all'articolo 41, che contemplano i requisiti di cui al capo 2 del presente titolo.

4. I sistemi di IA ad alto rischio sono sottoposti a una nuova procedura di valutazione della conformità dopo ogni modifica sostanziale, indipendentemente dal fatto che il sistema modificato sia destinato a essere ulteriormente distribuito o continui a essere usato dall'utente attuale.

   Per i sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio, le modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità e fanno parte delle informazioni contenute nella documentazione tecnica di cui all'allegato IV, punto 2, lettera f), non costituiscono una modifica sostanziale.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di aggiornare gli allegati VI e VII per introdurre elementi delle procedure di valutazione della conformità che divengano necessari alla luce del progresso tecnico.

6. Alla Commissione è conferito il potere di adottare atti delegati al fine di modificare i paragrafi 1 e 2 per assoggettare i sistemi di IA ad alto rischio di cui all'allegato III, punti da 2 a 8, alla procedura di valutazione della conformità di cui all'allegato VII o a parti di essa. La Commissione adotta tali atti delegati tenendo conto dell'efficacia della procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI nel prevenire o ridurre al minimo i rischi per la salute, la sicurezza e la protezione dei diritti fondamentali posti da tali sistemi, nonché della disponibilità di capacità e risorse adeguate tra gli organismi notificati.

Articolo 44
Certificati

1. I certificati rilasciati dagli organismi notificati a norma dell'allegato VII sono redatti in una delle lingue ufficiali dell'Unione scelta dallo Stato membro in cui è stabilito l'organismo notificato oppure in una lingua ufficiale dell'Unione altrimenti accettabile per l'organismo notificato.

2. I certificati sono validi per il periodo in essi indicato, che non può superare i cinque anni. Su domanda del fornitore, la validità di un certificato può essere prorogata per ulteriori periodi, ciascuno non superiore a cinque anni, sulla base di una nuova valutazione secondo le procedure di valutazione della conformità applicabili.

3. Qualora constati che il sistema di IA non soddisfa più i requisiti di cui al capo 2 del presente titolo, l'organismo notificato, tenendo conto del principio di proporzionalità, sospende o ritira il certificato rilasciato o impone limitazioni, a meno che la conformità a tali requisiti sia garantita mediante opportune misure correttive adottate dal fornitore del sistema entro un termine adeguato stabilito dall'organismo notificato. L'organismo notificato motiva la propria decisione.

Articolo 45
Ricorso contro le decisioni degli organismi notificati

Gli Stati membri provvedono affinché una procedura di ricorso contro le decisioni degli organismi notificati sia messa a disposizione delle parti aventi un interesse legittimo in tali decisioni.

Articolo 46
Obblighi di informazione degli organismi notificati

1. Gli organismi notificati informano l'autorità di notifica in merito a quanto segue:

   a) i certificati di valutazione della documentazione tecnica dell'Unione, i supplementi a tali certificati e le approvazioni dei sistemi di gestione della qualità rilasciati in conformità ai requisiti dell'allegato VII;

   b) qualsiasi rifiuto, limitazione, sospensione o ritiro di un certificato di valutazione della documentazione tecnica dell'Unione o un'approvazione del sistema di gestione della qualità rilasciati in conformità ai requisiti dell'allegato VII;

   c) qualsiasi circostanza che influisca sull'ambito o sulle condizioni della notifica;

   d) qualsiasi richiesta di informazioni che hanno ricevuto dalle autorità di vigilanza del mercato, in relazione ad attività di valutazione della conformità;

   e) su richiesta, le attività di valutazione della conformità effettuate nell'ambito della loro notifica e qualsiasi altra attività, incluse quelle transfrontaliere e il subappalto.

2. Ciascun organismo notificato informa gli altri organismi notificati in merito a quanto segue:

   a) le approvazioni dei sistemi di gestione della qualità da esso rifiutate, sospese o ritirate e, su richiesta, le approvazioni dei sistemi di qualità da esso rilasciate;

b) i certificati di valutazione della documentazione tecnica dell'UE o i relativi supplementi da esso rifiutati, ritirati, sospesi o altrimenti limitati e, su richiesta, i certificati e/o i relativi supplementi da esso rilasciati.

3. Ciascun organismo notificato fornisce agli altri organismi notificati che svolgono attività simili di valutazione della conformità riguardanti le stesse tecnologie di intelligenza artificiale informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, positivi della valutazione della conformità.

Articolo 47
Deroga alla procedura di valutazione della conformità

1. In deroga all'articolo 43, qualsiasi autorità di vigilanza del mercato può autorizzare l'immissione sul mercato o la messa in servizio di specifici sistemi di IA ad alto rischio nel territorio dello Stato membro interessato, per motivi eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente e dei principali beni industriali e infrastrutturali. Tale autorizzazione è valida per un periodo di tempo limitato, mentre sono in corso le necessarie procedure di valutazione della conformità, e termina una volta completate tali procedure. Il completamento di tali procedure è effettuato senza indebito ritardo.

2. L'autorizzazione di cui al paragrafo 1 è rilasciata solo se l'autorità di vigilanza del mercato conclude che il sistema di IA ad alto rischio è conforme ai requisiti di cui al capo 2 del presente titolo. L'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri di eventuali autorizzazioni rilasciate a norma del paragrafo 1.

3. Se, entro 15 giorni di calendario dal ricevimento dell'informazione di cui al paragrafo 2, né gli Stati membri né la Commissione sollevano obiezioni in merito a un'autorizzazione rilasciata da un'autorità di vigilanza del mercato di uno Stato membro in conformità al paragrafo 1, tale autorizzazione è considerata giustificata.

4. Se, entro 15 giorni di calendario dal ricevimento della notifica di cui al paragrafo 2, uno Stato membro solleva obiezioni in merito a un'autorizzazione rilasciata da un'autorità di vigilanza del mercato di un altro Stato membro, o se la Commissione ritiene che l'autorizzazione sia contraria al diritto dell'Unione o che la conclusione degli Stati membri riguardante la conformità del sistema di cui al paragrafo 2 sia infondata, la Commissione avvia senza ritardo consultazioni con lo Stato membro interessato; l'operatore o gli operatori interessati sono consultati e hanno la possibilità di esprimere il loro parere. In seguito a tale consultazione la Commissione decide se l'autorizzazione è giustificata o meno. La Commissione trasmette la propria decisione allo Stato membro interessato e all'operatore o agli operatori pertinenti.

5. Se l'autorizzazione è ritenuta ingiustificata, essa è ritirata dall'autorità di vigilanza del mercato dello Stato membro interessato.

6. In deroga ai paragrafi da 1 a 5, per i sistemi di IA ad alto rischio destinati a essere utilizzati come componenti di sicurezza di dispositivi, o che sono essi stessi dispositivi, disciplinati dal regolamento (UE) 2017/745 e dal regolamento (UE) 2017/746, l'articolo 59 del regolamento (UE) 2017/745 e l'articolo 54 del regolamento (UE) 2017/746 si applicano anche per quanto riguarda la deroga alla valutazione della conformità ai requisiti di cui al capo 2 del presente titolo.

Articolo 48
Dichiarazione di conformità UE

1. Il fornitore compila una dichiarazione scritta di conformità UE per ciascun sistema di IA e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA è stato immesso sul mercato. La dichiarazione di conformità UE identifica il sistema di IA per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è messa a disposizione delle pertinenti autorità nazionali competenti.

2. La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio in questione soddisfa i requisiti di cui al capo 2 del presente titolo. La dichiarazione di conformità UE riporta come minimo le informazioni di cui all'allegato V ed è tradotta in una lingua o nelle lingue ufficiali dell'Unione richieste dallo Stato membro nel quale il sistema di IA ad alto rischio è messo a disposizione.

3. Qualora i sistemi di IA ad alto rischio siano soggetti ad altre normative di armonizzazione dell'Unione che richiedano anch'esse una dichiarazione di conformità UE, è redatta un'unica dichiarazione di conformità UE in relazione a tutte le normative dell'Unione applicabili al sistema di IA ad alto rischio. La dichiarazione contiene tutte le informazioni necessarie per identificare la normativa di armonizzazione dell'Unione cui si riferisce la dichiarazione.

4. Redigendo la dichiarazione di conformità UE, il fornitore si assume la responsabilità della conformità ai requisiti di cui al capo 2 del presente titolo. Il fornitore tiene opportunamente aggiornata la dichiarazione di conformità UE.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di aggiornare il contenuto della dichiarazione di conformità UE di cui all'allegato V per introdurre elementi che si rendano necessari alla luce del progresso tecnico.

Articolo 49
Marcatura CE di conformità

1. La marcatura CE è apposta sul sistema di IA ad alto rischio in modo visibile, leggibile e indelebile. Qualora ciò sia impossibile o difficilmente realizzabile a causa della natura del sistema di IA ad alto rischio, il marchio è apposto sull'imballaggio o sui documenti di accompagnamento, a seconda dei casi.

2. La marcatura CE di cui al paragrafo 1 del presente articolo è soggetta ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.

3. Ove applicabile, la marcatura CE è seguita dal numero di identificazione dell'organismo notificato responsabile delle procedure di valutazione della conformità di cui all'articolo 43. Il numero d'identificazione è inoltre indicato in tutto il materiale promozionale in cui si afferma che il sistema di IA ad alto rischio soddisfa i requisiti per la marcatura CE.

Articolo 50
Conservazione dei documenti

Il fornitore, per un periodo che termina 10 anni dopo che il sistema di IA è stato immesso sul mercato o messo in servizio, tiene a disposizione delle autorità nazionali competenti:

a) la documentazione tecnica di cui all'articolo 11;

b) la documentazione relativa al sistema di gestione della qualità di cui all'articolo 17;

c) la documentazione relativa alle modifiche approvate dagli organismi notificati, ove applicabile;

d) le decisioni e gli altri documenti rilasciati dagli organismi notificati, ove applicabile;

e) la dichiarazione di conformità UE di cui all'articolo 48.

Articolo 51
Registrazione

Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, il fornitore o, ove applicabile, il rappresentante autorizzato registra tale sistema nella banca dati dell'UE di cui all'articolo 60.

TITOLO IV

OBBLIGHI DI TRASPARENZA PER DETERMINATI SISTEMI DI IA

Articolo 52
Obblighi di trasparenza per determinati sistemi di IA

1. I fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

2. Gli utenti di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica, che sono autorizzati dalla legge per accertare, prevenire e indagare reati.

3. Gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake") sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente.

   Tuttavia il primo comma non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

4. I paragrafi 1, 2 e 3 lasciano impregiudicati i requisiti e gli obblighi di cui al titolo III del presente regolamento.

TITOLO V

MISURE A SOSTEGNO DELL'INNOVAZIONE

Articolo 53
Spazi di sperimentazione normativa per l'IA

1. Gli spazi di sperimentazione normativa per l'IA istituiti da una o più autorità competenti degli Stati membri o dal Garante europeo della protezione dei dati forniscono un ambiente controllato che facilita lo sviluppo, le prove e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico. Ciò avviene sotto la guida e il controllo diretti delle autorità competenti al fine di garantire la conformità ai requisiti del presente regolamento e, se del caso, di altre normative dell'Unione e degli Stati membri controllate all'interno dello spazio di sperimentazione.

2. Gli Stati membri garantiscono che, nella misura in cui i sistemi di IA innovativi comportano il trattamento di dati personali o rientrano altrimenti nell'ambito di competenza di altre autorità nazionali o autorità competenti che forniscono o sostengono l'accesso ai dati, le autorità nazionali per la protezione dei dati e tali altre autorità nazionali siano associate al funzionamento dello spazio di sperimentazione normativa per l'IA.

3. Gli spazi di sperimentazione normativa per l'IA non pregiudicano i poteri correttivi e di controllo delle autorità competenti. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi deve comportare l'adozione di immediate misure di attenuazione e, in mancanza di ciò, la sospensione del processo di sviluppo e di prova fino a che tali rischi non risultino attenuati.

4. I partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi della normativa applicabile dell'Unione e degli Stati membri in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione.

5. Le autorità competenti degli Stati membri che hanno istituito spazi di sperimentazione normativa per l'IA coordinano le loro attività e cooperano nel quadro del comitato europeo per l'intelligenza artificiale. Esse presentano al Comitato e alla Commissione relazioni annuali sui risultati dell'attuazione di tali sistemi, comprese le buone pratiche, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione del presente regolamento e di altre normative dell'Unione soggette a controllo nell'ambito dello spazio di sperimentazione.

6. Le modalità e le condizioni di funzionamento degli spazi di sperimentazione normativa per l'IA, compresi i criteri di ammissibilità e la procedura per la domanda, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione, nonché i diritti e gli obblighi dei partecipanti sono stabiliti in atti di esecuzione. Tali atti di esecuzione sono adottati in conformità alla procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 54

Ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico

1. Nello spazio di sperimentazione normativa per l'IA i dati personali legalmente raccolti per altre finalità sono trattati ai fini dello sviluppo e delle prove nello spazio di sperimentazione di determinati sistemi di IA innovativi alle seguenti condizioni:

   a) i sistemi di IA innovativi sono sviluppati per salvaguardare un interesse pubblico rilevante in uno o più dei seguenti settori:

      i) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità competenti. Il trattamento si basa sul diritto degli Stati membri o dell'Unione;

      ii) la sicurezza pubblica e la sanità pubblica, compresi la prevenzione, il controllo e il trattamento delle malattie;

      iii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente;

   b) i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al titolo III, capo 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento anonimizzato, sintetico o di altri dati non personali;

   c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti fondamentali degli interessati durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento;

   d) i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo dei partecipanti e solo le persone autorizzate hanno accesso a tali dati;

   e) i dati personali trattati non devono essere trasmessi, trasferiti o altrimenti consultati da terzi;

   f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati;

   g) i dati personali trattati nell'ambito dello spazio di sperimentazione sono cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali;

   h) i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione e per 1 anno dopo la sua cessazione, al solo scopo di adempiere gli obblighi di rendicontazione e documentazione previsti dal presente articolo o da altre normative applicabili dell'Unione o degli Stati membri e solo per il tempo necessario per adempiere tali obblighi;

   i) una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata

insieme ai risultati delle prove nell'ambito della documentazione tecnica di cui all'allegato IV;

j) una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito web delle autorità competenti.

2. Il paragrafo 1 lascia impregiudicata la normativa dell'Unione o degli Stati membri che esclude il trattamento per fini diversi da quelli espressamente menzionati in tale normativa.

Articolo 55
Misure per i fornitori di piccole dimensioni e gli utenti

1. Gli Stati membri intraprendono le seguenti azioni:

a) fornire ai fornitori di piccole dimensioni e alle start-up un accesso prioritario agli spazi di sperimentazione normativa per l'IA nella misura in cui essi soddisfano le condizioni di ammissibilità;

b) organizzare specifiche attività di sensibilizzazione sull'applicazione del presente regolamento adattate alle esigenze dei fornitori di piccole dimensioni e degli utenti;

c) ove opportuno, istituire un canale dedicato per la comunicazione con i fornitori di piccole dimensioni, gli utenti e altri innovatori, al fine di fornire orientamenti e rispondere alle domande sull'attuazione del presente regolamento.

2. Nel fissare le tariffe per la valutazione della conformità a norma dell'articolo 43 si tiene conto degli interessi e delle esigenze specifici dei fornitori di piccole dimensioni, riducendo tali tariffe proporzionalmente alle loro dimensioni e alle dimensioni del loro mercato.

TITOLO VI

GOVERNANCE

CAPO 1

COMITATO EUROPEO PER L'INTELLIGENZA ARTIFICIALE

Articolo 56
Istituzione del comitato europeo per l'intelligenza artificiale

1. È istituito un "comitato europeo per l'intelligenza artificiale" (il "comitato").

2. Il comitato fornisce consulenza e assistenza alla Commissione al fine di:

a) contribuire all'efficace cooperazione delle autorità nazionali di controllo e della Commissione per quanto riguarda le materie disciplinate dal presente regolamento;

b) coordinare e contribuire agli orientamenti e all'analisi della Commissione, delle autorità nazionali di controllo e di altre autorità competenti sulle questioni

emergenti nel mercato interno in relazione alle materie disciplinate dal presente regolamento;

c) assistere le autorità nazionali di controllo e la Commissione nel garantire l'applicazione uniforme del presente regolamento.

Articolo 57
Struttura del comitato

1. Il comitato è composto dalle autorità nazionali di controllo, rappresentate dal capo di tale autorità o da un alto funzionario di livello equivalente, e dal Garante europeo della protezione dei dati. Altre autorità nazionali possono essere invitate alle riunioni, qualora le questioni discusse siano di loro pertinenza.

2. Il comitato adotta il suo regolamento interno a maggioranza semplice dei suoi membri, previo consenso della Commissione. Il regolamento interno contiene anche gli aspetti operativi relativi all'esecuzione dei compiti del comitato di cui all'articolo 58. Il comitato può istituire sottogruppi, se necessario, per esaminare questioni specifiche.

3. Il comitato è presieduto dalla Commissione. La Commissione convoca le riunioni e prepara l'ordine del giorno in conformità ai compiti del comitato a norma del presente regolamento e del relativo regolamento interno. La Commissione fornisce sostegno amministrativo e analitico per le attività del comitato a norma del presente regolamento.

4. Il comitato può invitare esperti e osservatori esterni a partecipare alle sue riunioni e può tenere scambi con terzi interessati al fine di orientare, nella giusta misura, le proprie attività. A tal fine la Commissione può agevolare gli scambi tra il comitato e altri organismi, uffici, agenzie e gruppi consultivi dell'Unione.

Articolo 58
Compiti del comitato

Nel fornire consulenza e assistenza alla Commissione nel contesto dell'articolo 56, paragrafo 2, il Comitato in particolare:

a) raccoglie e condivide conoscenze e migliori pratiche tra gli Stati membri;

b) contribuisce all'uniformità delle pratiche amministrative negli Stati membri, anche per il funzionamento degli spazi di sperimentazione normativi di cui all'articolo 53;

c) formula pareri, raccomandazioni o contributi scritti su questioni relative all'attuazione del presente regolamento, in particolare

   i) sulle specifiche tecniche o sulle norme esistenti relative ai requisiti di cui al titolo III, capo 2,

   ii) sull'uso delle norme armonizzate o delle specifiche comuni di cui agli articoli 40 e 41,

   iii) sulla preparazione di documenti di orientamento, compresi gli orientamenti per stabilire le sanzioni amministrative pecuniarie di cui all'articolo 71.

CAPO 2

AUTORITÀ NAZIONALI COMPETENTI

Articolo 59
Designazione delle autorità nazionali competenti

1. Ciascuno Stato membro istituisce o designa autorità nazionali competenti al fine di garantire l'applicazione e l'attuazione del presente regolamento. Le autorità nazionali competenti sono organizzate e gestite in modo che sia salvaguardata l'obiettività e l'imparzialità dei loro compiti e attività.

2. Ciascuno Stato membro designa un'autorità nazionale di controllo tra le autorità nazionali competenti. L'autorità nazionale di controllo agisce in qualità di autorità di notifica e di autorità di vigilanza del mercato, a meno che uno Stato membro non abbia motivi organizzativi e amministrativi per designare più di un'autorità.

3. Gli Stati membri informano la Commissione della loro designazione o delle loro designazioni e, ove applicabile, dei motivi che giustificano la designazione di più autorità.

4. Gli Stati membri garantiscono che le autorità nazionali competenti dispongano di risorse finanziarie e umane adeguate per svolgere i loro compiti a norma del presente regolamento. In particolare, le autorità nazionali competenti dispongono di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di intelligenza artificiale, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti.

5. Gli Stati membri riferiscono annualmente alla Commissione in merito allo stato delle risorse finanziarie e umane delle autorità nazionali competenti, con una valutazione della loro adeguatezza. La Commissione trasmette tali informazioni al comitato affinché le discuta e formuli eventuali raccomandazioni.

6. La Commissione agevola lo scambio di esperienze tra autorità nazionali competenti.

7. Le autorità nazionali competenti possono fornire orientamenti e consulenza sull'attuazione del presente regolamento, anche ai fornitori di piccole dimensioni. Ogniqualvolta le autorità nazionali competenti intendono fornire orientamenti e consulenza in relazione a un sistema di IA in settori disciplinati da altre normative dell'Unione, sono consultate le autorità nazionali competenti a norma di tale normativa dell'Unione, come opportuno. Gli Stati membri possono inoltre istituire un punto di contatto centrale per la comunicazione con gli operatori.

8. Nei casi in cui le istituzioni, le agenzie e gli organismi dell'Unione rientrano nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità competente per la loro vigilanza.

TITOLO VII

BANCA DATI DELL'UE PER I SISTEMI DI IA INDIPENDENTI AD ALTO RISCHIO

Articolo 60
Banca dati dell'UE per i sistemi di IA indipendenti ad alto rischio

1. La Commissione, in collaborazione con gli Stati membri, istituisce e mantiene una banca dati dell'UE contenente le informazioni di cui al paragrafo 2 relative ai sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2, registrati conformemente all'articolo 51.
2. I fornitori inseriscono nella banca dati dell'UE i dati elencati nell'allegato VIII. La Commissione fornisce loro sostegno tecnico e amministrativo.
3. Le informazioni contenute nella banca dati dell'UE sono accessibili al pubblico.
4. La banca dati dell'UE contiene dati personali solo nella misura necessaria per la raccolta e il trattamento delle informazioni in conformità al presente regolamento. Tali informazioni comprendono i nomi e i dati di contatto delle persone fisiche responsabili della registrazione del sistema e aventi l'autorità legale di rappresentare il fornitore.
5. La Commissione è il titolare del trattamento della banca dati dell'UE. Essa garantisce inoltre ai fornitori un adeguato sostegno tecnico e amministrativo.

TITOLO VIII

MONITORAGGIO SUCCESSIVO ALL'IMMISSIONE SUL MERCATO, CONDIVISIONE DELLE INFORMAZIONI, VIGILANZA DEL MERCATO

CAPO 1

MONITORAGGIO SUCCESSIVO ALL'IMMISSIONE SUL MERCATO

Articolo 61
Monitoraggio successivo all'immissione sul mercato effettuato dai fornitori e piano di monitoraggio successivo all'immissione sul mercato per i sistemi di IA ad alto rischio

1. I fornitori istituiscono e documentano un sistema di monitoraggio successivo all'immissione sul mercato che sia proporzionato alla natura delle tecnologie di intelligenza artificiale e ai rischi del sistema di IA ad alto rischio.
2. Il sistema di monitoraggio successivo all'immissione sul mercato raccoglie, documenta e analizza attivamente e sistematicamente i dati pertinenti forniti dagli utenti o raccolti tramite altre fonti sulle prestazioni dei sistemi di IA ad alto rischio per tutta la durata del loro ciclo di vita e consente al fornitore di valutare la costante conformità dei sistemi di IA ai requisiti di cui al titolo III, capo 2.

3. Il sistema di monitoraggio successivo all'immissione sul mercato si basa su un piano di monitoraggio successivo all'immissione sul mercato. Il piano di monitoraggio successivo all'immissione sul mercato fa parte della documentazione tecnica di cui all'allegato IV. La Commissione adotta un atto di esecuzione che stabilisce disposizioni dettagliate in cui si definisce un modello per il piano di monitoraggio successivo all'immissione sul mercato e un elenco di elementi da includere nel piano.

4. Per i sistemi di IA ad alto rischio disciplinati dagli atti giuridici di cui all'allegato II, qualora tale normativa preveda già un sistema e un piano di monitoraggio successivo all'immissione sul mercato, gli elementi di cui ai paragrafi 1, 2 e 3 sono integrati, come opportuno, in tale sistema e tale piano.

   Il primo comma si applica anche ai sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettera b), immessi sul mercato o messi in servizio da enti creditizi disciplinati dalla direttiva 2013/36/UE.

CAPO 2

CONDIVISIONE DI INFORMAZIONI SU INCIDENTI E MALFUNZIONAMENTI

Articolo 62
Segnalazione di incidenti gravi o malfunzionamenti

1. I fornitori di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi incidente grave o malfunzionamento di tali sistemi che costituisca una violazione degli obblighi previsti dal diritto dell'Unione intesi a tutelare i diritti fondamentali alle autorità di vigilanza del mercato degli Stati membri in cui tali incidenti o violazioni si sono verificati.

   Tale notifica è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente o il malfunzionamento o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che è venuto a conoscenza dell'incidente grave o del malfunzionamento.

2. Al ricevimento di una notifica relativa a una violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, l'autorità di vigilanza del mercato informa le autorità o gli organismi pubblici nazionali di cui all'articolo 64, paragrafo 3. La Commissione elabora orientamenti specifici per facilitare il rispetto degli obblighi di cui al paragrafo 1. Tali orientamenti sono emanati al più tardi 12 mesi dopo l'entrata in vigore del presente regolamento.

3. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettera b), immessi sul mercato o messi in servizio da fornitori che sono enti creditizi disciplinati dalla direttiva 2013/36/UE e per i sistemi di IA ad alto rischio che sono componenti di sicurezza di dispositivi, o sono essi stessi dispositivi, disciplinati dal regolamento (UE) 2017/745 e dal regolamento (UE) 2017/746, la notifica è limitata a incidenti gravi o malfunzionamenti che costituiscono una violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali.

CAPO 3

APPLICAZIONE

Articolo 63
Vigilanza del mercato e controllo dei sistemi di IA nel mercato dell'Unione

1. Il regolamento (UE) 2019/1020 si applica ai sistemi di IA disciplinati dal presente regolamento. Tuttavia, ai fini dell'efficace applicazione del presente regolamento:

   a) ogni riferimento a un operatore economico a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti gli operatori di cui al titolo III, capo 3, del presente regolamento;

   b) ogni riferimento a un prodotto a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti i sistemi di IA che rientrano nell'ambito di applicazione del presente regolamento.

2. L'autorità nazionale di controllo riferisce periodicamente alla Commissione in merito ai risultati delle pertinenti attività di vigilanza del mercato. L'autorità nazionale di controllo comunica senza indugio alla Commissione e alle pertinenti autorità nazionali garanti della concorrenza qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per l'applicazione del diritto dell'Unione in materia di concorrenza.

3. Per i sistemi di IA ad alto rischio, collegati a prodotti cui si applicano gli atti giuridici elencati nell'allegato II, sezione A, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità responsabile delle attività di vigilanza del mercato designata a norma di tali atti giuridici.

4. Per i sistemi di IA immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dalla normativa dell'Unione in materia di servizi finanziari, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità pertinente responsabile della vigilanza finanziaria di tali enti ai sensi di tale normativa.

5. Per i sistemi di IA elencati al punto 1, lettera a), nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, e ai punti 6 e 7 dell'allegato III, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma della direttiva (UE) 2016/680 o del regolamento (CE) n. 2016/679 o le autorità nazionali competenti che controllano le attività delle autorità di contrasto o delle autorità competenti in materia di immigrazione o di asilo che mettono in servizio o usano tali sistemi.

6. Nei casi in cui le istituzioni, le agenzie e gli organismi dell'Unione rientrano nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità di vigilanza del mercato.

7. Gli Stati membri agevolano il coordinamento tra le autorità di vigilanza del mercato designate a norma del presente regolamento e altre autorità o organismi nazionali pertinenti che controllano l'applicazione della normativa di armonizzazione dell'Unione elencata nell'allegato II o di altre normative dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III.

Articolo 64
Accesso ai dati e documentazione

1. Per quanto riguarda l'accesso ai dati e alla documentazione nell'ambito delle loro attività, alle autorità di vigilanza del mercato è concesso pieno accesso ai set di dati di addestramento, convalida e prova utilizzati dal fornitore, anche attraverso interfacce di programmazione delle applicazioni ("API") o altri mezzi tecnici e strumenti adeguati che consentano l'accesso remoto.

2. Ove necessario per valutare la conformità del sistema di IA ad alto rischio ai requisiti di cui al titolo III, capo 2, e su richiesta motivata, alle autorità di vigilanza del mercato è concesso l'accesso al codice sorgente del sistema di IA.

3. Le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali in relazione all'uso dei sistemi di IA ad alto rischio di cui all'allegato III hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi quando l'accesso a tale documentazione è necessario per l'adempimento delle competenze a norma del loro mandato entro i limiti della loro giurisdizione. L'autorità pubblica o l'organismo pubblico pertinente informa l'autorità di vigilanza del mercato dello Stato membro interessato di qualsiasi richiesta in tal senso.

4. Entro 3 mesi dall'entrata in vigore del presente regolamento, ciascuno Stato membro individua le autorità o gli organismi pubblici di cui al paragrafo 3 e pubblica un elenco sul sito web dell'autorità nazionale di controllo. Gli Stati membri notificano l'elenco alla Commissione e a tutti gli altri Stati membri e lo tengono aggiornato.

5. Qualora la documentazione di cui al paragrafo 3 non sia sufficiente per accertare un'eventuale violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, l'autorità pubblica o l'organismo pubblico di cui al paragrafo 3 può presentare all'autorità di vigilanza del mercato una richiesta motivata al fine di organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici. L'autorità di vigilanza del mercato organizza le prove coinvolgendo da vicino l'autorità pubblica o l'organismo pubblico richiedente entro un termine ragionevole dalla richiesta.

6. Qualsiasi informazione e documentazione ottenuta dalle autorità o dagli organismi pubblici nazionali di cui al paragrafo 3 a norma delle disposizioni del presente articolo è trattata nel rispetto degli obblighi di riservatezza di cui all'articolo 70.

Articolo 65
Procedura per i sistemi di IA che presentano un rischio a livello nazionale

1. Un sistema di IA che presenta un rischio è inteso come un prodotto che presenta un rischio definito all'articolo 3, punto 19, del regolamento (UE) 2019/1020 per quanto riguarda i rischi per la salute o la sicurezza o per la tutela dei diritti fondamentali delle persone.

2. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia motivi sufficienti per ritenere che un sistema di IA presenti un rischio di cui al paragrafo 1, essa effettua una valutazione del sistema di IA interessato per quanto riguarda la sua conformità a tutti i requisiti e gli obblighi di cui al presente regolamento. In presenza di rischi per la tutela dei diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti di cui

all'articolo 64, paragrafo 3. I pertinenti operatori cooperano, per quanto necessario, con le autorità di vigilanza del mercato e con le altre autorità o gli altri organismi pubblici nazionali di cui all'articolo 64, paragrafo 3.

Se, nel corso di tale valutazione, le autorità di vigilanza del mercato rilevano che il sistema di IA non è conforme ai requisiti e agli obblighi di cui al presente regolamento, esse chiedono senza ritardo al pertinente operatore di adottare tutte le misure correttive adeguate al fine di, a seconda dei casi, ripristinare la conformità del sistema di IA, ritirarlo dal mercato o richiamarlo entro un termine ragionevole e proporzionale alla natura del rischio.

L'autorità di vigilanza del mercato informa di conseguenza l'organismo notificato pertinente. L'articolo 18 del regolamento (UE) 2019/1020 si applica alle misure di cui al secondo comma.

3. Qualora ritenga che la non conformità non sia limitata al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri dei risultati della valutazione e delle azioni che hanno chiesto all'operatore economico di intraprendere.

4. L'operatore garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i sistemi di IA interessati che ha messo a disposizione sul mercato in tutta l'Unione.

5. Qualora l'operatore di un sistema di IA non adotti misure correttive adeguate nel periodo di cui al paragrafo 2, l'autorità di vigilanza del mercato adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione del sistema di IA sul mercato nazionale, per ritirare il prodotto dal mercato o per richiamarlo. Tale autorità informa senza ritardo la Commissione e gli altri Stati membri di tale misure.

6. Le informazioni di cui al paragrafo 5 includono tutti i particolari disponibili, soprattutto i dati necessari all'identificazione del sistema di IA non conforme, la sua origine, la natura della presunta non conformità e dei rischi connessi, la natura e la durata delle misure nazionali adottate, nonché gli argomenti espressi dal pertinente operatore. Le autorità di vigilanza del mercato indicano in particolare se la non conformità sia dovuta a una o più delle cause seguenti:

   a) mancato rispetto da parte del sistema di IA dei requisiti di cui al titolo III, capo 2;

   b) carenze nelle norme armonizzate o nelle specifiche comuni, di cui agli articoli 40 e 41, che conferiscono la presunzione di conformità.

7. Le autorità di vigilanza del mercato degli Stati membri diverse dall'autorità di vigilanza del mercato dello Stato membro che ha avviato la procedura comunicano senza ritardo alla Commissione e agli altri Stati membri tutte le misure adottate, tutte le altre informazioni a loro disposizione sulla non conformità del sistema di IA interessato e, in caso di disaccordo con la misura nazionale notificata, le loro obiezioni.

8. Se, entro tre mesi dal ricevimento delle informazioni di cui al paragrafo 5, uno Stato membro o la Commissione non sollevano obiezioni contro la misura provvisoria adottata da uno Stato membro, tale misura è ritenuta giustificata. Ciò non pregiudica i diritti procedurali dell'operatore interessato in conformità all'articolo 18 del regolamento (UE) 2019/1020.

9. Le autorità di vigilanza del mercato garantiscono che siano adottate senza ritardo adeguate misure restrittive in relazione al prodotto interessato, come il ritiro del prodotto dal loro mercato.

Articolo 66
Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di cui all'articolo 65, paragrafo 5, uno Stato membro solleva obiezioni contro la misura adottata da un altro Stato membro, o se la Commissione ritiene che la misura sia contraria al diritto dell'Unione, la Commissione consulta senza ritardo lo Stato membro e l'operatore o gli operatori pertinenti e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione decide se la misura nazionale sia giustificata o meno entro 9 mesi dalla notifica di cui all'articolo 65, paragrafo 5, e notifica tale decisione allo Stato membro interessato.

2. Se la misura nazionale è ritenuta giustificata, tutti gli Stati membri adottano le misure necessarie a garantire che il sistema di IA non conforme sia ritirato dal loro mercato e ne informano la Commissione. Se la misura nazionale è ritenuta ingiustificata, lo Stato membro interessato provvede a ritirarla.

3. Se la misura nazionale è ritenuta giustificata e la non conformità del sistema di IA viene attribuita alle carenze nelle norme armonizzate o nelle specifiche comuni di cui agli articoli 40 e 41 del presente regolamento, la Commissione applica la procedura di cui all'articolo 11 del regolamento (UE) n. 1025/2012.

Articolo 67
Sistemi di IA conformi che presentano un rischio

1. Se, dopo aver effettuato una valutazione a norma dell'articolo 65, l'autorità di vigilanza del mercato di uno Stato membro ritiene che, sebbene conforme al presente regolamento, il sistema di IA presenti un rischio per la salute o la sicurezza delle persone, per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore pertinente di adottare tutte le misure adeguate a far sì che il sistema di IA, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio o che sia, a seconda dei casi, ritirato dal mercato o richiamato entro un termine ragionevole, proporzionato alla natura del rischio.

2. Il fornitore o altri operatori pertinenti garantiscono l'adozione di misure correttive nei confronti di tutti i sistemi di IA interessati che hanno messo a disposizione sul mercato in tutta l'Unione entro il termine prescritto dall'autorità di vigilanza del mercato dello Stato membro di cui al paragrafo 1.

3. Lo Stato membro informa immediatamente la Commissione e gli altri Stati membri. Tali informazioni comprendono tutti i dettagli disponibili, in particolare i dati necessari all'identificazione del sistema di IA interessato, l'origine e la catena di approvvigionamento del sistema di IA, la natura del rischio connesso, nonché la natura e la durata delle misure nazionali adottate.

4. La Commissione avvia senza ritardo consultazioni con gli Stati membri e l'operatore o gli operatori pertinenti e valuta le misure nazionali adottate. In base ai risultati di tale valutazione, la Commissione decide se la misura sia giustificata o meno e propone, ove necessario, misure appropriate.

5. La Commissione trasmette la decisione agli Stati membri.

Articolo 68
Non conformità formale

1. Un'autorità di vigilanza del mercato di uno Stato membro che giunga a una delle conclusioni riportate di seguito chiede all'operatore pertinente di porre fine alla non conformità contestata:

   a) la marcatura di conformità è stata apposta in violazione dell'articolo 49;

   b) la marcatura di conformità non è stata apposta;

   c) la dichiarazione di conformità UE non è stata redatta;

   d) la dichiarazione di conformità UE non è stata redatta correttamente;

   e) il numero di identificazione dell'organismo notificato coinvolto nella procedura di valutazione della conformità, ove applicabile, non è stato apposto.

2. Se la non conformità di cui al paragrafo 1 permane, lo Stato membro interessato adotta tutte le misure appropriate per limitare o proibire la messa a disposizione sul mercato del sistema di IA ad alto rischio o garantisce che sia richiamato o ritirato dal mercato.

TITOLO IX

CODICI DI CONDOTTA

Articolo 69
Codici di condotta

1. La Commissione e gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta intesi a promuovere l'applicazione volontaria ai sistemi di IA diversi dai sistemi di IA ad alto rischio dei requisiti di cui al titolo III, capo 2, sulla base di specifiche tecniche e soluzioni che costituiscono mezzi adeguati per garantire la conformità a tali requisiti alla luce della finalità prevista dei sistemi.

2. La Commissione e il comitato incoraggiano e agevolano l'elaborazione di codici di condotta intesi a promuovere l'applicazione volontaria ai sistemi di IA dei requisiti relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità per le persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di IA e alla diversità dei gruppi che si occupano dello sviluppo sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi.

3. I codici di condotta possono essere elaborati da singoli fornitori di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione degli utenti e di tutti gli altri portatori di interessi e delle loro organizzazioni rappresentative. I codici di condotta possono riguardare uno o più sistemi di IA tenendo conto della similarità della finalità prevista dei sistemi pertinenti.

4. Nell'incoraggiare e agevolare l'elaborazione di codici di condotta, la Commissione e il comitato tengono conto degli interessi e delle esigenze specifici dei fornitori di piccole dimensioni e delle start-up.

TITOLO X

RISERVATEZZA E SANZIONI

Articolo 70
Riservatezza

1. Le autorità nazionali competenti e gli organismi notificati che partecipano all'applicazione del presente regolamento rispettano la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, in particolare:

   a) i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, tranne i casi cui si applica l'articolo 5 della direttiva 2016/943 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti;

   b) l'efficace attuazione del presente regolamento, in particolare per quanto riguarda ispezioni, indagini e audit; c) gli interessi di sicurezza pubblica e nazionale;

   c) l'integrità del procedimento penale o amministrativo.

2. Fatto salvo il paragrafo 1, nel momento in cui i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, sono utilizzati dalle autorità di contrasto o dalle autorità competenti in materia di immigrazione o di asilo, le informazioni scambiate in via riservata tra le autorità nazionali competenti e tra le autorità nazionali competenti e la Commissione non sono divulgate senza previa consultazione dell'autorità nazionale competente e dell'utente che hanno prodotto tali informazioni, qualora tale divulgazione rischi di compromettere gli interessi pubblici e di sicurezza nazionale.

   Qualora le autorità di contrasto o le autorità competenti in materia di immigrazione o di asilo siano fornitori di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, la documentazione tecnica di cui all'allegato IV rimane nei locali di tali autorità. Tali autorità garantiscono che le autorità di vigilanza del mercato di cui all'articolo 63, paragrafi 5 e 6, a seconda dei casi, possano, su richiesta, accedere immediatamente alla documentazione o ottenerne una copia. Solo il personale dell'autorità di vigilanza del mercato in possesso di un nulla osta di sicurezza di livello adeguato è autorizzato ad accedere a tale documentazione o a una copia della stessa.

3. I paragrafi 1 e 2 non pregiudicano i diritti e gli obblighi della Commissione, degli Stati membri e degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, né gli obblighi delle parti interessate di fornire informazioni a norma del diritto penale degli Stati membri.

4. La Commissione e gli Stati membri possono scambiare, ove necessario, informazioni riservate con le autorità di regolamentazione dei paesi terzi con i quali abbiano concluso accordi di riservatezza, bilaterali o multilaterali, che garantiscano un livello di riservatezza adeguato.

Articolo 71
Sanzioni

1. Nel rispetto dei termini e delle condizioni di cui al presente regolamento, gli Stati membri stabiliscono le regole relative alle sanzioni, comprese le sanzioni amministrative pecuniarie, applicabili in caso di violazione del presente regolamento e adottano tutte le misure necessarie per garantirne un'attuazione corretta ed efficace. Le sanzioni previste sono effettive, proporzionate e dissuasive. Esse tengono conto in particolare degli interessi dei fornitori di piccole dimensioni e delle start-up e della loro sostenibilità economica.

2. Gli Stati membri notificano tali regole e misure alla Commissione e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

3. Le seguenti violazioni sono soggette a sanzioni amministrative pecuniarie fino a 30 000 000 di EUR o, se l'autore del reato è una società, fino al 6 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

   a) inosservanza del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5;

   b) non conformità del sistema di IA ai requisiti di cui all'articolo 10.

4. La non conformità del sistema di IA ai requisiti o agli obblighi previsti dal presente regolamento, diversi da quelli di cui agli articoli 5 e 10, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 di EUR o, se l'autore del reato è una società, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

5. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 di EUR o, se l'autore del reato è una società, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

6. Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:

   a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

   b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione;

   c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione.

7. Ciascuno Stato membro può prevedere regole che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. A seconda dell'ordinamento giuridico degli Stati membri, le regole in materia di sanzioni amministrative pecuniarie possono essere applicate in modo tale che le sanzioni pecuniarie siano inflitte dai tribunali nazionali competenti o da altri organismi, quali applicabili in tali Stati membri. L'applicazione di tali regole in tali Stati membri ha effetto equivalente.

Articolo 72

Sanzioni amministrative pecuniarie imposte a istituzioni, agenzie e organismi dell'Unione

1. Il Garante europeo della protezione dei dati può infliggere sanzioni amministrative pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento. Nel decidere se infliggere una sanzione amministrativa pecuniaria e nel determinarne l'importo in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:

   a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

   b) la cooperazione con il Garante europeo della protezione dei dati al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, compreso il rispetto delle misure precedentemente disposte dal Garante europeo della protezione dei dati nei confronti dell'istituzione, dell'agenzia o dell'organismo dell'Unione in relazione allo stesso tema;

   c) eventuali precedenti violazioni analoghe commesse dall'istituzione, dall'agenzia o dall'organismo dell'Unione;

2. Le seguenti violazioni sono soggette a sanzioni amministrative pecuniarie fino a 500 000 EUR:

   a) inosservanza del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5;

   b) non conformità del sistema di IA ai requisiti di cui all'articolo 10.

3. La non conformità del sistema di IA ai requisiti o agli obblighi previsti dal presente regolamento, diversi da quelli di cui agli articoli 5 e 10, è soggetta a sanzioni amministrative pecuniarie fino a 250 000 EUR.

4. Prima di adottare qualsiasi decisione a norma del presente articolo, il Garante europeo della protezione dei dati dà all'istituzione, all'agenzia o all'organismo dell'Unione oggetto del procedimento avviato dal Garante europeo della protezione dei dati l'opportunità di esprimersi in merito all'eventuale violazione. Il Garante europeo della protezione dei dati basa le sue decisioni solo sugli elementi e le circostanze in merito ai quali le parti interessate sono state poste in condizione di esprimersi. Gli eventuali ricorrenti sono strettamente associati al procedimento.

5. Nel corso del procedimento sono pienamente garantiti i diritti di difesa delle parti interessate. Esse hanno diritto d'accesso al fascicolo del Garante europeo della protezione dei dati, fermo restando l'interesse legittimo delle persone fisiche o delle imprese alla tutela dei propri dati personali o segreti aziendali.

6. I fondi raccolti mediante l'imposizione di sanzioni pecuniarie in forza del presente articolo entrano nel bilancio generale dell'Unione.

TITOLO XI

DELEGA DI POTERE E PROCEDURA DI COMITATO

Articolo 73
Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. La delega di potere di cui all'articolo 4, all'articolo 7, paragrafo 1, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, e all'articolo 48, paragrafo 5, è conferita alla Commissione per un periodo indeterminato a decorrere dal [*data di entrata in vigore del presente regolamento*].

3. La delega di potere di cui all'articolo 4, all'articolo 7, paragrafo 1, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6 e all'articolo 48, paragrafo 5, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

5. Qualsiasi atto delegato adottato a norma dell'articolo 4, dell'articolo 7, paragrafo 1, dell'articolo 11, paragrafo 3, dell'articolo 43, paragrafi 5 e 6 e dell'articolo 48, paragrafo 5, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 74
Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

TITOLO XII

DISPOSIZIONI FINALI

Articolo 75
Modifica del regolamento (CE) n. 300/2008

All'articolo 4, paragrafo 3, del regolamento (CE) n. 300/2008 è aggiunto il comma seguente:

"Nell'adottare misure dettagliate relative alle specifiche tecniche e alle procedure per l'approvazione e l'uso delle attrezzature di sicurezza per quanto concerne i sistemi di intelligenza artificiale ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 76
Modifica del regolamento (UE) n. 167/2013

All'articolo 17, paragrafo 5, del regolamento (UE) n. 167/2013 è aggiunto il comma seguente:

"Nell'adottare atti delegati a norma del primo comma per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 77
Modifica del regolamento (UE) n. 168/2013

All'articolo 22, paragrafo 5, del regolamento (UE) n. 168/2013 è aggiunto il comma seguente:

"Nell'adottare atti delegati a norma del primo comma per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 78
Modifica della direttiva 2014/90/UE

All'articolo 8 della direttiva 2014/90/UE è aggiunto il paragrafo seguente:

"4. Per i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, nello svolgimento delle sue attività a norma del paragrafo 1 e nell'adottare specifiche tecniche e norme di prova conformemente ai paragrafi 2 e 3, la Commissione tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 79
Modifica della direttiva (UE) 2016/797

All'articolo 5 della direttiva (UE) 2016/797 è aggiunto il paragrafo seguente:

"12. Nell'adottare atti delegati a norma del paragrafo 1 e atti di esecuzione a norma del paragrafo 11 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 80
Modifica del regolamento (UE) 2018/858

All'articolo 5 del regolamento (UE) 2018/858 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti delegati a norma del paragrafo 3 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 81
Modifica del regolamento (UE) 2018/1139

Il regolamento (UE) 2018/1139 è così modificato:

1) all'articolo 17 è aggiunto il paragrafo seguente:

"3. Fatto salvo il paragrafo 2, nell'adottare atti di esecuzione a norma del paragrafo 1 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [*sull'intelligenza artificiale*] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).";

2) all'articolo 19 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

3) all'articolo 43 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti di esecuzione a norma del paragrafo 1 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

4) all'articolo 47 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE)

YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

5) all'articolo 57 è aggiunto il paragrafo seguente:

"Nell'adottare tali atti di esecuzione per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale], si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

6) all'articolo 58 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.".

Articolo 82
Modifica del regolamento (UE) 2019/2144

All'articolo 11 del regolamento (UE) 2019/2144 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti di esecuzione a norma del paragrafo 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).".

Articolo 83
Sistema di IA già immessi sul mercato o messi in servizio

1. Il presente regolamento non si applica ai sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'allegato IX che sono stati immessi sul mercato o messi in servizio prima del *[12 mesi dopo la data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2]*, a meno che la sostituzione o la modifica di tali atti giuridici non comporti una modifica significativa della progettazione o della finalità prevista del sistema di IA o dei sistemi di IA interessati.

   Si tiene conto dei requisiti di cui al presente regolamento, ove applicabile, nella valutazione di ciascun sistema IT su larga scala istituito dagli atti giuridici elencati nell'allegato IX da effettuare come previsto in tali atti.

2. Il presente regolamento si applica ai sistemi di IA ad alto rischio, diversi da quelli di cui al paragrafo 1, che sono stati immessi sul mercato o messi in servizio prima del [*data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*], solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione o finalità prevista.

Articolo 84
Valutazione e riesame

1. La Commissione valuta la necessità di modificare l'elenco di cui all'allegato III una volta l'anno dopo l'entrata in vigore del presente regolamento.

2. Entro [*tre anni dalla data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*] e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento. Le relazioni sono rese pubbliche.

3. Le relazioni di cui al paragrafo 2 dedicano particolare attenzione ai seguenti aspetti:

   a) lo stato delle risorse finanziarie e umane necessarie alle autorità nazionali competenti per lo svolgimento efficace dei compiti loro assegnati a norma del presente regolamento;

   b) lo stato delle sanzioni, in particolare delle sanzioni amministrative pecuniarie di cui all'articolo 71, paragrafo 1, applicate dagli Stati membri in caso di violazione delle disposizioni del presente regolamento.

4. Entro [*tre anni dalla data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*] e successivamente ogni quattro anni, la Commissione valuta l'impatto e l'efficacia dei codici di condotta per la promozione dell'applicazione dei requisiti di cui al titolo III, capo 2, ed eventualmente di altri requisiti supplementari per i sistemi di IA diversi dai sistemi di IA ad alto rischio.

5. Ai fini dei paragrafi da 1 a 4, il comitato, gli Stati membri e le autorità nazionali competenti forniscono alla Commissione informazioni su sua richiesta.

6. Nello svolgere le valutazioni e i riesami di cui ai paragrafi da 1 a 4, la Commissione tiene conto delle posizioni e delle conclusioni del comitato, del Parlamento europeo, del Consiglio, nonché di altri organismi o fonti pertinenti.

7. Se necessario, la Commissione presenta opportune proposte di modifica del presente regolamento tenendo conto, in particolare, degli sviluppi delle tecnologie e alla luce dei progressi della società dell'informazione.

Articolo 85
Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Il presente regolamento si applica a decorrere dal [*24 mesi dopo l'entrata in vigore del regolamento*].

3. In deroga al paragrafo 2:

   a) il titolo III, capo 4, e il titolo VI si applicano a decorrere da [*tre mesi dopo l'entrata in vigore del presente regolamento*];

   b) l'articolo 71 si applica a decorrere dal [*12 mesi dopo l'entrata in vigore del regolamento*].

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati

1.3. La proposta/iniziativa riguarda:

1.4. Obiettivi

1.4.1. Obiettivi generali

1.4.2. Obiettivi specifici

1.4.3. Risultati e incidenza previsti

1.4.4. Indicatori di prestazione

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

1.5.3. Insegnamenti tratti da esperienze analoghe

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

1.6. Durata e incidenza finanziaria della proposta/iniziativa

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione

1.2. Settore/settori interessati

Reti di comunicazione, contenuti e tecnologia.

Mercato interno, industria, imprenditoria e PMI.

L'incidenza sul bilancio riguarda i nuovi compiti affidati alla Commissione, compreso il sostegno al comitato europeo per l'intelligenza artificiale.

Attività: plasmare il futuro digitale dell'Europa.

1.3. La proposta/iniziativa riguarda:

X **una nuova azione**

☐ **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[64]

☐ **la proroga di un'azione esistente**

☐ **un'azione reindirizzata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi generali

L'obiettivo generale dell'intervento consiste nell'assicurare il corretto funzionamento del mercato unico creando le condizioni per lo sviluppo e l'utilizzo di intelligenza artificiale affidabile nell'Unione.

1.4.2. Obiettivi specifici

Obiettivo specifico 1

Fissare requisiti specifici per i sistemi di IA e obblighi per tutti i partecipanti alla catena del valore al fine di assicurare che i sistemi di IA immessi sul mercato e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione.

Obiettivo specifico 2

Assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'IA chiarendo quali requisiti essenziali, obblighi e procedure di conformità e rispetto dei requisiti debbano essere rispettati per l'immissione o l'utilizzo di un sistema di IA sul mercato dell'Unione.

Obiettivo specifico 3

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

[64] A norma dell'articolo 54, paragrafo 2, lettera a) o b), del regolamento finanziario.

mettendo a disposizione nuovi poteri, risorse e regole chiare per le autorità competenti in materia di valutazione della conformità e procedure di monitoraggio ex post nonché di divisione dei compiti di governance e controllo tra il livello nazionale e quello dell'UE.

Obiettivo specifico 4

Facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato intervenendo a livello dell'Unione per fissare requisiti minimi per i sistemi di IA che saranno immessi e utilizzati sul mercato dell'Unione nel rispetto della normativa vigente in materia di diritti fondamentali e sicurezza.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

I fornitori di IA dovrebbero trarre beneficio da una serie minima ma chiara di requisiti, che creano certezza del diritto e assicurano l'accesso all'intero mercato unico.

Gli utenti di IA dovrebbero beneficiare della certezza del diritto in merito al fatto che i sistemi di IA ad alto rischio che essi acquistano rispettano le normative e i valori europei.

I consumatori dovrebbero trarre vantaggio dalla riduzione del rischio di violazioni della loro sicurezza o dei loro diritti fondamentali.

1.4.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare l'attuazione della proposta/iniziativa.

Indicatore 1

Numero di incidenti gravi o prestazioni dell'IA che costituiscono un incidente grave o una violazione degli obblighi relativi ai diritti fondamentali (semestrale) per ambiti di applicazione e calcolati: a) in termini assoluti; b) come percentuale rispetto alle applicazioni distribuite; c) come percentuale di cittadini interessati.

Indicatore 2

a) Investimento totale nell'IA nell'UE (annuale)

b) Investimento totale nell'IA per Stato membro (annuale)

c) Percentuale di imprese che utilizzano l'IA (annuale)

d) Percentuale di PMI che utilizzano l'IA (annuale)

a) e b) saranno calcolati sulla base di fonti ufficiali e confrontati con stime private

c) e d) saranno dati raccolti mediante sondaggi aziendali periodici

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

Il regolamento dovrebbe essere pienamente applicabile un anno e mezzo dopo la sua adozione. Tuttavia gli elementi della struttura di governance dovrebbero essere posti in essere prima di tale data. In particolare, gli Stati membri devono aver nominato le autorità esistenti e/o istituito nuove autorità incaricate di svolgere i compiti previsti in precedenza dalla normativa ed è opportuno che il comitato europeo per l'intelligenza artificiale sia istituito e reso operativo. Entro la data di inizio dell'applicabilità, la banca dati europea dei sistemi di IA dovrebbe essere pienamente operativa. Parallelamente al processo di adozione, è pertanto necessario sviluppare la banca dati, affinché il suo sviluppo sia concluso al momento dell'entrata in vigore del regolamento.

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione

che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

Il formarsi di un quadro frammentario di regole nazionali potenzialmente divergenti ostacolerà la fornitura senza soluzione di continuità di sistemi di IA in tutta l'UE ed è inefficace nel garantire la sicurezza e la protezione dei diritti fondamentali e dei valori dell'Unione nei diversi Stati membri. Un'azione legislativa comune dell'UE in materia di IA potrebbe promuovere il mercato interno e presenta un notevole potenziale per fornire all'industria europea un vantaggio competitivo sulla scena globale oltre a economie di scala che non possono essere conseguite individualmente dai singoli Stati membri.

1.5.3. Insegnamenti tratti da esperienze analoghe

La direttiva 2000/31/CE sul commercio elettronico costituisce il quadro principale per il funzionamento del mercato unico e la vigilanza sui servizi digitali e offre una struttura di base per un meccanismo di cooperazione generale tra gli Stati membri, contemplando in linea di principio tutti i requisiti applicabili ai servizi digitali. La valutazione della direttiva ha indicato carenze in vari elementi di tale meccanismo di cooperazione, tra cui importanti aspetti procedurali come la mancanza di termini chiari per le risposte degli Stati membri, oltre a una generale mancanza di reattività alle richieste delle controparti. Nel corso degli anni ciò ha determinato una mancanza di fiducia tra gli Stati membri nell'affrontare le preoccupazioni relative ai fornitori di servizi digitali transfrontalieri. Dalla valutazione della direttiva è emersa la necessità di definire una serie distinta di regole e requisiti a livello europeo. Per questo motivo, l'attuazione degli obblighi specifici previsti dal presente regolamento richiederebbe un meccanismo di cooperazione specifico a livello dell'UE, con una struttura di governance che assicuri il coordinamento di organismi responsabili specifici a livello dell'UE.

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

Il regolamento che stabilisce regole armonizzate sull'intelligenza artificiale e modifica taluni atti legislativi dell'Unione definisce un nuovo quadro comune di requisiti applicabili ai sistemi di IA, che va ben oltre il quadro previsto dalla legislazione in vigore. Per questo motivo è necessario istituire con la presente proposta una nuova funzione di regolamentazione e coordinamento a livello nazionale ed europeo.

Per quanto concerne le possibili sinergie con altri strumenti adeguati, il ruolo delle autorità di notifica a livello nazionale può essere svolto dalle autorità nazionali aventi funzioni analoghe a norma di altri regolamenti dell'UE.

Inoltre, aumentando la fiducia nei confronti dell'IA e quindi incoraggiando gli investimenti nello sviluppo e nell'adozione dell'IA, la presente proposta integra il programma Europa digitale, per il quale promuovere la diffusione di IA costituisce una delle cinque priorità.

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

Il personale sarà riassegnato. Gli altri costi saranno sostenuti dalla dotazione del programma Europa digitale dato che l'obiettivo del presente regolamento, ossia

assicurare un'IA affidabile, contribuisce direttamente a un obiettivo fondamentale di Europa digitale: accelerare lo sviluppo e la diffusione dell'IA in Europa.

1.6. Durata e incidenza finanziaria della proposta/iniziativa

☐ **durata limitata**

– ☐ in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ incidenza finanziaria dal AAAA al AAAA per gli stanziamenti di impegno e dal AAAA al AAAA per gli stanziamenti di pagamento

X **durata illimitata**

– Attuazione con un periodo di avviamento di uno/due (da definire) anni

– e successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[65]

X **Gestione diretta** a opera della Commissione

– ☐ a opera dei suoi servizi, compreso il suo personale presso le delegazioni dell'Unione

– ☐ a opera delle agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☐ **Gestione indiretta** affidando compiti di esecuzione del bilancio:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e loro agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☐ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V TUE e indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

[65] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

Il regolamento sarà riesaminato e valutato dopo cinque anni dall'entrata in vigore del regolamento. La Commissione riferirà i risultati della valutazione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo.

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

Il regolamento stabilisce una nuova politica per quanto riguarda le regole armonizzate per la fornitura di sistemi di intelligenza artificiale nel mercato interno, garantendo nel contempo il rispetto della sicurezza e dei diritti fondamentali. Tali nuove regole richiedono un meccanismo di coerenza per l'applicazione transfrontaliera degli obblighi previsti dal presente regolamento sotto forma di un nuovo gruppo consultivo che coordina le attività delle autorità nazionali.

Al fine di far fronte a tali nuovi compiti, è necessario fornire risorse adeguate ai servizi della Commissione. Si stima che l'applicazione del nuovo regolamento richieda 10 equivalenti a tempo pieno (ETP) a regime (5 ETP per il sostegno ad attività del comitato e 5 ETP per il Garante europeo della protezione dei dati che agisce in veste di organismo di notifica per i sistemi di IA implementati da un organismo dell'Unione europea).

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

Al fine di assicurare che i membri del comitato abbiano la possibilità di effettuare analisi informate sulla base di prove fattuali, è previsto che il comitato sia supportato dalla struttura amministrativa della Commissione e che sia creato un gruppo di esperti incaricato di fornire ulteriori competenze laddove richiesto.

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

Quanto alle spese per riunioni, dato il basso valore per transazione (ad esempio rimborso delle spese di viaggio per un delegato per una riunione), le procedure di controllo abituali paiono sufficienti. Per quanto concerne lo sviluppo della banca dati, per l'aggiudicazione del contratto è previsto un rigido sistema di controllo interno presso la DG CNECT mediante attività di appalto centralizzate.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Le vigenti misure di prevenzione delle frodi applicabili alla Commissione si applicheranno agli stanziamenti supplementari necessari per il presente regolamento.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero	Diss./Non diss.[66]	di paesi EFTA[67]	di paesi candidati[68]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
7	20 02 06 Spese amministrative	Non diss.	NO	NO	NO	NO
1	02 04 03 Programma Europa digitale intelligenza artificiale	Diss.	SÌ	NO	NO	NO
1	02 01 30 01 Spese di supporto per il programma Europa digitale	Non diss.	SÌ	NO	NO	NO

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista delle spese sugli stanziamenti operativi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi

– X La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

66 Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

67 EFTA: Associazione europea di libero scambio.

68 Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	1	

DG: CNECT				Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**[69]	**TOTALE**	
• Stanziamenti operativi											
Linea di bilancio[70] 02 04 03		Impegni	(1a)		1,000						**1,000**
		Pagamenti	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Linea di bilancio		Impegni	(1b)								
		Pagamenti	(2b)								
Stanziamenti amministrativi finanziati dalla dotazione di programmi specifici[71]											
Linea di bilancio 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
TOTALE stanziamenti per la DG CNECT		Impegni	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Pagamenti	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 Dati indicativi e a seconda della disponibilità di bilancio.

70 Secondo la nomenclatura di bilancio ufficiale.

71 Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

• TOTALE stanziamenti operativi	Impegni	(4)		1,000						**1,000**
	Pagamenti	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
TOTALE stanziamenti per la RUBRICA 1 del quadro finanziario pluriennale	Impegni	=4+6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Pagamenti	=5+6		0,840	0,340	0,340	0,340	0,340		**2,200**

Se la proposta/iniziativa incide su più rubriche, ricopiare nella sezione sotto:

• TOTALE stanziamenti operativi (tutte le rubriche operative)	Impegni	(4)								
	Pagamenti	(5)								
• TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici (tutte le rubriche operative)		(6)								
TOTALE stanziamenti per le RUBRICHE da 1 a 6 del quadro finanziario pluriennale (importo di riferimento)	Impegni	=4+6								
	Pagamenti	=5+6								

Rubrica del quadro finanziario pluriennale	7	"Spese amministrative"

Sezione da compilare utilizzando i "dati di bilancio di natura amministrativa" che saranno introdotti nell'allegato della scheda finanziaria legislativa (allegato V delle norme interne), caricato su DECIDE a fini di consultazione interservizi.

Mio EUR (al terzo decimale)

		Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**Dopo il 2027**[72]	**TOTALE**
DG: CNECT								
• Risorse umane		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Altre spese amministrative		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
TOTALE DG CNECT	**Stanziamenti**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Garante europeo della protezione dei dati								
• Risorse umane		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Altre spese amministrative								
TOTALE GEPD	**Stanziamenti**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
TOTALE stanziamenti per la RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

Mio EUR (al terzo decimale)

		Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**		**TOTALE**
TOTALE stanziamenti	Impegni		2,770	1,770	1,770	1,770	1,770		**9,850**

[72] Tutte le cifre in questa colonna sono indicative e soggette al proseguimento dei programmi e alla disponibilità degli stanziamenti.

per le RUBRICHE da 1 a 7 del quadro finanziario pluriennale	Pagamenti		2,370	1,870	1,870	1,870	1,870	**9,850**

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩			Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		Dopo il **2027**[73]		**TOTALE**	
	RISULTATI																	
	Tipo	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. total e	Costo totale
OBIETTIVO SPECIFICO 1[74]…																		
Banca dati					1	1,000	1		1		1		1		1	0,100	1	1,000
Riunioni - Risultato					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Attività di comunicazione					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Totale parziale obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2 ...																		
- Risultato																		
Totale parziale obiettivo specifico 2																		
TOTALE					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Tutte le cifre in questa colonna sono indicative e soggette al proseguimento dei programmi e alla disponibilità degli stanziamenti.

[74] Come descritto nella sezione 1.4.2. "Obiettivi specifici..."

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

– X La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**Ogni anno dopo il 2027**[75]	**TOTALE**
RUBRICA 7 del quadro finanziario pluriennale								
Risorse umane		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Altre spese amministrative		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Totale parziale RUBRICA 7 del quadro finanziario pluriennale		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**

Esclusa la RUBRICA 7[76] **del quadro finanziario pluriennale**								
Risorse umane								
Altre spese amministrative		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Totale parziale esclusa la RUBRICA 7 del quadro finanziario pluriennale		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**

TOTALE		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese amministrative è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

[75] Tutte le cifre in questa colonna sono indicative e soggette al proseguimento dei programmi e alla disponibilità degli stanziamenti.

[76] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.1. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– X La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

.		Anno **2023**	Anno **2024**	Anno **2025**	**2026**	**2027**	**Dopo il 2027**[77]	
• Posti della tabella dell'organico (funzionari e agenti temporanei)								
20 01 02 01 (sede e uffici di rappresentanza della Commissione)		10	10	10	10	10	10	
20 01 02 03 (delegazioni)								
01 01 01 01 (ricerca indiretta)								
01 01 01 11 (ricerca diretta)								
Altre linee di bilancio (specificare)								
• Personale esterno (in equivalenti a tempo pieno: ETP)[78]								
20 02 01 (AC, END e INT della dotazione globale)								
20 02 03 (AC, AL, END, INT e JPD nelle delegazioni)								
XX 01 xx **yy zz**[79]	- in sede							
	- nelle delegazioni							
01 01 01 02 (AC, END, INT - ricerca indiretta)								
01 01 01 12 (AC, END, INT - ricerca diretta)								
Altre linee di bilancio (specificare)								
TOTALE		**10**	**10**	**10**	**10**	**10**	**10**	

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Il Garante europeo della protezione dei dati dovrebbe fornire la metà delle risorse necessarie.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	Preparare un totale di 13-16 riunioni, redigere relazioni, portare avanti le attività strategiche, ad esempio per quanto concerne le future modifiche dell'elenco delle applicazioni di IA ad alto rischio, e mantenere le relazioni con le autorità degli Stati membri richiederà quattro AD ETP e 1 AST ETP. Per i sistemi di IA sviluppati dalle istituzioni dell'UE, è responsabile il Garante europeo della protezione dei dati. Sulla base dell'esperienza passata, si può stimare che siano necessari 5 AD ETP per adempiere le responsabilità del Garante europeo della protezione dei dati conformemente al progetto di legge.

[77] Tutte le cifre in questa colonna sono indicative e soggette al proseguimento dei programmi e alla disponibilità degli stanziamenti.

[78] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

[79] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

Personale esterno	

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

La proposta/iniziativa:

– X può essere interamente finanziata mediante riassegnazione all'interno della pertinente rubrica del quadro finanziario pluriennale (QFP).

Non è necessaria alcuna riprogrammazione.

– ☐ comporta l'uso del margine non assegnato della pertinente rubrica del QFP e/o l'uso degli strumenti speciali definiti nel regolamento QFP.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate, gli importi corrispondenti e gli strumenti proposti.

– ☐ comporta una revisione del QFP.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

– X non prevede cofinanziamenti da terzi

– ☐ prevede il cofinanziamento da terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno **N**[80]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE stanziamenti cofinanziati								

[80] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021) e così per gli anni a seguire.

3.3. Incidenza prevista sulle entrate

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

– ☐ su altre entrate

– ☐ su altre entrate

– indicare se le entrate sono destinate a linee di spesa specifiche ☐

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[81]						
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo …….								

Per quanto riguarda le entrate con destinazione specifica, precisare la o le linee di spesa interessate.

Altre osservazioni (ad es. formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni).

[81] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.