Consiglio regionale della Calabria

DOSSIER

PL n. 339/12
di iniziativa del Consigliere F. MANCUSO,P. CAPUTO,G. GELARDI,G. MATTIANI recante:
"Disposizioni concernenti l''impiego di sistemi di intelligenza artificiale in ambito regionale"
relatore: L. DE FRANCESCO;

DATI DELL'ITER	
NUMERO DEL REGISTRO DEI PROVVEDIMENTI	
DATA DI PRESENTAZIONE ALLA SEGRETERIA DELL'ASSEMBLEA	10/12/2024
DATA DI ASSEGNAZIONE ALLA COMMISSIONE	10/12/2024
COMUNICAZIONE IN CONSIGLIO	
SEDE	MERITO
PARERE PREVISTO	II Comm.
NUMERO ARTICOLI	

ultimo aggiornamento: 30/05/2025

Testo del Provvedimento

Proposta di legge n. 339/XII di iniziativa dei consiglieri regionali Mancuso, Caputo e Gelardi — pag. 3

Disposizioni concernenti l'impiego di sistemi di intelligenza artificiale in ambito regionale.

Normativa comunitaria

Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 — pag. 15

Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale

Normativa comparata

Regione Puglia - Legge regionale n. 4 del 14 aprile 2025 — pag. 159

Misure di promozione in materia di innovazione aperta e intelligenza artificiale e disposizioni varie

Regione Toscana - Legge regionale n. 57 del 9 dicembre 2024 — pag. 168

Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla L.R. 54/2009.

Regione Umbria - Legge regionale n. 25 del 4 novembre 2024 - Art. 16 — pag. 192

Modificazioni e integrazioni di leggi regionali per la semplificazione, la digitalizzazione e il taglio di adempimenti. Art. 16 Modificazioni all'articolo 1 della legge regionale 29 aprile 2014, n. 9.

Regione Campania - Legge regionale n. 6 del 15 maggio 2024 – Art. 17 — pag. 193

Ordinamento e organizzazione degli uffici della Giunta regionale. Art. 17 Istituzione degli Uffici Speciali.

Documentazione citata

Conferenza delle Regioni del 20 dicembre 2023 — pag. 195

Posizionamento sull'Intelligenza Artificiale delle Regioni e Province Autonome

Commissione Europea 19 febbraio 2020 - Libro Bianco sull'intelligenza artificiale — pag. 208

Un approccio europeo all'eccellenza e alla fiducia

Documentazione correlata

Regione Puglia Delibera di Giunta n. 1488 del 30 ottobre 2023 — pag. 238

Istituzione del Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione.

AGID Agenzia per l'Italia Digitale — pag. 246

Strategia italiana per l'intelligenza artificiale 2024-2026

Consiglio Regionale della Calabria

Proposta di legge recante:

"Disposizioni concernenti l'impiego di sistemi di intelligenza artificiale in ambito regionale"

[redacted]

I Consiglieri regionali

f.to Filippo Mancuso

f.to Pierluigi Caputo

F.to GIUSEPPE GELARDI

Proposta di legge recante: "Disposizioni concernenti l'impiego di sistemi di intelligenza artificiale in ambito regionale".

RELAZIONE ILLUSTRATIVA

Il termine intelligenza artificiale (IA) identifica una tecnica di apprendimento automatico, logico o deduttivo, in grado di replicare capacità umane, impiegata in qualsiasi tipologia di dispositivo o programma informatico. L'IA contribuisce a creare una serie di tecnologie basate sull'elaborazione di dati per giungere a determinare processi e procedure in grado di offrire benefici in campo industriale e sociale. L'uso dell'intelligenza artificiale può essere vantaggioso in termini sociali, economici e ambientali, ma presenta anche potenziali rischi per le persone e la società in termini di sicurezza dei dati e di relazioni sociali.

Anche l'Unione Europea si sta muovendo per assicurare che i cittadini europei possano beneficiare di nuove tecnologie come l'IA secondo i principi fondamentali dell'Unione e per questo ha intrapreso un percorso di regolazione dell'IA. Negli ultimi anni il tema dell'Intelligenza Artificiale è diventato sempre più centrale nel dibattito pubblico.

Fra le recenti normative europee di alto profilo, passibili di avere un impatto diretto e notevole sulle società e sulle economie europee, spicca l'Artificial Intelligence Act, una pietra miliare nel quadro delle proposte legislative orizzontali sull'intelligenza artificiale, applicabili cioè a tutti i sistemi di IA usati o immessi sul mercato nell'UE. L'AI Act ambisce senz'altro a proporsi come uno standard regolativo globale, di ispirazione per altre giurisdizioni, analogamente a quanto avvenuto con il GDPR.

Il Regolamento 2024/1689 sull'intelligenza artificiale (Artificial Intelligence Act, AI Act) è il punto di arrivo di un percorso apertosi con una Strategia europea sull'IA (2018), orientamenti etici elaborati da un gruppo di esperti ad alto livello (2019) e l'adozione di un Libro bianco sull'IA (2020) poi sottoposto a consultazione pubblica. Un Piano coordinato con gli Stati membri sull'IA (2018) è stato aggiornato nell'aprile 2021, quando la Commissione europea ha presentato la proposta di Regolamento. Raggiunto un accordo politico nel dicembre 2023, il Regolamento è stato adottato da Parlamento e Consiglio tra marzo e maggio 2024 ed è entrato in vigore il 1° agosto 2024.

L'AI Act si applica trasversalmente a tutti i sistemi di IA e segue un approccio "basato sul rischio" nei confronti della società: maggiore il rischio, più rigorose le regole. Distinti insiemi di regole si applicano quindi ai vari usi dell'IA secondo una loro classificazione per livelli di rischio (minimo, elevato, inaccettabile). Il rischio inaccettabile comporta una proibizione: ad esempio, sono vietati i sistemi di credito sociale, mentre l'identificazione biometrica remota in tempo reale è proibita con l'eccezione di casi di evidente minaccia di un attacco terroristico, ricerca di vittime o indagini su reati gravi da parte delle autorità degli Stati membri.

Considerate le evoluzioni tecnologiche intervenute dalla presentazione della proposta, soprattutto per quanto riguarda l'IA generativa, Parlamento e Consiglio hanno concordato nuove disposizioni rivolte ai sistemi di "IA per finalità generali" (general purpose AI, GPAI), anche noti come "modelli di base" (foundation models), vale a dire i grandi sistemi in grado di svolgere un'ampia gamma di compiti distintivi quali la generazione di video, testi, immagini. L'AI Act, oltre ad occuparsi di regolamentazione e ad istituire un nuovo quadro di governance europea, estende le misure a sostegno dell'innovazione e gli spazi di sperimentazione normativa (regulatory sandboxes).

Nel settembre 2022, la Commissione europea ha presentato una Direttiva sull'adeguamento delle norme sulla responsabilità civile extracontrattuale all'intelligenza artificiale (AI Liability Directive). La proposta mira a stabilire norme uniformi per l'accesso alle informazioni e l'alleggerimento dell'onere della prova in relazione ai danni causati dai sistemi di AI, garantendo una protezione più ampia per le vittime (persone fisiche o imprese) e contribuendo a maggiore fiducia verso l'AI.

Nel gennaio 2024 la Commissione ha presentato un pacchetto di misure per sostenere le start-up e le PMI europee nello sviluppo di un'IA affidabile tramite un accesso privilegiato alle capacità di supercalcolo europee.

La regolamentazione europea ha l'obiettivo di offrire regole per lo sviluppo, l'immissione sul mercato e l'utilizzo di sistemi di IA nell'Unione con un approccio proporzionato basato sul rischio, con lo scopo di garantire che lo sviluppo e l'utilizzo dell'IA in Europa siano pienamente conformi ai principi e ai valori dell'Unione Europea. Questi principi includono il controllo umano, la sicurezza, la privacy, la trasparenza, la non discriminazione e il benessere sociale e ambientale.

La regolamentazione europea dei sistemi di intelligenza artificiale mira al sostegno dell'innovazione mediante la previsione di uno spazio digitale sicuro di sperimentazione normativa, creando i presupposti per la definizione di un quadro giuridico anche da parte dei singoli Stati membri. Anche l'Onu si è mobilitata annunciando la formazione di un nuovo Ente che "raccoglierà le necessarie competenze" sull'intelligenza artificiale e "le metterà a disposizione della comunità internazionale".

Il G7 ha recentemente approvato un Codice di condotta internazionale sull'IA, a cui aziende e organizzazioni possono aderire su base volontaria.

Anche l'Italia, in linea con l'interesse dell'UE al tema, con il Programma Strategico "Intelligenza Artificiale" e la costituzione di un gruppo di lavoro permanente ha avviato azioni sull'intelligenza artificiale: in particolare, è stato evidenziato l'obiettivo degli interventi sulla Pubblica Amministrazione, volti alla creazione di infrastrutture dati sicure per l'utilizzo dei big data pubblici, alla semplificazione e personalizzazione dell'offerta dei servizi pubblici e all'innovazione delle amministrazioni. La Conferenza delle Regioni del 20 dicembre 2023, poi, ha espresso il proprio posizionamento in merito all'introduzione dell'Intelligenza artificiale all'interno del sistema pubblico elaborando proposte e indicando le seguenti regole: le Regioni possono contribuire a definire linee guida e normative specifiche per l'implementazione dell'AI e a darne una contestuale attuazione, anche in forma sperimentale, nel rispetto dei valori e delle specifiche esigenze delle comunità territoriali; le Regioni possono, inoltre, promuovere un approccio etico all'AI incoraggiando la collaborazione tra settore pubblico, privato e accademico per sviluppare soluzioni tecnologiche che rispettino standard e processi di digitalizzazione condivisi nei territori anche nell'ottica di abbattimento del digital divide; le Regioni, da ultimo, possono promuovere la creazione di registri pubblici relativi all'uso di algoritmi da parte delle Pubbliche Amministrazioni per garantire la trasparenza nel loro uso nei confronti dei cittadini.

Per i motivi sopra esposti, in attesa di un quadro regolatorio europeo e nazionale, con lo scopo di promuovere l'innovazione e consentire lo sviluppo nel territorio regionale dell'intelligenza artificiale e dei suoi possibili usi, appare urgente adottare la presente proposta di legge per una disciplina temporanea e sperimentale dell'ecosistema di intelligenza artificiale al fine di non arrivare impreparati al termine dei lavori legislativi. In quest'ottica, la presente proposta di legge regionale della Calabria, che si inserisce nel contesto attuale europeo e nazionale ed è ad invarianza finanziaria per il bilancio dell'Ente, mira a contribuire alla promozione, allo sviluppo, alla diffusione, all'incentivazione, alla formazione, all'utilizzo, all'informazione, alla regolamentazione dell'impiego di sistemi di intelligenza artificiale nel territorio locale, nelle more dell'entrata in vigore dell'AI Act europeo e dell'annunciata proposta di legge del Ministero dell'Innovazione.

A partire da questo scenario, la presente proposta di legge intende disciplinare e favorire l'utilizzo dell'IA in Calabria, con particolare attenzione alle società partecipate e con l'obiettivo di favorire la diffusione dell'IA nei diversi settori economici e sociali della regione. Inoltre, la Regione Calabria intende offrire, attraverso l'Ufficio regionale per l'IA, un punto di confronto e di individuazione di prospettive - e possibili soluzioni - basate sull'intelligenza artificiale, da rendere sistemiche a beneficio dell'intero apparato amministrativo.

La presente proposta di legge riguarda nel dettaglio:

- la creazione e istituzione di un registro regionale di persone fisiche e giuridiche (imprese, aziende, startup, spin off, associazioni, enti pubblici, Università, Istituti scolastici, etc etc) che si occupano di IA;

- il riconoscimento di premialità nei bandi di finanziamento regionale ai soggetti iscritti nel registro regionale;

- la istituzione di un Ufficio regionale per l'IA per il coordinamento, il monitoraggio, la promozione, il controllo, la diffusione, la promozione e l'informazione dei sistemi di IA. L'Ufficio regionale per l'IA sarà gestito dal competente Settore della Giunta regionale, parteciperanno di diritto i referenti dei soggetti iscritti al registro regionale, i garanti per la privacy di Giunta e Consiglio regionale, i referenti degli enti locali, delle istituzioni scolastiche di ogni ordine e grado, le associazioni di categoria nonché esperti nel campo dell'innovazione tecnologica. La partecipazione è a titolo gratuito. L'attività principale dell'Ufficio regionale per l'IA dovrà essere basata sulla diffusione dell'informazione e della conoscenza e della comprensione delle caratteristiche della tecnologia di IA per un suo utilizzo condiviso, sicuro, equo e responsabile.

La proposta, pertanto, mira a promuovere una governance responsabile e trasparente nell'adozione di questa tecnologia, garantendo al contempo il rispetto dei diritti e della privacy dei cittadini. La legge contribuisce all'obiettivo di Regione Calabria di essere leader nazionale nello sviluppo di un'IA sicura, affidabile ed etica, come dichiarato e richiesto dal Consiglio e dal Parlamento europeo, e garantisce la tutela dei principi etici.

.La proposta si compone di 9 articoli, di seguito descritti:

L'Articolo 1 definisce l'oggetto e le finalità della legge.

L'Articolo 2 contiene definizioni generali del sistema di IA in armonia con quanto ipotizzato anche a livello europeo.

L'Articolo 3 individua alcune azioni per la promozione di sistemi di IA affidabili e sicuri.

L'Articolo 4 istituisce il Registro regionale dei soggetti che utilizzano sistemi di IA affidabili, per come previsto nella Conferenza delle Regioni del 20 dicembre 2023.

L'Articolo 5 istituisce l'Ufficio regionale per l'IA per il monitoraggio dei sistemi di IA affidabile.

L'Articolo 6 definisce le attività dell' Ufficio regionale per l'IA.

L'Articolo 7 prevede la clausola valutativa.

L'articolo 8 contiene una norma di rinvio alla normativa unionale e statale vigente in materia di IA.

L'art. 9 prevede l'invarianza finanziaria di tale proposta di legge regionale, in considerazione della sua natura squisitamente ordinamentale in quanto alle attività di promozione, alla istituzione del Registro regionale e all'attività di coordinamento dei lavori dell' Ufficio regionale per l'IA si farà fronte con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Relazione tecnico-finanziaria

La presente proposta di legge reca disposizioni di carattere ordinamentale che non comportano nuovi o maggiori oneri finanziari per il bilancio regionale in quanto tutte le attività di promozione sono svolte dal dipartimento regionale competente con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Come specificato dalla clausola di invarianza finanziaria di cui all'articolo 9 all'attuazione della legge di cui alla presente legge si provvede nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico del bilancio regionale.

In particolare:

- il personale che gestisce il Registro regionale di cui all'articolo 4 è individuato nell'ambito della dotazione organica della Regione Calabria, senza nuovi o maggiori oneri a carico del bilancio regionale;

- analogamente senza nuovi o maggiori oneri a carico del bilancio regionale sono le attività di coordinamento dei lavori dell'Ossevatorio regionale e le attività di cui alla clausola valutativa, svolte dal personale regionale.

Quadro di riepilogo analisi economico finanziaria

Titolo: "Disposizioni concernenti l'impiego di sistemi di intelligenza artificiale in ambito regionale".

Tab. l - Oneri finanziari:

Articolo	Descrizione spese	Tipologia I o C	Carattere Temporale A o P	Importo
1	Definisce l'oggetto e le finalità della legge. Ha carattere ordinamentale.	//	//	//
2	Contiene definizioni generali di IA in armonia con quanto ipotizzato	//	//	//

	anche a livello europeo. Ha carattere ordinamentale.			
3	Individua alcune azioni per la promozione di sistemi di IA affidabili e sicuri.Non comporta nuovi oneri in quanto le attività sono svolte dal dipartimento competente con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.	//	//	//
4	Istituisce il Registro regionale dei soggetti che utilizzano sistemi di IA affidabili, per come previsto nella Conferenza delle Regioni del 20 dicembre 2023. Il Registro è istituito e gestito dal personale del dipartimento regionale competente, senza nuovi o maggiori oneri.	//	//	//
5	Istituisce l'Ufficio regionale per l'IA per il monitoraggio dei sistemi di IA affidabile. La partecipazione ai lavori è gratuita e le riunioni si svolgono in modalità web conference. Il coordinamento dei lavori è effettuato a cura del dipartimento regionale competente, senza nuovi o maggiori oneri a carico del bilancio regionale.	//	//	//
6	Definisce le attività che l'Ufficio regionale per l'IA svolge senza nuovi o maggiori oneri a carico del bilancio regionale.	//	//	//
7	Prevede il monitoraggio dell'attuazione della presente legge da parte del dipartimento regionale competente senza nuovi o maggiori a carico del bilancio regionale.	//	//	//
8	Contiene una norma di rinvio alla normativa unionale e statale vigente in materia di IA. Ha carattere ordinamentale.	//	//	//
9	Prevede l'invarianza finanziaria di tale proposta di legge regionale, in quanto le attività di promozione regionale, di istituzione e gestione del Registro, di costituzione e coordinamento dei lavori dell'Ufficio regionale per l'IA e di monitoraggio dell'attuazione della legge, sono effettuate senza nuovi o maggiori oneri a carico del bilancio regionale avvalendosi delle risorse	//	//	//

	umane, strumentali e finanziarie disponibili a legislazione vigente.			

Criteri di quantificazione degli oneri finanziari

Atteso che la presente legge reca disposizioni che non implicano nuovi o maggiori oneri finanziari per il bilancio regionale, non vengono esplicitati i criteri di quantificazione.

Tab. 2 Copertura finanziaria:

Indicare nella Tabella 2 il Programma e/o capitolo del bilancio di copertura degli oneri finanziari indicate nella tabella l.

Programma/ Capitolo	Anno 2024	Anno 2025	Anno 2026	Totale
//	//	//	//	//
Totale	//	//	//	//

"Disposizioni concernenti l'impiego di sistemi di intelligenza artificiale in ambito regionale".

Art. 1

(Oggetto e finalità)

1. La presente legge, nel rispetto delle competenze e della normativa unionale e statale di settore, reca disposizioni concernenti l'impiego di sistemi di intelligenza artificiale (IA) presso la pubblica amministrazione regionale, anche con riguardo ai rischi associati all'utilizzo di tale tecnologia, nonché in materia di politiche regionali sull'impiego dell'IA, in modo affidabile e conforme alle libertà e ai diritti fondamentali della persona.

2. La Regione Calabria promuove l'adozione responsabile di sistemi di IA presso la pubblica amministrazione regionale anche per migliorare la qualità dei servizi offerti ai cittadini.

3. Tutti i sistemi basati sull'IA utilizzati dall'amministrazione regionale devono rispettare le normative vigenti in materia di protezione dei dati personali e sicurezza informatica e devono essere soggetti a revisione umana nel rispetto dei principi di trasparenza, responsabilità ed equità.

4. La Regione Calabria riconosce le opportunità derivanti dall'impiego di sistemi di IA affidabile e persegue la programmazione coordinata di sviluppo e di utilizzo di sistemi di IA in ambito regionale, nel rispetto delle norme etiche e di quelle vigenti in materia di protezione dei dati, dei diritti digitali e della sicurezza informatica.

Art. 2

(Definizioni)

1. Ai fini della presente legge si intende per sistema di IA un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

2. Un sistema di intelligenza artificiale è considerato affidabile se rispetta, sia nei requisiti di progettazione sia nella modalità di funzionamento, la normativa unionale e statale vigente in materia, se è soggetto a supervisione umana, intesa come capacità di intervento dell'uomo in tutte le fasi del funzionamento del sistema e se garantisce la propria verificabilità, intesa come la possibilità di valutare algoritmi, dati e processi di progettazione utilizzati.

Art. 3

(Promozione di sistemi di IA affidabile)

1. La Regione promuove lo sviluppo e l'adozione di sistemi di IA affidabile basati sulla prevenzione dei rischi connessi al loro utilizzo e, in particolare, promuove:

a) l'impiego di tecnologie digitali per migliorare la fruizione dei servizi erogati in favore del cittadino nel rispetto del principio di buon andamento dell'amministrazione regionale;

b) attività e iniziative di organizzazioni pubbliche e private che contribuiscono a diffondere l'utilizzo di sistemi di IA affidabile;

c) programmi e corsi di formazione in materia di uso dei dati conforme alla normativa vigente in materia di protezione dei dati personali e sicurezza informatica, al fine di garantire una corretta comprensione e gestione della tecnologia di IA;

d) campagne di sensibilizzazione su rischi e opportunità legate all'utilizzo dell'IA nella pubblica amministrazione regionale.

2. All'attuazione delle finalità di cui al comma 1 provvede la Giunta regionale, nei limiti delle risorse disponibili a legislazione vigente.

Art. 4

(Registro regionale dei soggetti che utilizzano sistemi di IA affidabili)

1. Entro sessanta giorni dall'entrata in vigore della presente legge, allo scopo di monitorare i sistemi di IA affidabile in uso in ambito regionale e assicurare la prestazione di un sistema adeguato e conforme alla normativa di settore vigente, è istituito, presso il dipartimento regionale competente in materia di transizione digitale, il Registro regionale dei soggetti che realizzano, sperimentano ovvero fanno uso di sistemi di gestione di IA affidabili, di seguito indicato come Registro.

2. La Regione, al fine di promuovere l'implementazione nel territorio regionale dei sistemi di IA affidabile, può prevedere il riconoscimento di premialità nei bandi di finanziamento regionale ai soggetti iscritti nel Registro.

3. Il Registro è istituito e gestito senza nuovi oneri a carico del bilancio regionale, con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

4. La Giunta regionale adotta, entro sei mesi dalla entrata in vigore della presente legge e senza oneri aggiuntivi per il bilancio regionale, il regolamento per definire le modalità di istituzione, iscrizione, aggiornamento e gestione del Registro.

.

Art. 5

(Ufficio regionale per l'IA)

1. È istituito, senza oneri aggiuntivi per il bilancio regionale, presso il dipartimento regionale competente in materia di transizione digitale, l'Ufficio regionale per l'IA quale centro delle competenze in materia di IA in tutta la Calabria. Svolge un ruolo chiave nell'attuazione della presente legge, in particolare per l'IA generica, promuovendo lo sviluppo e l'uso di un sistema di IA affidabile e si relaziona con l'Ufficio europeo per l'IA e con analoghi organismi e osservatori istituiti a livello

regionale e statale. Garantisce un approccio regionale strategico con compiti di monitoraggio e coordinamento dei sistemi di IA affidabile in ambito regionale.

Fanno parte dell'Ufficio regionale per l'IA:

a) il dirigente generale del dipartimento regionale competente in materia di transizione digitale, o suo delegato, con funzioni di presidente;

b) tre rappresentanti designati dalle associazioni delle imprese operanti nel settore dell'intelligenza artificiale;

d) tre esperti provenienti dalle Università della Calabria, designati da queste ultime, su invito della Regione;

e) tre esperti designati da centri di ricerca in materia di intelligenza artificiale;

f) garanti per la privacy e responsabili Open data di Giunta e Consiglio regionale.

2. Alle sedute dell'Ufficio regionale per l'IA partecipano di diritto i referenti dei soggetti iscritti al Registro regionale di cui all'articolo 4, i referenti degli enti locali e delle istituzioni scolastiche di ogni ordine e grado nonché rappresentanti di categorie di portatori di interesse in relazione agli argomenti iscritti all'ordine del giorno.

3. Le sedute dell'Ufficio regionale per l'IA si svolgono in modalità web conference. La partecipazione ai lavori è a titolo gratuito e non dà diritto alla corresponsione di alcun compenso, indennità, emolumento comunque denominato, né rimborso spese di qualsiasi genere.

Art. 6

(Attività dell'Ufficio regionale per l'IA)

1. L'Ufficio regionale per l'IA, attraverso il coinvolgimento, tramite appositi accordi, dell'Agenzia per l'Italia Digitale, svolge le seguenti attività:

a) indagare, analizzare, comprendere, monitorare e valutare tutte le implicazioni etiche, normative, infrastrutturali, economiche e la sostenibilità di applicazioni, sistemi, strumenti e soluzioni di IA nella pubblica amministrazione regionale;

b) sperimentare l'utilizzo di applicazioni, sistemi, strumenti e soluzioni di IA in ambito regionale, all'interno di processi e sistemi dell'Ente, coinvolgendo, allo scopo, anche la Rete di responsabili della transizione al digitale delle agenzie e delle in house regionali.

c) contribuire alla definizione degli obiettivi e delle strategie di medio e lungo periodo della Regione nella promozione dell'utilizzo dei sistemi di IA;

d) proporre soluzioni per l'adozione di sistemi di IA affidabile da parte degli operatori economici;

e) raccogliere e divulgare studi e ricerche riguardanti politiche e buone pratiche realizzate a livello regionale, nazionale e internazionale sul riconoscimento dei benefici economico-sociali derivanti dall'uso di IA affidabile;

f) promuovere l'inserimento, nel programma formativo delle strutture amministrative di Giunta e Consiglio regionale, di attività formative finalizzate alla corretta comprensione e gestione dell'IA in ambito regionale;

g) diffondere l'informazione e la conoscenza delle caratteristiche della tecnologia di IA per un suo utilizzo condiviso, sicuro, equo e responsabile;

h) recepire proposte per l'utilizzo dell'IA da parte di portatori di pubblico interesse al fine di consolidare una innovazione partecipata nel campo dell'IA nell'interesse della collettività;

i) individuare le particolarità e le esigenze nell'ambito di settori strategici locali al fine di promuovere attività di ricerca e sviluppo (R&D), industrializzazione e formazione di nuovi prodotti o servizi di IA con particolare riferimento ai seguenti settori: manifatturiero, educativo e formativo, agroalimentare, culturale e turistico, e-health, ambientale;

j) promuovere e diffondere l'impiego di IA nella pubblica amministrazione regionale e negli enti locali calabresi favorendo la collaborazione tra gli stessi, i soggetti iscritti nel Registro regionale di cui all'articolo 4, soggetti terzi con sede nel territorio nazionale o internazionale, ai fini anche della sperimentazione di nuovi prodotti o servizi per sostenere nuove tipologie di IA in ambito istituzionale;

k) creare una rete regionale pubblico/privato per creare uno spazio digitale di sperimentazione in qualsiasi settore di interesse;

l) promuovere attività volte alla forma sperimentale, nel rispetto dei valori e delle specifiche esigenze delle comunità territoriali;

m) promuovere un approccio etico all'IA incoraggiando la collaborazione tra settore pubblico, privato e accademico per sviluppare soluzioni tecnologiche che rispettano standard e processi di digitalizzazione condivisi nei territori anche nell'ottica di abbattimento del digital divide;

n) promuovere la produzione di leggi di qualità in grado di creare valore pubblico intergenerazionale con l'analisi preventiva dell'outcome raggiungibile inteso come incremento congiunto ed equilibrato del benessere economico, sociale, educativo, assistenziale, ambientale a favore dei cittadini e delle aziende;

o) promuovere attività volte alla creazione di infrastrutture dati sicure per l'utilizzo dei big data pubblici, alla semplificazione e personalizzazione dell'offerta dei servizi pubblici e all'innovazione dell'amministrazione regionale.

2. L'Ufficio regionale per l'IA elabora una relazione annuale da trasmettere alla Giunta regionale e al Consiglio regionale contenente osservazioni, dati e materiale utile all'analisi dello stato di avanzamento della promozione e dell'introduzione dei sistemi di IA in Calabria.

Art. 7

(Clausola valutativa)

1. Il Consiglio regionale valuta l'attuazione della presente legge e i risultati progressivamente ottenuti nel favorire l'implementazione dei sistemi di IA affidabile e il contrasto dei sistemi di IA ad alto rischio. A questo scopo, entro il 31 marzo dell'anno successivo a quello di approvazione della presente legge, la Giunta regionale trasmette al Consiglio una relazione che descrive e documenta:

a) gli interventi realizzati, specificandone gli ambiti, gli obiettivi, i soggetti coinvolti e le loro caratteristiche;

b) in che misura la Regione ha eventualmente finanziato gli interventi realizzati e in che modo tali risorse risultano distribuite sul territorio regionale e fra i soggetti coinvolti;

c) quali punti di forza e di debolezza si sono riscontrati nel corso dell'attuazione degli interventi.

2. Successivamente, con cadenza biennale al 31 marzo, la Giunta regionale trasmette al Consiglio una relazione che, oltre alle informazioni di cui al comma 1, comprende una sezione che documenta e descrive i risultati conseguiti.

3. Gli esiti delle attività dell'Ufficio regionale per l'IA sono parte integrante della relazione al Consiglio.

4. Il Presidente del Consiglio regionale può audire in qualsiasi momento i membri dell'Ufficio regionale per l'IA per operare il monitoraggio continuo e circolare dei target intermedi raggiunti e può proporre l'inserimento di meccanismi di calibrazione per sperimentare processi innovativi ibridi con verifica e valutazione congiunta da parte di tutti i soggetti interessati nonché la previsione di ulteriori attività finalizzate al raggiungimento dello scopo della presente legge.

5. La Giunta regionale rende accessibili, sul proprio sito istituzionale in formato aperto, i dati e le informazioni raccolte per le attività valutative previste dalla presente legge.

6. Il Consiglio regionale rende pubblici, sul proprio sito istituzionale in formato aperto, i documenti che concludono l'esame svolto, unitamente alla relazione che ne è stata oggetto e formula indirizzi vincolanti rispetto alla implementazione delle misure e del livello di integrazione degli interventi.

Art. 8

(Norma di rinvio)

1. Per tutto quanto non espressamente previsto dalla presente legge, si applicano le disposizioni di leggi unionali e statali in materia di protezione di dati e di IA.

Art. 9

(Clausola di invarianza degli oneri finanziari)

1. All'attuazione della presente legge si provvede nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico del bilancio regionale.

F.to Filippo Mancuso

F.to Pierluigi Caputo

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 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 a fini di attività di contrasto, dell'uso dei sistemi di IA per le valutazione dei rischi delle persone fisiche a fini di attività di contrasto e dell'uso dei sistemi di IA di categorizzazione biometrica 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.

(4) L'IA consiste in una famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'IA, 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 e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi.

(5) L'IA può nel contempo, a seconda delle circostanze relative alla sua applicazione, al suo utilizzo e al suo livello di sviluppo tecnologico specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale, compreso il pregiudizio fisico, psicologico, sociale o economico.

(6) In considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani.

(7) 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 regole comuni per i sistemi di IA ad alto rischio. Tali regole dovrebbero essere coerenti con la Carta, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Dovrebbero inoltre tenere conto della dichiarazione europea sui diritti e i principi digitali per il decennio digitale e degli orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG).

(8) Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, come riconosciuti e tutelati dal diritto dell'Unione. Per conseguire tale obiettivo, è opportuno stabilire regole che disciplinino l'immissione sul mercato, la messa in servizio e l'uso 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. Tali norme dovrebbero essere chiare e solide nel tutelare i diritti fondamentali, sostenere nuove soluzioni innovative e consentire un ecosistema europeo di attori pubblici e privati che creino sistemi di IA in linea con i valori dell'Unione e sblocchino il potenziale della trasformazione digitale in tutte le regioni dell'Unione. Stabilendo tali regole nonché le misure a sostegno dell'innovazione, con particolare attenzione alle piccole e medie imprese (PMI), comprese le start-up, il presente regolamento contribuisce all'obiettivo di promuovere l'approccio antropocentrico europeo all'IA ed essere un leader mondiale nello sviluppo di un'IA sicura, affidabile ed etica, come affermato dal Consiglio europeo ([5]), e garantisce la tutela dei principi etici, come specificamente richiesto dal Parlamento europeo ([6]).

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

(9) È opportuno che le norme armonizzate 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 ([7]), alla decisione n, 768/2008/CE del Parlamento europeo e del Consiglio ([8]) e al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio ([9]) («nuovo quadro legislativo»). Le norme armonizzate stabilite nel presente regolamento dovrebbero applicarsi in tutti i settori e, in linea con il nuovo quadro legislativo, non dovrebbero pregiudicare il vigente diritto dell'Unione, in particolare in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione e protezione dei lavoratori e sicurezza dei prodotti, al quale il presente regolamento è complementare. Di conseguenza, restano impregiudicati e pienamente applicabili tutti i diritti e i mezzi di ricorso previsti da tali disposizioni di diritto dell'Unione a favore dei consumatori e delle altre persone su cui i sistemi di IA possono avere un impatto negativo, anche in relazione al risarcimento di eventuali danni a norma della direttiva 85/374/CEE del Consiglio ([10]). Inoltre, nel contesto dell'occupazione e della protezione dei lavoratori, il presente regolamento non dovrebbe pertanto incidere sul diritto dell'Unione in materia di politica sociale né sul diritto del lavoro nazionale, in conformità del diritto dell'Unione, per quanto riguarda le condizioni di impiego e le condizioni di lavoro, comprese la salute e la sicurezza sul luogo di lavoro, e il rapporto tra datori di lavoro e lavoratori. Il presente regolamento non dovrebbe inoltre pregiudicare l'esercizio dei diritti fondamentali riconosciuti dagli Stati membri e a livello di Unione, compresi il diritto o la libertà di sciopero o il diritto o la libertà di intraprendere altre azioni contemplate dalla disciplina delle relazioni industriali negli Stati membri nonché il diritto di negoziare, concludere ed eseguire accordi collettivi, o di intraprendere azioni collettive in conformità del diritto nazionale. Il presente regolamento dovrebbe lasciare impregiudicate le disposizioni volte a migliorare le condizioni di lavoro nel lavoro mediante piattaforme digitali di cui alla direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali. Inoltre, il presente regolamento mira a rafforzare l'efficacia di tali diritti e mezzi di ricorso esistenti definendo requisiti e obblighi specifici, anche per quanto riguarda la trasparenza, la documentazione tecnica e la conservazione delle registrazioni dei sistemi di IA. Oltre a ciò, gli obblighi imposti a vari operatori coinvolti nella catena del valore dell'IA a norma del presente regolamento dovrebbero applicarsi senza pregiudizio del diritto nazionale, in conformità del diritto dell'Unione, e avere l'effetto di limitare l'uso di determinati sistemi di IA qualora tale diritto non rientri nell'ambito di applicazione del presente regolamento o persegua obiettivi legittimi di interesse pubblico diversi da quelli perseguiti dal presente regolamento. Ad esempio, il presente regolamento non dovrebbe incidere sulla normativa nazionale in materia di lavoro e sulla normativa in materia di protezione dei minori, ossia le persone di età inferiore ai 18 anni, tenendo conto del commento generale n, 25 della Convenzione sui diritti dell'infanzia e dell'adolescenza (2021) sui diritti dei minori in relazione all'ambiente digitale, nella misura in cui esse non riguardino in modo specifico i sistemi di IA e perseguano altri obiettivi legittimi di interesse pubblico.

(10) Il diritto fondamentale alla protezione dei dati personali è garantito in particolare dai regolamenti (UE) 2016/679 ([11]) e (UE) 2018/1725 ([12]) del Parlamento europeo e del Consiglio e dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([13]). La direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([14]) tutela inoltre la vita privata e la riservatezza delle comunicazioni, in particolare stabilendo le condizioni per l'archiviazione di dati personali e non personali e l'accesso ai dati in apparecchi terminali. Tali atti giuridici dell'Unione costituiscono la base per un trattamento sostenibile e responsabile dei dati, anche nei casi in cui gli insiemi di dati comprendono una combinazione di dati personali e non personali. Il presente regolamento non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti. Inoltre, lascia impregiudicati gli obblighi dei fornitori e dei deployer dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento derivanti dal diritto dell'Unione o nazionale in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali. È inoltre

([7]) Regolamento (CE) n, 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e che abroga il regolamento (CEE) n, 339/93 (GU L 218 del 13.8.2008, pag. 30).

([8]) 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).

([9]) 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).

([10]) Direttiva 85/374/CEE del Consiglio, del 25 luglio 1985, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi (GU L 210 del 7.8.1985, pag. 29).

([11]) 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).

([12]) 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).

([13]) 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 (GU L 119 del 4.5.2016, pag. 89).

([14]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

opportuno chiarire che gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti da tale diritto dell'Unione, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione. Norme armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA istituiti a norma del presente regolamento dovrebbero facilitare l'efficace attuazione e consentire l'esercizio dei diritti degli interessati e di altri mezzi di ricorso garantiti dal diritto dell'Unione in materia di protezione dei dati personali nonché degli altri diritti fondamentali.

(11) Il presente regolamento non dovrebbe pregiudicare le disposizioni relative alla responsabilità dei prestatori intermediari di cui al regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio ([15]).

(12) La nozione di «sistema di IA» di cui al presente regolamento dovrebbe essere definita in maniera chiara e dovrebbe essere strettamente allineata al lavoro delle organizzazioni internazionali che si occupano di IA al fine di garantire la certezza del diritto, agevolare la convergenza internazionale e un'ampia accettazione, prevedendo nel contempo la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici in questo ambito. Inoltre, la definizione dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati consentendo l'apprendimento, il ragionamento o la modellizzazione. Il termine «automatizzato» si riferisce al fatto che il funzionamento dei sistemi di IA prevede l'uso di macchine. Il riferimento a obiettivi espliciti o impliciti sottolinea che i sistemi di IA possono operare in base a obiettivi espliciti definiti o a obiettivi impliciti. Gli obiettivi del sistema di IA possono essere diversi dalla finalità prevista del sistema di IA in un contesto specifico. Ai fini del presente regolamento, gli ambienti dovrebbero essere intesi come i contesti in cui operano i sistemi di IA, mentre gli output generati dal sistema di IA riflettono le diverse funzioni svolte dai sistemi di IA e comprendono previsioni, contenuti, raccomandazioni o decisioni. I sistemi di IA sono progettati per funzionare con livelli di autonomia variabili, il che significa che dispongono di un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano. L'adattabilità che un sistema di IA potrebbe presentare dopo la diffusione si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso. I sistemi di IA possono essere utilizzati come elementi indipendenti (stand-alone) o come componenti di un 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).

(13) La nozione di «deployer» di cui al presente regolamento dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal deployer.

(14) La nozione di «dati biometrici» utilizzata nel presente regolamento dovrebbe essere interpretata alla luce della nozione di dati biometrici di cui all'articolo 4, punto 14, del regolamento (UE) 2016/679, all'articolo 3, punto 18, del regolamento (UE) 2018/172 e all'articolo 3, punto 13, della direttiva (UE) 2016/680. I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche.

(15) La nozione di «identificazione biometrica» di cui al presente regolamento dovrebbe essere definita come il riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali.

([15]) Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU L 277 del 27.10.2022, pag. 1).

(16) La nozione di «categorizzazione biometrica» di cui al presente regolamento dovrebbe essere definita come l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico. Ciò non comprende i sistemi di categorizzazione biometrica che sono una caratteristica puramente accessoria intrinsecamente legata a un altro servizio commerciale, il che significa che l'elemento non può, per ragioni tecniche oggettive, essere utilizzato senza il servizio principale e che l'integrazione di tale caratteristica o funzionalità non rappresenta un mezzo per eludere l'applicabilità delle norme del presente regolamento. Ad esempio, i filtri che classificano le caratteristiche facciali o del corpo utilizzate sui mercati online potrebbero costituire una tale caratteristica accessoria, in quanto possono essere utilizzati solo in relazione al servizio principale che consiste nel vendere un prodotto consentendo al consumatore di visualizzare in anteprima il prodotto su se stesso e aiutarlo a prendere una decisione di acquisto. Anche i filtri utilizzati nei servizi di social network online che classificano le caratteristiche facciali o del corpo per consentire agli utenti di aggiungere o modificare immagini o video potrebbero essere considerati una caratteristica accessoria, in quanto tale filtro non può essere utilizzato senza il servizio principale dei servizi di social network consistente nella condivisione di contenuti online.

(17) È opportuno definire a livello funzionale la nozione di «sistema di identificazione biometrica remota» di cui al presente regolamento, quale sistema di IA destinato all'identificazione, tipicamente a distanza, di persone fisiche senza il loro coinvolgimento attivo mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, a prescindere dalla tecnologia, dai processi o dai tipi specifici di dati biometrici utilizzati. Tali sistemi di identificazione biometrica remota sono generalmente utilizzati per percepire più persone o il loro comportamento simultaneamente al fine di facilitare in modo significativo l'identificazione di persone fisiche senza il loro coinvolgimento attivo. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali. Tale esclusione è giustificata dal fatto che detti sistemi hanno probabilmente un impatto minore sui diritti fondamentali delle persone fisiche rispetto ai sistemi di identificazione biometrica remota, che possono essere utilizzati per il trattamento dei dati biometrici di un numero elevato di persone senza il loro coinvolgimento attivo. 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 è opportuno impedire l'elusione delle regole del presente regolamento per quanto attiene all'uso «in tempo reale» dei sistemi di IA interessati 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.

(18) La nozione di «sistema di riconoscimento delle emozioni» di cui al presente regolamento dovrebbe essere definita come un sistema di IA finalizzato a identificare o inferire emozioni o intenzioni di persone fisiche, sulla base dei loro dati biometrici. La nozione si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento. Non comprende stati fisici, quali dolore o affaticamento, compresi, ad esempio, ai sistemi utilizzati per rilevare lo stato di affaticamento dei piloti o dei conducenti professionisti al fine di prevenire gli incidenti. Non comprende neppure la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, a meno che non siano utilizzati per identificare o inferire emozioni. Tali espressioni possono essere espressioni facciali di base quali un aggrottamento delle sopracciglia o un sorriso, gesti quali il movimento di mani, braccia o testa, o caratteristiche della voce di una persona, ad esempio una voce alta o un sussurro.

(19) Ai fini del presente regolamento la nozione di «spazio accessibile al pubblico» dovrebbe essere intesa come riferita a qualsiasi luogo fisico accessibile a un numero indeterminato di persone fisiche e a prescindere dal fatto che il luogo in questione sia di proprietà pubblica o privata, indipendentemente dall'attività per la quale il luogo può essere utilizzato, quali il commercio (ad esempio negozi, ristoranti, bar), i servizi (ad esempio banche, attività professionali, ospitalità), lo sport (ad esempio piscine, palestre, stadi), i trasporti (ad esempio stazioni di autobus, metropolitane e ferroviarie, aeroporti, mezzi di trasporto), l'intrattenimento (ad esempio cinema, teatri, musei, sale da concerto e sale conferenze), il tempo libero o altro (ad esempio strade e piazze pubbliche, parchi, foreste, parchi giochi). Un luogo dovrebbe essere classificato come accessibile al pubblico anche se, indipendentemente da potenziali restrizioni di capacità o di sicurezza, l'accesso è soggetto a determinate condizioni predeterminate, che possono essere soddisfatte da un numero indeterminato di persone, quali l'acquisto di un biglietto o titolo di trasporto, la registrazione previa o il raggiungimento di una determinata età. Per contro, un luogo non dovrebbe essere considerato accessibile al pubblico se l'accesso è limitato a persone fisiche specifiche e definite attraverso il diritto dell'Unione o nazionale direttamente connesso alla pubblica sicurezza o attraverso la chiara manifestazione di volontà da parte della persona che ha l'autorità pertinente sul luogo. La sola possibilità concreta di accesso (ad

esempio una porta sbloccata, un cancello aperto in una recinzione) non implica che il luogo sia accessibile al pubblico in presenza di indicazioni o circostanze che suggeriscono il contrario (ad esempio segnaletica che vieta o limita l'accesso). I locali delle imprese e delle fabbriche, come pure gli uffici e i luoghi di lavoro destinati ad essere accessibili solo dai pertinenti dipendenti e prestatori di servizi, sono luoghi non accessibili al pubblico. Gli spazi accessibili al pubblico non dovrebbero includere le carceri o i controlli di frontiera. Alcune altre zone possono comprendere sia aree non accessibili al pubblico che aree accessibili al pubblico, come l'atrio di un edificio residenziale privato da cui è possibile accedere a uno studio medico o un aeroporto. Non sono del pari contemplati gli spazi online, dato che non sono luoghi fisici. 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.

(20) Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA. Tali nozioni possono variare in relazione al contesto pertinente e possono includere la comprensione della corretta applicazione degli elementi tecnici durante la fase di sviluppo del sistema di IA, le misure da applicare durante il suo utilizzo, le modalità adeguate per interpretare l'output del sistema di IA e, nel caso delle persone interessate, le conoscenze necessarie per comprendere in che modo le decisioni adottate con l'assistenza dell'IA incideranno su di esse. Nel contesto dell'applicazione del presente regolamento, l'alfabetizzazione in materia di IA dovrebbe fornire a tutti i pertinenti attori della catena del valore dell'IA le conoscenze necessarie per garantire l'adeguata conformità e la sua corretta esecuzione. Inoltre, l'ampia attuazione delle misure di alfabetizzazione in materia di IA e l'introduzione di adeguate azioni di follow-up potrebbero contribuire a migliorare le condizioni di lavoro e, in ultima analisi, sostenere il consolidamento e il percorso di innovazione di un'IA affidabile nell'Unione. Il consiglio europeo per l'intelligenza artificiale («consiglio per l'IA») dovrebbe sostenere la Commissione al fine di promuovere gli strumenti di alfabetizzazione in materia di IA, la sensibilizzazione del pubblico e la comprensione dei benefici, dei rischi, delle garanzie, dei diritti e degli obblighi in relazione all'uso dei sistemi di IA. In cooperazione con i pertinenti portatori di interessi, la Commissione e gli Stati membri dovrebbero agevolare l'elaborazione di codici di condotta volontari per migliorare l'alfabetizzazione in materia di IA tra le persone che si occupano di sviluppo, funzionamento e uso dell'IA.

(21) 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 ai deployer dei sistemi di IA stabiliti nell'Unione.

(22) 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 in un paese terzo in relazione a un'attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio. In tali circostanze il sistema di IA utilizzato dall'operatore in un paese terzo 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 ai deployer di sistemi di IA stabiliti in un paese terzo, nella misura in cui l'output prodotto da tali sistemi è destinato a essere utilizzato nell'Unione. Cionondimeno, per tener conto degli accordi vigenti e delle esigenze particolari per la cooperazione futura 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 della cooperazione o di accordi internazionali conclusi a livello dell'Unione o nazionale per la cooperazione delle autorità giudiziarie e di contrasto con l'Unione o con gli Stati membri, a condizione che il paese terzo o le organizzazioni internazionali pertinenti forniscano garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone. Se del caso, ciò può riguardare le attività di entità incaricate dai paesi terzi di svolgere compiti specifici a sostegno di tale cooperazione delle autorità giudiziarie e di contrasto. Tali quadri per la cooperazione o accordi sono stati istituiti bilateralmente tra Stati membri e paesi terzi o tra l'Unione europea, Europol e altre agenzie dell'Unione e paesi terzi e organizzazioni internazionali. Le autorità competenti per il controllo delle autorità giudiziarie e di contrasto ai sensi del presente regolamento dovrebbero valutare se tali quadri per la cooperazione o accordi internazionali includano garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone.

Le autorità nazionali destinatarie e le istituzioni, gli organi e gli organismi dell'Unione che si avvalgono di tali output nell'Unione, restano responsabili di garantire che il loro utilizzo sia conforme al diritto dell'Unione. In caso di revisione di tali accordi internazionali o di conclusione di nuovi accordi internazionali in futuro, le parti contraenti dovrebbero adoperarsi quanto più possibile per allineare tali accordi ai requisiti del presente regolamento.

(23) È altresì opportuno che il presente regolamento si applichi alle istituzioni, agli organi e agli organismi dell'Unione quando agiscono in qualità di fornitori o deployer di un sistema di IA.

(24) Se, e nella misura in cui, i sistemi di IA sono immessi sul mercato, messi in servizio o utilizzati con o senza modifica di tali sistemi per scopi militari, di difesa o di sicurezza nazionale, essi dovrebbero essere esclusi dall'ambito di applicazione del presente regolamento indipendentemente dal tipo di entità che svolge tali attività, ad esempio se si tratta di un'entità pubblica o privata. Per quanto riguarda gli scopi militari e di difesa, tale esclusione è giustificata sia dall'articolo 4, paragrafo 2, TUE sia dalle specificità della politica di difesa comune degli Stati membri e dell'Unione di cui al titolo V, capo 2, TUE che sono soggette al diritto internazionale pubblico, che costituisce pertanto il quadro giuridico più appropriato per la regolamentazione dei sistemi di IA nel contesto dell'uso letale della forza e di altri sistemi di IA nel contesto delle attività militari e di difesa. Per quanto riguarda le finalità di sicurezza nazionale, l'esclusione è giustificata sia dal fatto che la sicurezza nazionale resta di esclusiva competenza degli Stati membri ai sensi dell'articolo 4, paragrafo 2, TUE, sia dalla natura specifica e dalle esigenze operative delle attività di sicurezza nazionale, nonché dalle specifiche norme nazionali applicabili a tali attività. Tuttavia, se un sistema di IA sviluppato, immesso sul mercato, messo in servizio o utilizzato per scopi militari, di difesa o di sicurezza nazionale è usato al di fuori di tali finalità, in via temporanea o permanente, per altri scopi, ad esempio a fini civili o umanitari, per scopi di attività di contrasto o di sicurezza pubblica, tale sistema rientrerebbe nell'ambito di applicazione del presente regolamento. In tal caso, l'entità che utilizza il sistema di IA per finalità diverse da quelle militari, di difesa o di sicurezza nazionale dovrebbe garantire la conformità del sistema di IA al presente regolamento, a meno che il sistema non sia già conforme al presente regolamento. Rientrano nell'ambito di applicazione del presente regolamento i sistemi di IA immessi sul mercato o messi in servizio per una finalità esclusa, ossia militare, di difesa o di sicurezza nazionale, e per una o più finalità non escluse, ad esempio scopi civili o attività di contrasto, e i fornitori di tali sistemi dovrebbero garantire la conformità al presente regolamento. In tali casi, il fatto che un sistema di IA possa rientrare nell'ambito di applicazione del presente regolamento non dovrebbe incidere sulla possibilità per le entità che svolgono attività militari, di sicurezza nazionale e di difesa, indipendentemente dal tipo di entità che svolge tali attività, di utilizzare sistemi di IA per scopi di sicurezza nazionale, militari e di difesa, l'uso dei quali è escluso dall'ambito di applicazione del presente regolamento. Un sistema di IA immesso sul mercato per scopi civili o di attività di contrasto che è utilizzato con o senza modifiche a fini militari, di difesa o di sicurezza nazionale non dovrebbe rientrare nell'ambito di applicazione del presente regolamento, indipendentemente dal tipo di entità che svolge tali attività.

(25) Il presente regolamento dovrebbe sostenere l'innovazione, rispettare la libertà della scienza e non dovrebbe pregiudicare le attività di ricerca e sviluppo. È pertanto necessario escludere dal suo ambito di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. È inoltre necessario garantire che il regolamento non incida altrimenti sulle attività scientifiche di ricerca e sviluppo relative ai sistemi o modelli di IA prima dell'immissione sul mercato o della messa in servizio. Per quanto riguarda le attività di ricerca, prova e sviluppo orientate ai prodotti relative ai sistemi o modelli di IA, le disposizioni del presente regolamento non dovrebbero nemmeno applicarsi prima che tali sistemi e modelli siano messi in servizio o immessi sul mercato. Tale esclusione non pregiudica l'obbligo di conformarsi al presente regolamento qualora un sistema di IA che rientra nell'ambito di applicazione del presente regolamento sia immesso sul mercato o messo in servizio in conseguenza di tale attività di ricerca e sviluppo, così come non pregiudica l'applicazione delle disposizioni sugli spazi di sperimentazione normativa per l'IA e sulle prove in condizioni reali. Inoltre, fatta salva l'esclusione dei sistemi di IA specificamente sviluppati e messi in servizio solo a scopo di ricerca e sviluppo in ambito scientifico, qualsiasi altro sistema di IA che possa essere utilizzato per lo svolgimento di qualsiasi attività di ricerca e sviluppo dovrebbe rimanere soggetto alle disposizioni del presente regolamento. In ogni caso, qualsiasi attività di ricerca e sviluppo dovrebbe essere svolta conformemente alle norme etiche e professionali riconosciute nell'ambito della ricerca scientifica e dovrebbe essere condotta conformemente al diritto dell'Unione applicabile.

(26) 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 IA inaccettabili, 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.

(27) Sebbene l'approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un'IA affidabile del 2019 elaborati dall'AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che sono intesi a contribuire a garantire che l'IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. Fatti salvi i requisiti giuridicamente vincolanti del presente regolamento e di qualsiasi altra disposizione di diritto dell'Unione applicabile, tali orientamenti contribuiscono all'elaborazione di un'IA coerente, affidabile e antropocentrica, in linea con la Carta e con i valori su cui si fonda l'Unione. Secondo gli orientamenti dell'AI HLEG con «intervento e sorveglianza umani» si intende che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani. Con «robustezza tecnica e sicurezza» si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire la robustezza nel caso di problemi e resilienza contro i tentativi di alterare l'uso o le prestazioni del sistema di IA in modo da consentire l'uso illegale da parte di terzi e ridurre al minimo i danni involontari. Con «vita privata e governance dei dati» si intende che i sistemi di IA sono sviluppati e utilizzati nel rispetto delle norme in materia di vita privata e protezione dei dati, elaborando al contempo dati che soddisfino livelli elevati in termini di qualità e integrità. Con «trasparenza» si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i deployer delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti. Con «diversità, non discriminazione ed equità» si intende che i sistemi di IA sono sviluppati e utilizzati in modo da includere soggetti diversi e promuovere la parità di accesso, l'uguaglianza di genere e la diversità culturale, evitando nel contempo effetti discriminatori e pregiudizi ingiusti vietati dal diritto dell'Unione o nazionale. Con «benessere sociale e ambientale» si intende che i sistemi di IA sono sviluppati e utilizzati in modo sostenibile e rispettoso dell'ambiente e in modo da apportare benefici a tutti gli esseri umani, monitorando e valutando gli impatti a lungo termine sull'individuo, sulla società e sulla democrazia. L'applicazione di tali principi dovrebbe essere tradotta, ove possibile, nella progettazione e nell'utilizzo di modelli di IA. Essi dovrebbero in ogni caso fungere da base per l'elaborazione di codici di condotta a norma del presente regolamento. Tutti i portatori di interessi, compresi l'industria, il mondo accademico, la società civile e le organizzazioni di normazione, sono incoraggiati a tenere conto, se del caso, dei principi etici per lo sviluppo delle migliori pratiche e norme volontarie.

(28) L'IA 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 abusive e dovrebbero essere vietate poiché sono contrarie ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori.

(29) Le tecniche di manipolazione basate sull'IA possono essere utilizzate per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la libera scelta. L'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA con l'obiettivo o l'effetto di distorcere materialmente il comportamento umano, con il rischio di causare danni significativi, in particolare aventi effetti negativi sufficientemente importanti sulla salute fisica, psicologica o sugli interessi finanziari, sono particolarmente pericolosi e dovrebbero pertanto essere vietati. Tali sistemi di IA impiegano componenti subliminali quali stimoli audio, grafici e video che le persone non sono in grado di percepire poiché tali stimoli vanno al di là della percezione umana o altre tecniche manipolative o ingannevoli che sovvertono o pregiudicano l'autonomia, il processo decisionale o la libera scelta di una persona senza che sia consapevole di tali tecniche o, se ne è consapevole, senza che sia in grado di controllarle o resistervi o possa evitare l'inganno. Ciò potrebbe essere facilitato, ad esempio, da interfacce cervello-computer o dalla realtà virtuale, in quanto queste consentono un livello più elevato di controllo degli stimoli presentati alle persone, nella misura in cui possono distorcerne materialmente il comportamento in modo significativamente nocivo. In aggiunta, i sistemi di IA possono inoltre sfruttare in altro modo le vulnerabilità di una persona o di uno specifico gruppo di persone dovute all'età, a disabilità ai sensi della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio ([16]) o a una specifica situazione sociale o economica che potrebbe rendere tali persone più vulnerabili allo sfruttamento, come le persone che vivono in condizioni di povertà estrema e le minoranze etniche o religiose. Tali sistemi di IA possono essere immessi sul mercato, messi in servizio o utilizzati con l'obiettivo o l'effetto di distorcere materialmente il comportamento di una persona e in un modo che provochi o possa verosimilmente provocare a tale persona o a un'altra persona o gruppo di persone un danno significativo, compresi danni che possono essere

([16]) Direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi (GU L 151 del 7.6.2019, pag. 70).

accumulati nel tempo, e dovrebbero pertanto essere vietati. Potrebbe non essere possibile presumere che vi sia l'intenzione di distorcere il comportamento qualora la distorsione sia determinata da fattori esterni al sistema di IA, che sfuggono al controllo del fornitore o del deployer, ossia fattori che non possono essere ragionevolmente prevedibili e non possono quindi essere attenuati dal fornitore o dal deployer del sistema di IA. In ogni caso, non è necessario che il fornitore o il deployer abbiano l'intento di provocare un danno significativo, purché tale danno derivi da pratiche manipolative o di sfruttamento consentite dall'IA. Il divieto di tali pratiche di IA è complementare alle disposizioni contenute nella direttiva 2005/29/CE del Parlamento europeo e del Consiglio ([17]), in particolare le pratiche commerciali sleali che comportano danni economici o finanziari per i consumatori sono vietate in ogni circostanza, indipendentemente dal fatto che siano attuate attraverso sistemi di IA o in altro modo. I divieti di pratiche manipolative e di sfruttamento di cui al presente regolamento non dovrebbero pregiudicare le pratiche lecite nel contesto di trattamenti medici, quali il trattamento psicologico di una malattia mentale o la riabilitazione fisica, quando tali pratiche sono svolte conformemente al diritto applicabile e alle norme in ambito medico, ad esempio il consenso esplicito delle persone fisiche o dei loro rappresentanti legali. Inoltre, le pratiche commerciali comuni e legittime, ad esempio nel settore della pubblicità, che sono conformi alla normativa applicabile non dovrebbero essere considerate di per sé come pratiche consentite dall'IA manipolative o dannose.

(30) Dovrebbero essere vietati i sistemi di categorizzazione biometrica basati sui dati biometrici di persone fisiche, quali il volto o le impronte digitali, per trarre deduzioni o inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona. Tale divieto non dovrebbe riguardare l'etichettatura, il filtraggio o la categorizzazione legali dei set di dati biometrici acquisiti in linea con il diritto dell'Unione o nazionale in funzione dei dati biometrici, come la selezione di immagini in base al colore dei capelli o degli occhi, che possono essere utilizzati, ad esempio, nel settore delle attività di contrasto.

(31) I sistemi di IA che permettono ad attori pubblici o privati di attribuire un punteggio sociale alle persone fisiche 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 le persone fisiche o i gruppi di persone fisiche sulla base di vari punti di dati riguardanti il loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note, inferite o previste nell'arco di determinati periodi di tempo. 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. I sistemi di IA che comportano tali pratiche inaccettabili di punteggio aventi risultati pregiudizievoli o sfavorevoli dovrebbero pertanto essere vietati. Tale divieto non dovrebbe pregiudicare le pratiche lecite di valutazione delle persone fisiche effettuate per uno scopo specifico in conformità del diritto dell'Unione e nazionale.

(32) 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 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. 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. Tali possibili risultati distorti ed effetti discriminatori sono particolarmente importanti per quanto riguarda l'età, l'etnia, la razza, il sesso o le disabilità. 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 interessate nell'ambito delle attività di contrasto, o che sono da queste condizionate.

(33) L'uso di tali sistemi a fini di attività di contrasto dovrebbe pertanto essere vietato, eccezion fatta per le 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 determinate vittime di reato, comprese le persone scomparse, determinate minacce per la vita o l'incolumità fisica delle persone fisiche o un attacco terroristico nonché la localizzazione o l'identificazione degli autori o dei sospettati di reati elencati nell'allegato del presente regolamento qualora tali reati siano punibili nello Stato membro interessato

([17]) Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n, 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali») (GU L 149 dell'11.6.2005, pag. 22).

con una pena o una misura di sicurezza privativa della libertà personale della durata massima di almeno quattro anni e sono definiti conformemente al diritto di tale Stato membro. Tale soglia per la pena o la misura di sicurezza privativa della libertà personale in conformità del 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, l'elenco dei reati di cui all'allegato del presente regolamento è basato sui 32 reati elencati nella decisione quadro 2002/584/GAI del Consiglio ([18]), tenendo conto che alcuni reati risultano più pertinenti di altri, poiché il grado di necessità e proporzionalità del ricorso all'identificazione biometrica remota «in tempo reale» potrebbe essere prevedibilmente molto variabile per quanto concerne il perseguimento pratico della localizzazione o dell'identificazione 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. Una minaccia imminente per la vita o l'incolumità fisica delle persone fisiche potrebbe anche derivare da un grave danneggiamento dell'infrastruttura critica quale definita all'articolo 2, punto 4, della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio ([19]), ove il danneggiamento o la distruzione di tale infrastruttura critica possa comportare una minaccia imminente per la vita o l'integrità fisica di una persona, anche in ragione di un grave danno alla fornitura di forniture di base alla popolazione o all'esercizio della funzione essenziale dello Stato. Il presente regolamento dovrebbe altresì preservare la capacità delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo di svolgere controlli d'identità in presenza della persona interessata, conformemente alle condizioni stabilite per tali controlli dal diritto dell'Unione e nazionale. In particolare, le autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo dovrebbero poter utilizzare i sistemi di informazione, conformemente al diritto dell'Unione o nazionale, per identificare le persone che, durante un controllo d'identità, rifiutano di essere identificate o non sono in grado di dichiarare o dimostrare la loro identità, senza essere tenute, a norma del presente regolamento, a ottenere un'autorizzazione preventiva. Potrebbe trattarsi, ad esempio, di una persona coinvolta in un reato che, a causa di un incidente o di un problema di salute, non vuole rivelare la propria identità alle autorità di contrasto o non è in grado di farlo.

(34) Al fine di garantire che tali sistemi siano utilizzati in modo responsabile e proporzionato, è altresì importante stabilire che, in ciascuna delle 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 impiegato solo per confermare l'identità della persona specificamente interessata e dovrebbe essere limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale, con particolare riguardo a indicazioni o elementi probatori relativi a minacce, vittime o autori di reati. L'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico dovrebbe essere autorizzato solo se l'autorità di contrasto pertinente ha completato una valutazione d'impatto sui diritti fondamentali e, salvo disposizione contraria del presente regolamento, ha registrato il sistema nella banca dati di cui al presente regolamento. La banca dati di riferimento delle persone dovrebbe risultare adeguata per ogni caso d'uso in ciascuna delle situazioni di cui sopra.

(35) È opportuno subordinare ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a un'autorizzazione esplicita e specifica da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente di uno Stato membro la cui decisione sia vincolante. Tale autorizzazione dovrebbe, in linea di principio, essere ottenuta prima dell'uso del sistema di IA al fine di identificare una o più persone. Eccezioni a tale regola dovrebbero essere ammesse in situazioni di urgenza debitamente giustificate, vale a dire le situazioni in cui la necessità di utilizzare i sistemi interessati è tale da far sì che sia effettivamente e oggettivamente impossibile ottenere un'autorizzazione prima di iniziare a utilizzare il sistema di IA. In tali situazioni di urgenza, è opportuno limitare l'uso del sistema di IA 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. In tali situazioni, inoltre, l'autorità di contrasto dovrebbe richiedere tale autorizzazione, indicando contestualmente i motivi per cui non ha potuto richiederla prima, senza indebito ritardo e al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso dei sistemi di identificazione biometrica «in tempo reale» collegati a tale autorizzazione dovrebbe essere interrotto con effetto immediato e tutti i dati relativi a tale uso dovrebbero essere eliminati e cancellati. Tali dati comprendono i dati di input acquisiti direttamente da un

([18]) 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).

([19]) Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (GU L 333 del 27.12.2022, pag. 164).

sistema di IA nel corso dell'uso di tale sistema, nonché i risultati e gli output dell'uso connessi a tale autorizzazione. Non dovrebbero includere gli input acquisiti legalmente in conformità di altre disposizioni del diritto dell'Unione o nazionale. In ogni caso, nessuna decisione che produca effetti giuridici negativi su una persona dovrebbe essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota.

(36) Affinché svolgano i loro compiti conformemente alle prescrizioni del presente regolamento e alle norme nazionali, è opportuno notificare alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati ogni uso del sistema di identificazione biometrica «in tempo reale». Le autorità di vigilanza del mercato e le autorità nazionali per la protezione dei dati che sono state notificate dovrebbero presentare alla Commissione una relazione annuale sull'uso dei sistemi di identificazione biometrica «in tempo reale».

(37) È altresì opportuno prevedere, nell'ambito del quadro esaustivo stabilito dal presente regolamento, che tale uso nel territorio di uno Stato membro in conformità del presente regolamento sia possibile solo nel caso e nella misura in cui lo Stato membro interessato 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. Tali regole nazionali dovrebbero essere notificate alla Commissione entro 30 giorni dalla loro adozione.

(38) 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 (UE) 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 dare attuazione a tale autorizzazione.

(39) 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, dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 10 della direttiva (UE) 2016/680. Per fini diversi dalle attività di contrasto, l'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e l'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 vietano il trattamento di dati biometrici fatte salve limitate eccezioni previste da tali articoli. Nell'applicazione dell'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, l'uso dell'identificazione biometrica remota a fini diversi dalle attività di contrasto è già stato oggetto di decisioni di divieto da parte delle autorità nazionali per la protezione dei dati.

(40) 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, primo comma, lettera g), nella misura in cui si applica all'uso di sistemi di categorizzazione biometrica per le attività nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, all'articolo 5, paragrafo 1, primo comma, lettera d), nella misura in cui si applica all'uso dei sistemi di IA contemplati da tale disposizione, all'articolo 5, paragrafo 1, primo comma, lettera h), paragrafi da 2 a 6, e all'articolo 26, paragrafo 10, 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.

(41) 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, primo comma, lettera g), nella misura in cui si applica all'uso di sistemi di categorizzazione biometrica per le attività nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, all'articolo 5, paragrafo 1, primo comma, lettera d), nella misura in cui si applica all'uso dei sistemi di IA contemplati da tale disposizione, all'articolo 5, paragrafo 1, primo comma,

lettera h), paragrafi da 2 a 6, e all'articolo 26, paragrafo 10, 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.

(42) In linea con la presunzione di innocenza, le persone fisiche nell'Unione dovrebbero sempre essere giudicate in base al loro comportamento effettivo. Le persone fisiche non dovrebbero mai essere giudicate sulla base di un comportamento previsto dall'IA basato unicamente sulla profilazione, sui tratti della personalità o su caratteristiche quali la cittadinanza, il luogo di nascita, il luogo di residenza, il numero di figli, il livello di indebitamento o il tipo di automobile, senza che vi sia un ragionevole sospetto che la persona sia coinvolta in un'attività criminosa sulla base di fatti oggettivi verificabili e senza una valutazione umana al riguardo. Pertanto, dovrebbero essere vietate le valutazioni del rischio effettuate in relazione a persone fisiche intese a determinare la probabilità che queste ultime commettano un reato o volte a prevedere il verificarsi di un reato effettivo o potenziale unicamente sulla base della loro profilazione o della valutazione dei loro tratti della personalità e delle loro caratteristiche. In ogni caso, tale divieto non fa riferimento né riguarda l'analisi del rischio che non è basata sulla profilazione delle persone o sui tratti della personalità e sulle caratteristiche delle persone, come i sistemi di IA che utilizzano l'analisi dei rischi per valutare il rischio di frode finanziaria da parte di imprese sulla base di transazioni sospette o di strumenti di analisi del rischio per prevedere la probabilità di localizzazione di stupefacenti o merci illecite da parte delle autorità doganali, ad esempio sulla base di rotte di traffico conosciute.

(43) L'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso dovrebbero essere vietati, in quanto tale pratica accresce il senso di sorveglianza di massa e può portare a gravi violazioni dei diritti fondamentali, compreso il diritto alla vita privata.

(44) Sussistono serie preoccupazioni in merito alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, in particolare perché l'espressione delle emozioni varia notevolmente in base alle culture e alle situazioni e persino in relazione a una stessa persona. Tra le principali carenze di tali sistemi figurano la limitata affidabilità, la mancanza di specificità e la limitata generalizzabilità. Pertanto, i sistemi di IA che identificano o inferiscono emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici possono portare a risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate. Considerando lo squilibrio di potere nel contesto del lavoro o dell'istruzione, combinato con la natura invasiva di tali sistemi, questi ultimi potrebbero determinare un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche. È pertanto opportuno vietare l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati per rilevare lo stato emotivo delle persone in situazioni relative al luogo di lavoro e all'istruzione. Tale divieto non dovrebbe riguardare i sistemi di IA immessi sul mercato esclusivamente per motivi medici o di sicurezza, come i sistemi destinati all'uso terapeutico.

(45) Il presente regolamento non dovrebbe incidere sulle pratiche vietate dal diritto dell'Unione, ivi incluso dal diritto in materia di protezione dei dati, non discriminazione, protezione dei consumatori e concorrenza.

(46) È opportuno che i sistemi di IA ad alto rischio siano immessi sul mercato dell'Unione, messi in servizio o utilizzati 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. In base al nuovo quadro legislativo, come chiarito nella comunicazione della Commissione «La "Guida blu" all'attuazione della normativa UE sui prodotti 2022» ([20]), la regola generale è che più di un atto giuridico della normativa di armonizzazione dell'Unione, come i regolamenti (UE) 2017/745 ([21]) e (UE) 2017/746 ([22]) del Parlamento europeo e del Consiglio o la direttiva n, 2006/42/CE del Parlamento europeo e del Consiglio ([23]), può essere applicabile a un solo prodotto, poiché quest'ultimo può essere messo a disposizione o messo in servizio solo se risulta conforme a tutta la normativa di armonizzazione dell'Unione applicabile. Al fine di garantire la coerenza ed evitare oneri

([20]) GU C 247 del 29.6.2022, pag. 1.
([21]) 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).
([22]) 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).
([23]) Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24).

amministrativi o costi non necessari, i fornitori di un prodotto contenente uno o più sistemi di IA ad alto rischio cui si applicano i requisiti del presente regolamento e della normativa di armonizzazione dell'Unione elencata in un allegato del presente regolamento dovrebbero avere flessibilità per quanto riguarda le decisioni operative sui modi per garantire in modo ottimale la conformità di un prodotto contenente uno o più sistemi di IA a tutti i requisiti applicabili della normativa di armonizzazione 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 dovrebbe ridurre al minimo eventuali potenziali restrizioni al commercio internazionale.

(47) I sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei 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.

(48) 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 il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, 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 il fatto che i minori godono di diritti specifici sanciti dall'articolo 24 della Carta e dalla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, ulteriormente sviluppati nell'osservazione generale n, 25 della Convenzione delle Nazioni Unite dell'infanzia e dell'adolescenza 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.

(49) 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 ([24]), del regolamento (UE) n, 167/2013 del Parlamento europeo e del Consiglio ([25]), del regolamento (UE) n, 168/2013 del Parlamento europeo e del Consiglio ([26]), della direttiva 2014/90/UE del Parlamento europeo e del Consiglio ([27]), della direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio ([28]), del regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio ([29]), del regolamento (UE)

([24]) 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).

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) 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).

2018/1139 del Parlamento europeo e del Consiglio ([30]), e del regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio ([31]), è opportuno modificare i suddetti atti per garantire che, nell'adottare qualsiasi atto delegato o di esecuzione pertinente sulla base di tali atti, la Commissione tenga conto, sulla base 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.

(50) 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 elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato 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, dispositivi medico-diagnostici *in vitro*, veicoli automobilistici e aeronautici.

(51) 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 i regolamenti (UE) 2017/745 e (UE) 2017/746, in cui è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio.

(52) Per quanto riguarda i sistemi di IA indipendenti, ossia i sistemi di IA ad alto rischio diversi da quelli che sono componenti di sicurezza dei 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 presente 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 che la Commissione dovrebbe avere il potere di adottare, mediante atti delegati, per tenere conto del rapido ritmo dello sviluppo tecnologico nonché dei potenziali cambiamenti nell'uso dei sistemi di IA.

(53) È altresì importante chiarire che possono esservi casi specifici in cui i sistemi di IA riferiti a settori predefiniti indicati nel presente regolamento non comportano un rischio significativo di pregiudicare gli interessi giuridici tutelati nell'ambito di tali settori in quanto non influenzano materialmente il processo decisionale né pregiudicano tali interessi in modo sostanziale. Ai fini del presente regolamento, un sistema di IA che non influenza materialmente l'esito del processo decisionale dovrebbe essere inteso come un sistema di IA che non ha un impatto sulla sostanza, e quindi sull'esito, del processo decisionale, sia esso umano o automatizzato. Un sistema di IA che non influenza materialmente l'esito del processo decisionale potrebbe includere situazioni in cui sono soddisfatte una o più delle seguenti condizioni. La prima di tali condizioni dovrebbe essere che il sistema di IA sia destinato a svolgere un compito procedurale ristretto, come un sistema di IA che trasforma dati non strutturati in dati strutturati, un sistema di IA che classifica i documenti in entrata per categorie o un sistema di IA utilizzato per rilevare duplicati tra un gran numero di applicazioni. Tali compiti sono di natura così ristretta e limitata da comportare solo rischi limitati che non aumentano con l'uso di un sistema di IA in un contesto elencato come uso ad alto rischio in un allegato del presente regolamento. La seconda condizione dovrebbe essere che il compito svolto dal sistema di IA sia inteso

([30]) 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).

([31]) 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).

a migliorare il risultato di un'attività umana precedentemente completata che può essere pertinente ai fini degli usi ad alto rischio elencati nell' allegato del presente regolamento. Tenuto conto di tali caratteristiche, il sistema di IA fornisce solo un livello aggiuntivo a un'attività umana con conseguente riduzione del rischio. Tale condizione si applicherebbe, ad esempio, ai sistemi di IA destinati a migliorare il linguaggio utilizzato in documenti redatti in precedenza, ad esempio in relazione al tono professionale, allo stile accademico del linguaggio o allineando il testo a una determinata comunicazione di marchio. La terza condizione dovrebbe essere che il sistema di IA sia inteso a individuare modelli decisionali o deviazioni da modelli decisionali precedenti. Il rischio sarebbe ridotto in quanto l'uso del sistema di IA segue una valutazione umana precedentemente completata che non è destinato a sostituire o influenzare, senza un'adeguata revisione umana. Tali sistemi di IA comprendono, ad esempio, quelli che, dato un determinato modello di valutazione di un insegnante, possono essere utilizzati per verificare *ex post* se l'insegnante possa essersi discostato dal modello di valutazione in modo da segnalare potenziali incongruenze o anomalie. La quarta condizione dovrebbe essere che il sistema di IA sia destinato a svolgere un compito che è solo preparatorio rispetto a una valutazione pertinente ai fini dei sistemi di IA elencati in un allegato del presente regolamento, e pertanto la probabilità che l'output del sistema presenti un rischio per la valutazione posteriore è molto ridotto. Tale condizione riguarda, in particolare, soluzioni intelligenti per la gestione dei fascicoli, che comprendono varie funzioni quali l'indicizzazione, la ricerca, l'elaborazione testuale e vocale o il collegamento dei dati ad altre fonti di dati, o i sistemi di IA utilizzati per la traduzione di documenti iniziali. In ogni caso, è opportuno ritenere che i sistemi di IA utilizzati usi ad alto rischio elencati nell' allegato del presente regolamento comportino rischi significativi di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche se il sistema di IA implica la profilazione ai sensi dell'articolo 4, punto 4, del regolamento (UE) 2016/679, o dell'articolo 3, punto 4, della direttiva (UE) 2016/680 o dell'articolo 3, punto 5, del regolamento (UE) 2018/1725. Al fine di garantire la tracciabilità e la trasparenza, un fornitore che ritiene che un sistema di IA non sia ad alto rischio sulla base delle condizioni di cui sopra dovrebbe redigere la documentazione relativa alla valutazione prima che tale sistema sia immesso sul mercato o messo in servizio e dovrebbe fornire tale documentazione alle autorità nazionali competenti su richiesta. Tale fornitore dovrebbe essere tenuto a registrare il sistema di IA nella banca dati dell'UE istituita a norma del presente regolamento. Al fine di fornire ulteriori orientamenti per l'attuazione pratica delle condizioni alle quali i sistemi di IA elencati in un allegato del presente regolamento sono, in via eccezionale, non ad alto rischio, la Commissione, previa consultazione del consiglio per l'IA, dovrebbe fornire orientamenti che specifichino tale attuazione pratica completati da un elenco completo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e casi d'uso che non lo sono.

(54) Poiché i dati biometrici costituiscono una categoria particolare di dati personali, è opportuno classificare come ad alto rischio diversi casi di uso critico di sistemi biometrici, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale. 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. Il rischio di tali risultati distorti ed effetti discriminatori è particolarmente importante per quanto riguarda l'età, l'etnia, la razza, il sesso o le disabilità. I sistemi destinati all'identificazione biometrica remota dovrebbero pertanto essere classificati come ad alto rischio in considerazione dei rischi che comportano. Tale classificazione esclude i sistemi di IA destinati a essere utilizzati per la verifica biometrica, inclusa l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è chi dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso sicuro a locali. Inoltre, è opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti a norma dell'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 sulla base di dati biometrici, nella misura in cui non sono vietati a norma del presente regolamento, e i sistemi di riconoscimento delle emozioni che non sono vietati a norma del presente regolamento. I sistemi biometrici destinati a essere utilizzati al solo scopo di consentire la cibersicurezza e le misure di protezione dei dati personali non dovrebbero essere considerati sistemi di IA ad alto rischio.

(55) 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 e del funzionamento delle infrastrutture digitali critiche di cui all'allegato, punto 8, della direttiva (UE) 2022/2557, 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. I componenti di sicurezza delle infrastrutture critiche, comprese le infrastrutture digitali critiche, sono sistemi utilizzati per proteggere direttamente l'integrità fisica delle infrastrutture critiche ovvero la salute e la sicurezza delle persone e dei beni ma che non sono necessari per il funzionamento del sistema. Un guasto o malfunzionamento di tali componenti

potrebbe comportare direttamente rischi per l'integrità fisica delle infrastrutture critiche e quindi per la salute e la sicurezza delle persone e dei beni. I componenti destinati a essere utilizzati esclusivamente a fini di cibersicurezza non dovrebbero essere considerati componenti di sicurezza. Tra gli esempi di componenti di sicurezza di tali infrastrutture critiche possono rientrare i sistemi di monitoraggio della pressione idrica o sistemi di controllo degli incendi nei centri di cloud computing.

(56) La diffusione dei sistemi di IA nell'istruzione è importante per promuovere un'istruzione e una formazione digitali di alta qualità e per consentire a tutti i discenti e gli insegnanti di acquisire e condividere le competenze e le abilità digitali necessarie, compresa l'alfabetizzazione mediatica, e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici. Tuttavia, i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento delle persone, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono essere particolarmente intrusivi e violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e 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.

(57) 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 riguardanti le condizioni del rapporto di lavoro la promozione e la cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti sulla base dei comportamenti individuali, dei tratti o delle caratteristiche personali e 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 prospettive di carriera e sostentamento e di diritti dei lavoratori. I pertinenti rapporti contrattuali di lavoro dovrebbero coinvolgere, in modo significativo, i dipendenti e le persone che forniscono servizi tramite piattaforme, come indicato nel programma di lavoro annuale della Commissione per il 2021. 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 comprometterne i diritti fondamentali in materia di protezione dei dati e vita privata.

(58) Un altro settore in cui l'utilizzo dei sistemi di IA merita particolare attenzione è l'accesso ad alcuni servizi e prestazioni essenziali, pubblici e privati, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi. In particolare, le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, vale a dire servizi sanitari, prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia, gli infortuni sul lavoro, la dipendenza o la vecchiaia e la perdita di occupazione e l'assistenza sociale e abitativa, sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità responsabili. I sistemi di IA, se utilizzati per determinare se tali prestazioni e servizi dovrebbero essere concessi, negati, ridotti, revocati o recuperati dalle autorità, compreso se i beneficiari hanno legittimamente diritto a tali prestazioni o servizi, 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 e dovrebbero pertanto essere classificati 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. È inoltre 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 tali fini possono portare alla discriminazione fra persone o gruppi e possono perpetuare modelli storici di discriminazione, come quella basata sull'origine razziale o etnica, sul genere, sulle disabilità, sull'età o sull'orientamento sessuale, o possono dar vita a nuove forme di impatti discriminatori. Tuttavia, i sistemi di IA previsti dal diritto dell'Unione al fine di individuare frodi nell'offerta di servizi finanziari e a fini prudenziali per calcolare i requisiti patrimoniali degli enti creditizi e delle imprese assicurative non dovrebbero essere considerati ad alto rischio ai sensi del presente regolamento. Inoltre, anche i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione

dei prezzi in relazione alle persone fisiche per assicurazioni sulla vita e assicurazioni sanitarie possono avere un impatto significativo sul sostentamento delle persone e, se non debitamente progettati, sviluppati e utilizzati, possono violare i loro diritti fondamentali e comportare gravi conseguenze per la vita e la salute delle persone, tra cui l'esclusione finanziaria e la discriminazione. Infine, è opportuno classificare come ad alto rischio anche i sistemi di IA utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, anche da parte di polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza in quanto prendono decisioni in situazioni molto critiche per la vita e la salute delle persone e per i loro beni.

(59) Tenuto conto del loro ruolo e della loro responsabilità, 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 prestazione, 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, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale, 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 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, o per loro conto, o dagli organi o organismi dell'Unione a sostegno delle autorità di contrasto per valutare il rischio per una persona fisica di diventare vittima di reati, come poligrafi e strumenti analoghi, valutare l'affidabilità degli elementi probatori nel corso dell'accertamento e del perseguimento di reati, e, nella misura in cui non è vietato a norma del presente regolamento, determinare il rischio di reato o recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche, ma anche della valutazione dei tratti e delle caratteristiche della personalità o del comportamento criminale pregresso delle persone fisiche o dei gruppi, ai fini della profilazione nel corso dell'indagine, dell'accertamento e del perseguimento di reati. I sistemi di IA specificamente destinati a essere utilizzati per procedimenti amministrativi dalle autorità fiscali e doganali, come pure dalle unità di informazione finanziaria che svolgono compiti amministrativi di analisi delle informazioni conformemente al diritto dell'Unione in materia di antiriciclaggio, non dovrebbero essere classificati come sistemi di IA ad alto rischio utilizzati dalle autorità di contrasto a fini di prevenzione, accertamento, indagine e perseguimento di reati. L'utilizzo degli strumenti di IA da parte delle autorità di contrasto e delle altre pertinenti autorità non dovrebbe diventare un fattore di disuguaglianza o esclusione. L'impatto dell'utilizzo degli strumenti di IA sul diritto alla difesa degli indagati non dovrebbe essere ignorato, in particolare la difficoltà di ottenere informazioni significative sul funzionamento di tali sistemi e la difficoltà che ne risulta nel confutarne i risultati in tribunale, in particolare per le persone fisiche sottoposte a indagini.

(60) I sistemi di IA utilizzati nel settore della migrazione, dell'asilo e della gestione 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, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale, i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, o per loro conto, o dalle istituzioni, dagli organi o dagli organismi dell'Unione, incaricati di compiti in materia di migrazione, asilo e gestione del controllo delle frontiere, come poligrafi e strumenti analoghi, 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 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, compresa la connessa valutazione dell'affidabilità degli elementi probatori, al fine di individuare, riconoscere o identificare persone fisiche nel contesto della migrazione, dell'asilo e della gestione del controllo delle frontiere con l'eccezione della verifica dei documenti di viaggio. I sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere disciplinati dal presente regolamento dovrebbero essere conformi ai pertinenti requisiti procedurali stabiliti dal regolamento (CE) n, 810/2009 del Parlamento europeo e del Consiglio ([32]), dalla

([32]) 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).

direttiva 2013/32/UE del Parlamento europeo e del Consiglio, ([33]) e da altre pertinenti disposizioni di diritto dell'Unione. I sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere non dovrebbero in alcun caso essere utilizzati dagli Stati membri o dalle istituzioni, dagli organi o dagli organismi dell'Unione come mezzo per eludere gli obblighi internazionali a essi derivanti a titolo della convenzione delle Nazioni Unite relativa allo status dei rifugiati firmata a Ginevra il 28 luglio 1951, modificata dal protocollo del 31 gennaio 1967. Essi non dovrebbero essere utilizzati per violare in alcun modo il principio di non respingimento o per negare sicure ed efficaci vie legali di ingresso nel territorio dell'Unione, compreso il diritto alla protezione internazionale.

(61) 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 a essere utilizzati da un'autorità giudiziaria o per suo conto per 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. Anche i sistemi di IA destinati a essere utilizzati dagli organismi di risoluzione alternativa delle controversie a tali fini dovrebbero essere considerati ad alto rischio quando gli esiti dei procedimenti di risoluzione alternativa delle controversie producono effetti giuridici per le parti. L'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana. Non è tuttavia opportuno estendere la classificazione dei sistemi di IA come ad alto rischio 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.

(62) Fatte salve le norme previste dal regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio ([34]), e al fine di affrontare i rischi di indebite interferenze esterne sul diritto di voto sancito dall'articolo 39 della Carta e di effetti negativi sulla democrazia e sullo Stato di diritto, i sistemi di IA destinati a essere utilizzati per influenzare l'esito di elezioni o referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum dovrebbero essere classificati come sistemi di IA ad alto rischio, ad eccezione dei sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.

(63) Il fatto che un sistema di IA sia classificato come sistema di IA ad alto rischio a norma del presente regolamento non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia 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 dei 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, salvo quando diversamente disposto in modo specifico dal presente regolamento.

(64) Al fine di attenuare i rischi derivanti dai sistemi di IA ad alto rischio immessi sul mercato o messi in servizio e per garantire un elevato livello di affidabilità, è opportuno applicare determinati requisiti obbligatori ai sistemi di IA ad alto rischio, tenendo conto della finalità prevista e del contesto dell'uso del sistema di IA e conformemente al sistema di gestione dei rischi che deve essere stabilito dal fornitore. Le misure adottate dai fornitori per conformarsi ai requisiti obbligatori del presente regolamento dovrebbero tenere conto dello stato dell'arte generalmente riconosciuto in materia di IA ed essere proporzionate ed efficaci per conseguire gli obiettivi del presente regolamento. Sulla base del nuovo quadro legislativo, come chiarito nella comunicazione della Commissione «La "Guida blu" all'attuazione della normativa UE sui prodotti 2022», di norma più di un atto giuridico della normativa di armonizzazione dell'Unione può essere applicabile a un prodotto, poiché quest'ultimo può essere messo a disposizione o messo in servizio solo se risulta conforme a tutta la normativa di armonizzazione dell'Unione applicabile. I pericoli dei sistemi di IA disciplinati dai requisiti del presente regolamento riguardano aspetti diversi rispetto alla vigente normativa di armonizzazione dell'Unione e pertanto i requisiti del presente regolamento completerebbero il corpus esistente della normativa di armonizzazione dell'Unione. Ad esempio, le macchine o i dispositivi medici in cui è integrato un sistema di IA potrebbero presentare rischi non affrontati dai requisiti

([33]) 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).

([34]) Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al targeting della pubblicità politica (GU L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

essenziali di sicurezza e di tutela della salute stabiliti nella pertinente normativa armonizzata dell'Unione, in quanto tale normativa settoriale non affronta i rischi specifici dei sistemi di IA. Ciò richiede un'applicazione simultanea e complementare dei vari atti legislativi. Al fine di garantire la coerenza ed evitare oneri amministrativi e costi inutili, i fornitori di un prodotto contenente uno o più sistemi di IA ad alto rischio cui si applicano i requisiti del presente regolamento e della normativa di armonizzazione dell'Unione basata sul nuovo quadro legislativo ed elencata in un allegato del presente regolamento dovrebbero avere flessibilità per quanto riguarda le decisioni operative sulle maniere per garantire in modo ottimale la conformità di un prodotto contenente uno o più sistemi di IA a tutti i requisiti applicabili di tale normativa armonizzata dell'Unione. Tale flessibilità potrebbe significare, ad esempio, che il fornitore decide di integrare una parte dei necessari processi di prova e comunicazione, nonché delle informazioni e della documentazione richieste a norma del presente regolamento nella documentazione e nelle procedure già esistenti richieste dalla vigente normativa di armonizzazione dell'Unione sulla base del nuovo quadro legislativo ed elencate in un allegato del presente regolamento. Ciò non dovrebbe in alcun modo compromettere l'obbligo del fornitore di rispettare tutti i requisiti applicabili.

(65) Il sistema di gestione dei rischi dovrebbe essere costituito da un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio. Tale processo dovrebbe mirare a individuare e attenuare i rischi pertinenti dei sistemi di IA per la salute, la sicurezza e i diritti fondamentali. Il sistema di gestione dei rischi dovrebbe essere periodicamente riesaminato e aggiornato per garantirne l'efficacia costante, nonché la giustificazione e la documentazione delle eventuali decisioni e azioni significative adottate a norma del presente regolamento. Tale processo dovrebbe garantire che il fornitore individui rischi o impatti negativi e attui misure di attenuazione per i rischi noti e ragionevolmente prevedibili dei sistemi di IA per la salute, la sicurezza e i diritti fondamentali alla luce della loro finalità prevista e del loro uso improprio ragionevolmente prevedibile, compresi gli eventuali rischi derivanti dall'interazione tra il sistema di IA e l'ambiente in cui opera. Il sistema di gestione dei rischi dovrebbe adottare le misure di gestione dei rischi più appropriate alla luce dello stato dell'arte in materia di IA. Nell'individuare le misure di gestione dei rischi più appropriate, il fornitore dovrebbe documentare e spiegare le scelte effettuate e, se del caso, coinvolgere esperti e portatori di interessi esterni. Nell'individuare l'uso improprio ragionevolmente prevedibile dei sistemi di IA ad alto rischio, il fornitore dovrebbe contemplare gli usi di sistemi di IA che, pur non essendo direttamente coperti dalla finalità prevista e considerati nelle istruzioni per l'uso, si può ragionevolmente prevedere derivino da un comportamento umano facilmente prevedibile nel contesto delle caratteristiche e dell'uso specifici di un determinato sistema di IA. Qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità della 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, dovrebbe essere inclusa nelle istruzioni per l'uso fornite dal fornitore. L'obiettivo è garantire che il deployer sia consapevole e ne tenga conto quando utilizza il sistema di IA ad alto rischio. L'individuazione e l'attuazione di misure di attenuazione dei rischi per un uso improprio prevedibile a norma del presente regolamento non dovrebbero richiedere, da parte del fornitore per farvi fronte, specifiche formazioni aggiuntive per il sistema di IA ad alto rischio. I fornitori sono tuttavia incoraggiati a prendere in considerazione tali misure di formazione aggiuntive per attenuare gli usi impropri ragionevolmente prevedibili, ove necessario e opportuno.

(66) Tali requisiti dovrebbero applicarsi ai sistemi di IA ad alto rischio per quanto concerne la gestione dei rischi, la qualità e la pertinenza dei set di dati utilizzati, la documentazione tecnica e la conservazione delle registrazioni, la trasparenza e la fornitura di informazioni ai deployer, 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 e, non essendo ragionevolmente disponibili altre misure meno restrittive degli scambi, non costituiscono limitazioni ingiustificate del commercio.

(67) Dati di alta qualità e l'accesso a dati di alta qualità svolgono un ruolo essenziale nel fornire una struttura e garantire 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 una fonte di discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessario attuare adeguate pratiche di governance e gestione dei dati. I set di dati di addestramento, convalida e prova, incluse le etichette, dovrebbero essere pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista del sistema. Al fine di agevolare il rispetto del diritto dell'Unione in materia di protezione dei dati, come il regolamento (UE) 2016/679, le pratiche di governance e di gestione dei dati dovrebbero includere, nel caso dei dati personali, la trasparenza in merito alla finalità originaria della raccolta dei dati. I set di dati dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato, prestando particolare attenzione all'attenuazione di possibili distorsioni nei set di dati, suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli

output di dati influenzano gli input per operazioni future (feedback loops - «circuiti di feedback»). Le distorsioni possono ad esempio essere intrinseche ai set di dati di base, specie se si utilizzano dati storici, o generate quando i sistemi sono attuati in contesti reali. I risultati forniti dai sistemi di IA potrebbero essere influenzati da tali distorsioni intrinseche, che sono destinate ad aumentare gradualmente e quindi a perpetuare e amplificare le discriminazioni esistenti, in particolare nei confronti delle persone che appartengono a determinati gruppi vulnerabili, inclusi gruppi razziali o etnici. Il requisito secondo cui i set di dati dovrebbero essere, per quanto possibile, completi ed esenti da errori non dovrebbe incidere sull'uso di tecniche di tutela della vita privata nel contesto dello sviluppo e della prova dei sistemi di IA. In particolare i set di dati dovrebbero tenere conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, contestuale, comportamentale o funzionale nel quale il sistema di IA ad alto rischio è destinato a essere usato. I requisiti relativi alla governance dei dati possono essere soddisfatti ricorrendo a terzi che offrono servizi di conformità certificati, compresa la verifica della governance dei dati, dell'integrità dei set di dati e delle pratiche di addestramento, convalida e prova dei dati, purché sia garantita la conformità ai requisiti in materia di dati di cui al presente regolamento.

(68) Ai fini dello sviluppo e della valutazione di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli europei dell'innovazione digitale, gli impianti di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei settori di attività di tali attori soggetti 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 IA a partire da 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.

(69) Il diritto alla vita privata e alla protezione dei dati personali deve essere garantito durante l'intero ciclo di vita del sistema di IA. A tale riguardo, i principi della minimizzazione dei dati e della protezione dei dati fin dalla progettazione e per impostazione predefinita, sanciti dal diritto dell'Unione in materia di protezione dei dati, sono applicabili nel trattamento dei dati personali. Le misure adottate dai fornitori per garantire il rispetto di tali principi possono includere non solo l'anonimizzazione e la cifratura, ma anche l'uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di IA senza trasmissione tra le parti o copia degli stessi dati grezzi o strutturati, fatti salvi i requisiti in materia di governance dei dati di cui al presente regolamento.

(70) Al fine di proteggere i diritti altrui contro la discriminazione che potrebbe derivare dalla distorsione nei sistemi di IA, è opportuno che i fornitori, in via eccezionale e nella misura strettamente necessaria al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche e previa attuazione di tutte le condizioni applicabili previste dal presente regolamento unitamente alle condizioni previste dai regolamenti (UE) 2016/679 e (UE) 2018/1725 e dalla direttiva (UE) 2016/680, siano in grado di trattare anche categorie particolari di dati personali, come questione di interesse pubblico rilevante ai sensi dell'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679 e dell'articolo 10, paragrafo 2, lettera g), del regolamento (UE) 2018/1725.

(71) Disporre di informazioni comprensibili 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 consentire la tracciabilità di tali sistemi, verificare la conformità ai requisiti di cui al presente regolamento, monitorarne il funzionamento e svolgere il monitoraggio successivo all'immissione sul mercato. 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 e agevolare il monitoraggio successivo all'immissione sul mercato. 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 redatta in forma chiara e comprensibile. È opportuno tenere aggiornata in modo adeguato la documentazione tecnica durante l'intero ciclo di vita del sistema di IA. Inoltre, i sistemi di IA ad alto rischio dovrebbero consentire, a livello tecnico, la registrazione automatica degli eventi, mediante «log», per la durata del ciclo di vita del sistema.

(72) Per rispondere alle preoccupazioni relative all'opacità e alla complessità di determinati sistemi di IA e aiutare i deployer ad adempiere ai loro obblighi a norma del presente regolamento, è opportuno imporre la trasparenza per i sistemi di IA ad alto rischio prima che siano immessi sul mercato o messi in servizio. I sistemi di IA ad alto rischio dovrebbero essere progettati in modo da consentire ai deployer di comprendere il funzionamento del sistema di IA, valutarne la funzionalità e comprenderne i punti di forza e i limiti. I sistemi di IA ad alto rischio dovrebbero essere accompagnati da informazioni adeguate sotto forma di istruzioni per l'uso. Tali informazioni dovrebbero includere le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA. Tali elementi comprenderebbero informazioni su possibili circostanze note e prevedibili connesse all'uso del sistema di IA ad alto rischio, compresa l'azione del deployer suscettibile di influenzare il comportamento e le prestazioni del sistema, nel quadro dei quali il sistema di IA può comportare rischi per la salute, la sicurezza e i diritti fondamentali, sulle modifiche che sono state predeterminate e valutate a fini di conformità dal fornitore e sulle pertinenti misure di sorveglianza umana, comprese le misure volte a facilitare l'interpretazione degli output del sistema di IA da parte dei deployer. La trasparenza, comprese le istruzioni per l'uso che la accompagnano, dovrebbe aiutare i deployer a utilizzare il sistema e a prendere decisioni informate. Tra l'altro, i deployer dovrebbero essere nella posizione migliore per effettuare la scelta corretta del sistema che intendono utilizzare alla luce degli obblighi loro applicabili, essere a conoscenza degli usi previsti e vietati e utilizzare il sistema di IA in modo corretto e opportuno. Al fine di migliorare la leggibilità e l'accessibilità delle informazioni incluse nelle istruzioni per l'uso, se del caso, dovrebbero essere inclusi, esempi illustrativi, ad esempio sulle limitazioni e sugli usi previsti e vietati del sistema di IA. I fornitori dovrebbero garantire che tutta la documentazione, comprese le istruzioni per l'uso, contenga informazioni significative, complete, accessibili e comprensibili, tenendo conto delle esigenze e delle conoscenze prevedibili dei deployer destinatari. Le istruzioni per l'uso dovrebbero essere messe a disposizione in una lingua che possa essere compresa facilmente dai deployer destinatari, secondo quanto stabilito dallo Stato membro interessato.

(73) I sistemi di IA ad alto rischio dovrebbero essere progettati e sviluppati in modo da consentire alle persone fisiche di sorvegliarne il funzionamento, garantire che siano utilizzati come previsto e che i loro impatti siano affrontati durante il ciclo di vita del sistema. 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. È inoltre essenziale, se del caso, garantire che i sistemi di IA ad alto rischio includano meccanismi per guidare e informare la persona fisica alla quale è stata affidata la sorveglianza umana affinché prenda decisioni informate in merito alla possibilità, ai tempi e alle modalità di intervento, onde evitare conseguenze negative o rischi, oppure affinché arresti il sistema, qualora non funzionasse come previsto. Tenuto conto delle conseguenze significative per le persone in caso di una corrispondenza non corretta da parte di determinati sistemi di identificazione biometrica, è opportuno prevedere un requisito rafforzato di sorveglianza umana per tali sistemi, in modo che il deployer non possa adottare alcuna azione o decisione sulla base dell'identificazione risultante dal sistema, a meno che ciò non sia stato verificato e confermato separatamente da almeno due persone fisiche. Tali persone potrebbero provenire da una o più entità e comprendere la persona che gestisce o utilizza il sistema. Tale requisito non dovrebbe comportare oneri o ritardi inutili e potrebbe essere sufficiente che le verifiche separate da parte delle diverse persone siano automaticamente registrate nei log generati dal sistema. Date le specificità dei settori delle attività di contrasto, della migrazione, del controllo delle frontiere e dell'asilo, tale requisito non dovrebbe applicarsi se il diritto dell'Unione o nazionale ritenga sproporzionata la sua applicazione.

(74) 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, alla luce della loro finalità prevista e conformemente allo stato dell'arte generalmente riconosciuto. La Commissione e le organizzazioni e i portatori di interessi pertinenti sono incoraggiati a tenere in debita considerazione l'attenuazione dei rischi e degli impatti negativi del sistema di IA. Il livello atteso delle metriche di prestazione dovrebbe essere dichiarato nelle istruzioni per l'uso che accompagnano il sistema. I fornitori sono invitati a comunicare tali informazioni ai deployer in modo chiaro e facilmente comprensibile, senza malintesi o affermazioni fuorvianti. Il diritto dell'Unione in materia di metrologia legale, comprese le direttive 2014/31/UE ([35]) e 2014/32/UE ([36]) del Parlamento europeo e del Consiglio, mira a garantire l'accuratezza delle misurazioni e a favorire la trasparenza e l'equità delle transazioni commerciali. In tale contesto, in cooperazione con i portatori di interessi e le organizzazioni pertinenti, quali le autorità di metrologia e di analisi comparativa, la Commissione dovrebbe incoraggiare, se del caso, lo sviluppo di parametri di riferimento e metodologie di misurazione per i sistemi di IA. A tal fine, la Commissione dovrebbe prendere atto dei partner internazionali che operano nel settore della metrologia, collaborando con essi, e dei pertinenti indicatori di misurazione relativi all'IA.

([35]) Direttiva 2014/31/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di strumenti per pesare a funzionamento non automatico (GU L 96 del 29.3.2014, pag. 107).

([36]) Direttiva 2014/32/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di strumenti di misura (GU L 96 del 29.3.2014, pag. 149).

(75) La robustezza tecnica è un requisito fondamentale dei sistemi di IA ad alto rischio. Essi dovrebbero essere resilienti in relazione a comportamenti dannosi o altrimenti indesiderati che possono derivare da limitazioni all'interno dei sistemi o dell'ambiente in cui i sistemi funzionano (ad esempio errori, guasti, incongruenze, situazioni impreviste). È pertanto opportuno adottare misure tecniche e organizzative per garantire la robustezza dei sistemi di IA ad alto rischio, ad esempio progettando e sviluppando soluzioni tecniche adeguate per prevenire o ridurre al minimo i comportamenti dannosi o altrimenti indesiderati. Tali soluzioni tecniche possono comprendere, ad esempio, meccanismi che consentano al sistema di interrompere in modo sicuro il proprio funzionamento (piani fail-safe) in presenza di determinate anomalie o quando il funzionamento ha luogo al di fuori di determinati limiti prestabiliti. La mancata protezione da tali rischi potrebbe avere ripercussioni sulla sicurezza o incidere negativamente sui diritti fondamentali, ad esempio a causa di decisioni errate o di output sbagliati o distorti generati dal sistema di IA.

(76) 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 il data poisoning, «avvelenamento dei dati») o i modelli addestrati (ad esempio gli adversarial attacks, «attacchi antagonisti» o la membership inference, «attacchi inferenziali»), 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, come controlli di sicurezza, anche tenendo debitamente conto dell'infrastruttura TIC sottostante.

(77) Fatti salvi i requisiti relativi alla robustezza e all'accuratezza di cui al presente regolamento, i sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, ai sensi di tale regolamento possono dimostrare la conformità ai requisiti di cibersicurezza del presente regolamento rispettando i requisiti essenziali di cibersicurezza a norma di tale regolamento. Quando rispettano i requisiti essenziali del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, i sistemi di IA ad alto rischio dovrebbero essere considerati conformi ai requisiti di cibersicurezza di cui al presente regolamento nella misura in cui il rispetto di tali requisiti sia dimostrato nella dichiarazione di conformità UE, o in parti di essa, rilasciata a norma di tale regolamento. A tal fine, la valutazione dei rischi di cibersicurezza, associati a un prodotto con elementi digitali classificati come sistemi di IA ad alto rischio ai sensi del presente regolamento, effettuata a norma del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, dovrebbe tenere in considerazione i rischi per la ciberresilienza di un sistema di IA per quanto riguarda i tentativi di terzi non autorizzati di modificarne l'uso, il comportamento o le prestazioni, comprese le vulnerabilità specifiche dell'IA, quali il data poisoning («avvelenamento dei dati») o gli adversarial attack («attacchi antagonisti»), nonché, se del caso, i rischi per i diritti fondamentali come disposto dal presente regolamento.

(78) La procedura di valutazione della conformità di cui al presente regolamento dovrebbe applicarsi in relazione ai requisiti essenziali di cibersicurezza di un prodotto con elementi digitali disciplinato dal regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e classificato come sistema di IA ad alto rischio a norma del presente regolamento. Tuttavia, tale norma non dovrebbe comportare una riduzione del livello di garanzia necessario per i prodotti con elementi digitali critici disciplinati dal regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali. Pertanto, in deroga a detta norma, i sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento e che sono anche qualificati come prodotti con elementi digitali importanti e critici a norma del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno in allegato al presente regolamento, sono soggetti alle disposizioni in materia di valutazione della conformità del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali per quanto riguarda i requisiti essenziali di cibersicurezza di tale regolamento. In tal caso, per tutti gli altri aspetti disciplinati dal presente regolamento dovrebbero applicarsi le rispettive disposizioni in materia di valutazione della conformità basata sul controllo interno, in allegato al presente regolamento. Sulla base delle conoscenze e delle competenze dell'ENISA in merito alla politica in materia di cibersicurezza e ai relativi compiti assegnati all'ENISA a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([37]), la Commissione dovrebbe cooperare con l'ENISA sulle questioni relative alla cibersicurezza dei sistemi di IA.

([37]) 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).

(79) 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.

(80) In qualità di firmatari della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, l'Unione e gli Stati membri sono tenuti, dal punto di vista giuridico, a proteggere le persone con disabilità dalla discriminazione e a promuoverne l'uguaglianza, a garantire che le persone con disabilità abbiano accesso, su un piano di parità con gli altri, alle tecnologie e ai sistemi di informazione e comunicazione e a garantire il rispetto della vita privata delle persone con disabilità. In considerazione dell'importanza e dell'utilizzo crescenti dei sistemi di IA, l'applicazione dei principi della progettazione universale a tutti i nuovi servizi e tecnologie dovrebbe garantire un accesso pieno e paritario a tutti coloro che sono potenzialmente interessati dalle tecnologie di IA o che le utilizzano, ivi comprese le persone con disabilità, in modo da tenere pienamente conto delle loro dignità e diversità intrinseche. È pertanto essenziale che i fornitori garantiscano la piena conformità ai requisiti di accessibilità, anche alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio ([38]) e alla direttiva (UE) 2019/882. I fornitori dovrebbero garantire il rispetto di tali requisiti fin dalla progettazione. Pertanto, le misure necessarie dovrebbero essere quanto più possibile integrate nella progettazione dei sistemi di IA ad alto rischio.

(81) 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. I fornitori di sistemi di IA ad alto rischio che sono soggetti a obblighi relativi ai sistemi di gestione della qualità conformemente al pertinente diritto settoriale dell'Unione dovrebbero avere la possibilità di includere gli elementi del sistema di gestione della qualità di cui al presente regolamento nell'ambito del sistema di gestione della qualità esistente previsto da tale altro diritto settoriale dell'Unione. La complementarità tra il presente regolamento e il diritto settoriale vigente dell'Unione dovrebbe essere tenuta in considerazione anche nelle future attività di normazione o negli orientamenti adottati dalla Commissione. 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 interessata.

(82) 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, i fornitori stabiliti in paesi terzi dovrebbero nominare, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione. Tale rappresentante autorizzato svolge un ruolo chiave nel garantire la conformità dei sistemi di IA ad alto rischio immessi sul mercato o messi in servizio nell'Unione da tali fornitori non stabiliti nell'Unione e nel servire da loro referente stabilito nell'Unione.

(83) Alla luce della natura e della complessità della catena del valore per i sistemi di IA e in linea con il nuovo quadro legislativo, è essenziale garantire la certezza del diritto e facilitare il rispetto del presente regolamento. È pertanto necessario chiarire il ruolo e gli obblighi specifici degli operatori pertinenti lungo tale catena del valore, come importatori e distributori che possono contribuire allo sviluppo dei sistemi di IA. In determinate situazioni tali operatori potrebbero agire contemporaneamente in più di un ruolo e dovrebbero pertanto adempiere cumulativamente tutti gli obblighi pertinenti associati a tali ruoli. Ad esempio, un operatore potrebbe agire contemporaneamente come distributore e importatore.

(84) Al fine di garantire la certezza del diritto, è necessario chiarire che, a determinate condizioni specifiche, qualsiasi distributore, importatore, deployer o altro terzo dovrebbe essere considerato un fornitore di un sistema di IA ad alto rischio e, pertanto, assumere tutti gli obblighi del caso. Ciò si verifica ove tale parte apponga il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi. Ciò si verifica anche ove tale parte apporti una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio e in modo che resti un sistema di IA ad alto rischio a norma del presente regolamento, ovvero ove modifichi la finalità prevista di un sistema di IA, compreso un sistema di IA per finalità generali, che non è stato classificato come sistema ad alto rischio ed è già immesso sul mercato o messo in servizio, in modo tale da rendere il sistema di IA un sistema di IA ad alto rischio a norma del presente regolamento. Tali disposizioni dovrebbero applicarsi fatte salve le disposizioni più specifiche stabilite in alcune normative di armonizzazione dell'Unione basate sul nuovo quadro legislativo, unitamente al quale dovrebbe applicarsi il presente regolamento. Ad esempio, l'articolo 16, paragrafo 2, del

([38]) Direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio, del 26 ottobre 2016, relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici (GU L 327 del 2.12.2016, pag. 1).

regolamento (UE) 2017/745, che stabilisce che talune modifiche non dovrebbero essere considerate modifiche di un dispositivo tali da compromettere la sua conformità alle prescrizioni applicabili, dovrebbe continuare ad applicarsi ai sistemi di IA ad alto rischio che sono dispositivi medici ai sensi di tale regolamento.

(85) I sistemi di IA per finalità generali possono essere utilizzati da soli come sistemi di IA ad alto rischio o essere componenti di altri sistemi di IA ad alto rischio. Pertanto, data la loro natura particolare e al fine di garantire un'equa ripartizione delle responsabilità lungo la catena del valore dell'IA, i fornitori di tali sistemi, indipendentemente dal fatto che questi possano essere utilizzati di per sé come sistemi di IA ad alto rischio da altri fornitori o come componenti di sistemi di IA ad alto rischio, e salvo se diversamente disposto dal presente regolamento, dovrebbero cooperare strettamente con i fornitori dei pertinenti sistemi di IA ad alto rischio per consentire loro di conformarsi ai pertinenti obblighi previsti dal presente regolamento e con le autorità competenti istituite a norma del presente regolamento.

(86) Qualora, alle condizioni di cui al presente regolamento, il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA non dovesse più essere considerato il fornitore ai fini del presente regolamento, e se tale fornitore non ha espressamente escluso la modifica del sistema di IA in un sistema di IA ad alto rischio, il precedente fornitore dovrebbe comunque cooperare strettamente e mettere a disposizione le informazioni necessarie nonché fornire l'accesso tecnico ragionevolmente atteso e qualsiasi altra forma di assistenza che sono richiesti per l'adempimento degli obblighi di cui al presente regolamento, in particolare per quanto riguarda la conformità alla valutazione della conformità dei sistemi di IA ad alto rischio.

(87) Inoltre, se un sistema di IA ad alto rischio che è un componente di sicurezza di un prodotto rientrante nell'ambito di applicazione della normativa di armonizzazione dell'Unione basata sul nuovo quadro legislativo non è immesso sul mercato o messo in servizio separatamente dal prodotto, il fabbricante del prodotto quale definito in tale normativa dovrebbe adempiere gli obblighi del fornitore stabiliti nel presente regolamento e, in particolare, dovrebbe garantire che il sistema di IA integrato nel prodotto finale soddisfa i requisiti del presente regolamento.

(88) Lungo la catena del valore dell'IA, spesso più parti forniscono sistemi di IA, strumenti e servizi, ma anche componenti o processi, che sono integrati dal fornitore nel sistema di IA con varie finalità, inclusi l'addestramento dei modelli, la riqualificazione dei modelli, la prova e la valutazione dei modelli, l'integrazione nel software o altri aspetti dello sviluppo dei modelli. Tali parti svolgono un ruolo importante nella catena del valore nei confronti del fornitore del sistema di IA ad alto rischio in cui i loro sistemi di IA, strumenti, servizi, componenti o processi sono integrati e dovrebbero fornire a tale fornitore mediante accordo scritto le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari sulla base dello stato dell'arte generalmente riconosciuto, al fine di consentire al fornitore di adempiere pienamente gli obblighi di cui al presente regolamento, senza compromettere i propri diritti di proprietà intellettuale o segreti commerciali.

(89) I terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti di IA diversi dai modelli di IA per finalità generali non dovrebbero essere tenuti a conformarsi a requisiti relativi alle responsabilità lungo la catena del valore dell'IA, in particolare nei confronti del fornitore che li ha utilizzati o integrati, quando tali strumenti, servizi, processi o componenti di IA sono resi accessibili con licenza libera e open source. Gli sviluppatori di strumenti, servizi, processi o componenti di IA liberi e open source diversi dai modelli di IA per finalità generali dovrebbero essere incoraggiati ad attuare pratiche di documentazione ampiamente adottate, come schede di modelli e schede dati, al fine di accelerare la condivisione delle informazioni lungo la catena del valore dell'IA, consentendo la promozione di sistemi di IA affidabili nell'Unione.

(90) La Commissione potrebbe elaborare e raccomandare clausole contrattuali tipo volontarie tra i fornitori di sistemi di IA ad alto rischio e i terzi che forniscono strumenti, servizi, componenti o processi utilizzati o integrati in sistemi di IA ad alto rischio, al fine di agevolare la cooperazione lungo la catena del valore. Nell'elaborare clausole contrattuali tipo volontarie, la Commissione dovrebbe altresì tenere conto dei possibili requisiti contrattuali applicabili in determinati settori o casi commerciali.

(91) 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 i deployer. È in particolare opportuno che i deployer adottino misure tecniche e organizzative adeguate per garantire di utilizzare 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. Inoltre, i deployer dovrebbero garantire che le persone alle quali è affidata l'attuazione delle istruzioni per l'uso e della sorveglianza umana di cui al presente regolamento dispongano delle competenze necessarie, in particolare un livello

adeguato di alfabetizzazione, formazione e autorità in materia di IA per svolgere adeguatamente tali compiti. Tali obblighi dovrebbero lasciare impregiudicati altri obblighi dei deployer in relazione ai sistemi di IA ad alto rischio previsti dal diritto dell'Unione o nazionale.

(92) Il presente regolamento lascia impregiudicati gli obblighi dei datori di lavoro di informare o di informare e consultare i lavoratori o i loro rappresentanti a norma del diritto e delle prassi dell'Unione o nazionali, compresa la direttiva 2002/14/CE del Parlamento europeo e del Consiglio ([39]), in merito alle decisioni di mettere in servizio o utilizzare sistemi di IA. Rimane necessario garantire che i lavoratori e i loro rappresentanti siano informati in merito alla diffusione programmata dei sistemi di IA ad alto rischio sul luogo di lavoro, qualora non siano soddisfatte le condizioni per tali obblighi di informazione o di informazione e consultazione previsti da altri strumenti giuridici. Inoltre, tale diritto di informazione è accessorio e necessario rispetto all'obiettivo di tutelare i diritti fondamentali alla base del presente regolamento. È pertanto opportuno prevedere nel presente regolamento un obbligo di informazione con tale finalità, lasciando impregiudicati i diritti esistenti dei lavoratori.

(93) Se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche dal modo in cui tali sistemi di IA sono utilizzati. I deployer di sistemi di IA ad alto rischio svolgono pertanto un ruolo fondamentale nel garantire la tutela dei diritti fondamentali, integrando gli obblighi del fornitore nello sviluppo del sistema di IA. I deployer sono nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili. I deployer dei sistemi di IA ad alto rischio elencati in un allegato del presente regolamento svolgono inoltre un ruolo cruciale per informare le persone fisiche e, quando adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche, dovrebbero informare, se del caso, queste ultime che sono soggette all'uso del sistema di IA ad alto rischio. Tale informazione dovrebbe includere la finalità prevista e il tipo di decisioni adottate. Il deployer dovrebbe informare inoltre le persone fisiche del loro diritto a una spiegazione previsto dal presente regolamento. Per quanto riguarda i sistemi di IA ad alto rischio utilizzati a fini di attività di contrasto, tale obbligo dovrebbe essere attuato conformemente all'articolo 13 della direttiva (UE) 2016/680.

(94) Qualsiasi trattamento di dati biometrici interessati dall'uso di sistemi di IA a fini di identificazione biometrica a scopo di contrasto deve essere conforme all'articolo 10 della direttiva (UE) 2016/680, che consente tale trattamento solo se strettamente necessario, fatte salve le tutele adeguate per i diritti e le libertà dell'interessato, e se autorizzato dal diritto dell'Unione o degli Stati membri. Tale uso, se autorizzato, deve inoltre rispettare i principi di cui all'articolo 4, paragrafo 1, della direttiva (UE) 2016/680, tra cui liceità, correttezza e trasparenza, determinazione delle finalità, esattezza e limitazione della conservazione.

(95) Fatto salvo il diritto dell'Unione applicabile, in particolare il regolamento (UE) 2016/679 e la direttiva (UE) 2016/680, tenendo in considerazione la natura invasiva dei sistemi di identificazione biometrica remota a posteriori, l'uso di tali sistemi dovrebbe essere soggetto a tutele. I sistemi di identificazione biometrica remota a posteriori dovrebbero sempre essere utilizzati in modo proporzionato, legittimo e strettamente necessario e quindi mirato, per quanto riguarda le persone da identificare, il luogo e l'ambito temporale e sulla base di un set di dati chiuso di filmati acquisiti legalmente. In ogni caso, i sistemi di identificazione biometrica remota a posteriori non dovrebbero essere utilizzati nel quadro delle attività di contrasto per condurre una sorveglianza indiscriminata. Le condizioni per l'identificazione biometrica remota a posteriori non dovrebbero, in ogni caso, fornire una base per eludere le condizioni del divieto e le rigorose eccezioni per l'identificazione biometrica remota «in tempo reale».

(96) Al fine di garantire in modo efficiente la tutela dei diritti fondamentali, i deployer di sistemi di IA ad alto rischio che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici e deployer di taluni sistemi di IA ad alto rischio elencati nell'allegato del presente regolamento, come i soggetti bancari o assicurativi, dovrebbero svolgere una valutazione d'impatto sui diritti fondamentali prima di metterli in uso. I servizi importanti di natura pubblica per le persone possono essere forniti anche da soggetti privati. Gli enti privati che forniscono tali servizi pubblici sono legati a compiti di interesse pubblico, ad esempio nei settori dell'istruzione, dell'assistenza sanitaria, dei servizi sociali, degli alloggi e dell'amministrazione della giustizia. L'obiettivo della valutazione d'impatto sui diritti fondamentali è consentire al deployer di individuare i rischi specifici per i diritti delle persone o dei gruppi di persone che potrebbero essere interessati e di individuare le misure da adottare al concretizzarsi di tali rischi. La valutazione

([39]) Direttiva 2002/14/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2002, che istituisce un quadro generale relativo all'informazione e alla consultazione dei lavoratori — (GU L 80 del 23.3.2002, pag. 29).

d'impatto dovrebbe essere svolta prima del primo impiego del sistema di IA ad alto rischio e dovrebbe essere aggiornata quando il deployer ritiene che uno qualsiasi dei fattori pertinenti sia cambiato. La valutazione d'impatto dovrebbe individuare i processi pertinenti del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista e dovrebbe includere una descrizione del periodo di tempo in cui il sistema è destinato a essere usato e della relativa frequenza, nonché delle categorie specifiche di persone fisiche e gruppi che potrebbero essere interessati nel contesto specifico di utilizzo. La valutazione dovrebbe altresì comprendere l'individuazione di rischi specifici di danno che possono incidere sui diritti fondamentali di tali persone o gruppi. Nell'effettuare tale valutazione, il deployer dovrebbe tenere conto delle informazioni pertinenti per un'adeguata valutazione dell'impatto, comprese, tra l'altro, le informazioni trasmesse dal fornitore del sistema di IA ad alto rischio nelle istruzioni per l'uso. Alla luce dei rischi individuati, i deployer dovrebbero stabilire le misure da adottare al concretizzarsi di tali rischi, compresi, ad esempio, i meccanismi di governance in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana secondo le istruzioni per l'uso, o le procedure di gestione dei reclami e di ricorso, dato che potrebbero essere determinanti nell'attenuare i rischi per i diritti fondamentali in casi d'uso concreti. Dopo aver effettuato tale valutazione d'impatto, il deployer dovrebbe darne notifica alla pertinente autorità di vigilanza del mercato. Se del caso, per raccogliere le informazioni pertinenti necessarie a effettuare la valutazione d'impatto, i deployer di sistemi di IA ad alto rischio, in particolare quando i sistemi di IA sono utilizzati nel settore pubblico, potrebbero coinvolgere i portatori di interessi pertinenti, compresi i rappresentanti di gruppi di persone che potrebbero essere interessati dal sistema di IA, gli esperti indipendenti e le organizzazioni della società civile nello svolgimento di tali valutazioni d'impatto e nella progettazione delle misure da adottare al concretizzarsi dei rischi. L'ufficio europeo per l'IA («ufficio per l'IA») dovrebbe elaborare un modello di questionario al fine di agevolare la conformità e ridurre gli oneri amministrativi per i deployer.

(97) La nozione di modelli di IA per finalità generali dovrebbe essere chiaramente definita e distinta dalla nozione di sistemi di IA per consentire la certezza del diritto. La definizione dovrebbe basarsi sulle principali caratteristiche funzionali di un modello di IA per finalità generali, in particolare la generalità e la capacità di svolgere con competenza un'ampia gamma di compiti distinti. Questi modelli sono solitamente addestrati su grandi quantità di dati con diversi metodi, come l'apprendimento autosupervisionato, non supervisionato o per rinforzo. I modelli di IA per finalità generali possono essere immessi sul mercato in vari modi, tra cui biblioteche, interfacce di programmazione delle applicazioni (API), download diretto o copia fisica. Tali modelli possono essere ulteriormente modificati o perfezionati con nuovi modelli. Sebbene i modelli di IA siano componenti essenziali dei sistemi di IA, essi non costituiscono di per sé sistemi di IA. I modelli di IA necessitano dell'aggiunta di altri componenti, ad esempio un'interfaccia utente, per diventare sistemi di IA. I modelli di IA sono generalmente integrati nei sistemi di IA e ne fanno parte. Il presente regolamento stabilisce norme specifiche per i modelli di IA per finalità generali e per i modelli di IA per finalità generali che presentano rischi sistemici, le quali dovrebbero applicarsi anche quando tali modelli sono integrati o fanno parte di un sistema di IA. Resta inteso che gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero applicarsi una volta che i modelli di IA per finalità generali sono immessi sul mercato. Quando il fornitore di un modello di IA per finalità generali integra un modello proprio nel suo sistema di IA messo a disposizione sul mercato o messo in servizio, tale modello dovrebbe essere considerato immesso sul mercato e, pertanto, gli obblighi di cui al presente regolamento per i modelli dovrebbero continuare ad applicarsi in aggiunta a quelli per i sistemi di IA. Gli obblighi previsti per i modelli non dovrebbero in ogni caso applicarsi quando un modello proprio è utilizzato per processi puramente interni che non sono essenziali per fornire un prodotto o un servizio a terzi e i diritti delle persone fisiche restano impregiudicati. Considerati i loro potenziali effetti negativi significativi, i modelli di IA per finalità generali con rischio sistemico dovrebbero sempre essere soggetti ai pertinenti obblighi a norma del presente regolamento. La definizione non dovrebbe includere i modelli di IA utilizzati prima della loro immissione sul mercato solo a scopo di ricerca, sviluppo e prototipazione. Ciò non pregiudica l'obbligo di conformarsi al presente regolamento quando, in seguito a tali attività, un modello è immesso sul mercato.

(98) Mentre la generalità di un modello potrebbe, tra gli altri criteri, essere determinata anche da una serie di parametri, i modelli con almeno un miliardo di parametri e addestrati con grandi quantità di dati utilizzando l'autosupervisione su larga scala dovrebbero ritenersi caratterizzati da una generalità significativa e in grado di svolgere con competenza un'ampia gamma di compiti distinti.

(99) I grandi modelli di IA generativi sono un tipico esempio di modello di IA per finalità generali, dato che consentono una generazione flessibile di contenuti, ad esempio sotto forma di testo, audio, immagini o video, che possono prontamente rispondere a un'ampia gamma di compiti distinti.

(100) Quando un modello di IA per finalità generali è integrato in un sistema di IA o ne fa parte, tale sistema dovrebbe essere considerato un sistema di IA per finalità generali qualora, a causa di tale integrazione, il sistema abbia la capacità di perseguire varie finalità. Un sistema di IA per finalità generali può essere utilizzato direttamente o può essere integrato in altri sistemi di IA.

(101) I fornitori di modelli di IA per finalità generali hanno un ruolo e una responsabilità particolari lungo la catena del valore dell'IA, poiché i modelli che forniscono possono costituire la base per una serie di sistemi a valle, spesso forniti da fornitori a valle che richiedono una buona comprensione dei modelli e delle loro capacità, sia per consentire l'integrazione di tali modelli nei loro prodotti, sia per adempiere i rispettivi obblighi a norma del presente regolamento o di altri regolamenti. È pertanto opportuno prevedere misure di trasparenza proporzionate, tra cui la redazione e l'aggiornamento della documentazione e la fornitura di informazioni sul modello di IA per finalità generali ai fini del suo utilizzo da parte dei fornitori a valle. La documentazione tecnica dovrebbe essere preparata e tenuta aggiornata dal fornitore del modello di IA per finalità generali allo scopo di metterla a disposizione, su richiesta, dell'ufficio per l'IA e delle autorità nazionali competenti. La serie minima di elementi da includere in tale documentazione dovrebbe essere stabilita in specifici allegati del presente regolamento. Alla Commissione dovrebbe essere conferito il potere di modificare tali allegati mediante atti delegati alla luce degli sviluppi tecnologici in evoluzione.

(102) I software e i dati, compresi i modelli, rilasciati con licenza libera e open source che consentano loro di essere condivisi apertamente e che gli utenti possano liberamente consultare, utilizzare, modificare e ridistribuire, comprese le loro versioni modificate, possono contribuire alla ricerca e all'innovazione nel mercato e possono offrire notevoli opportunità di crescita per l'economia dell'Unione. I modelli di IA per finalità generali rilasciati con licenza libera e open source dovrebbero essere presi in considerazione per garantire elevati livelli di trasparenza e apertura, se i loro parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici. La licenza dovrebbe essere considerata libera e open source anche quando consente agli utenti di eseguire, copiare, distribuire, studiare, modificare e migliorare i software e i dati, compresi i modelli, purché il modello sia attribuito al fornitore originario e siano rispettate condizioni di distribuzione identiche o comparabili.

(103) I componenti di IA liberi e open source comprendono i software e i dati, compresi i modelli e i modelli di IA per finalità generali, gli strumenti, i servizi o i processi di un sistema di IA. I componenti di IA liberi e open source possono essere forniti attraverso diversi canali e possono inoltre essere sviluppati su archivi aperti. Ai fini del presente regolamento, i componenti di IA forniti a pagamento o altrimenti monetizzati, anche tramite la fornitura di assistenza tecnica o altri servizi, ad esempio attraverso una piattaforma software, in relazione al componente di IA, o l'utilizzo di dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software, ad eccezione delle transazioni tra microimprese, non dovrebbero beneficiare delle eccezioni previste per i componenti di IA liberi e open source. La messa a disposizione di componenti di IA tramite archivi aperti non dovrebbe, di per sé, costituire monetizzazione.

(104) I fornitori di modelli di IA per finalità generali che sono rilasciati con licenza libera e open source e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono messi pubblicamente a disposizione dovrebbero essere soggetti ad eccezioni per quanto riguarda i requisiti relativi alla trasparenza imposti ai modelli di IA per finalità generali, a meno che non si possa ritenere che presentino un rischio sistemico, nel qual caso la circostanza che il modello sia trasparente e corredato di una licenza open source non dovrebbe ritenersi un motivo sufficiente per escludere la conformità agli obblighi di cui al presente regolamento. In ogni caso, dato che il rilascio di modelli di IA per finalità generali con licenza libera e open source non rivela necessariamente informazioni sostanziali sul set di dati utilizzato per l'addestramento o il perfezionamento del modello e sulla modalità con cui è stata in tal modo garantita la conformità al diritto d'autore, l'eccezione prevista per i modelli di IA per finalità generali concernente il rispetto dei requisiti relativi alla trasparenza non dovrebbe riguardare l'obbligo di produrre una sintesi del contenuto utilizzato per l'addestramento dei modelli e l'obbligo di attuare una politica volta ad adempiere la normativa europea in materia di diritto d'autore, in particolare di individuare e rispettare la riserva dei diritti a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio ([40]).

(105) I modelli di IA per finalità generali, in particolare i grandi modelli di IA generativa, in grado di generare testo, immagini e altri contenuti, presentano opportunità di innovazione uniche, ma anche sfide per artisti, autori e altri creatori e per le modalità con cui i loro contenuti creativi sono creati, distribuiti, utilizzati e fruiti. Lo sviluppo e l'addestramento di tali modelli richiedono l'accesso a grandi quantità di testo, immagini, video e altri dati. Le tecniche di estrazione di testo e di dati possono essere ampiamente utilizzate in tale contesto per il reperimento e l'analisi di tali contenuti, che possono essere protetti da diritto d'autore e da diritti connessi. Qualsiasi utilizzo di contenuti protetti da diritto d'autore richiede l'autorizzazione del titolare dei diritti interessato, salvo se si applicano eccezioni e limitazioni pertinenti al diritto d'autore. La direttiva (UE) 2019/790 ha introdotto eccezioni e limitazioni che consentono, a determinate condizioni, riproduzioni ed estrazioni effettuate da opere o altri materiali ai fini

([40]) Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (GU L 130 del 17.5.2019, pag. 92).

dell'estrazione di testo e di dati. In base a tali norme, i titolari dei diritti hanno la facoltà di scegliere che l'utilizzo delle loro opere e di altri materiali sia da essi riservato per evitare l'estrazione di testo e di dati, salvo a fini di ricerca scientifica. Qualora il diritto di sottrarsi sia stato espressamente riservato in modo appropriato, i fornitori di modelli di IA per finalità generali devono ottenere un'autorizzazione dai titolari dei diritti, qualora intendano compiere l'estrazione di testo e di dati su tali opere.

(106) I fornitori che immettono modelli di IA per finalità generali sul mercato dell'Unione dovrebbero garantire la conformità ai pertinenti obblighi del presente regolamento. A tal fine, i fornitori di modelli di IA per finalità generali dovrebbero mettere in atto una politica volta a rispettare il diritto dell'Unione in materia di diritto d'autore e diritti connessi, in particolare per individuare e rispettare la riserva dei diritti espresse dai titolari dei diritti a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790. Qualsiasi fornitore che immetta sul mercato dell'Unione un modello di IA per finalità generali dovrebbe rispettare tale obbligo, indipendentemente dalla giurisdizione in cui hanno luogo gli atti pertinenti in materia di diritto d'autore alla base dell'addestramento di tali modelli di IA per finalità generali. Ciò è necessario per garantire condizioni di parità tra i fornitori di modelli di IA per finalità generali, dato che nessun fornitore dovrebbe essere in grado di ottenere un vantaggio competitivo nel mercato dell'Unione applicando norme in materia di diritto d'autore meno rigorose di quelle previste nell'Unione.

(107) Al fine di aumentare la trasparenza sui dati utilizzati nelle fasi di pre-addestramento e addestramento dei modelli di IA per finalità generali, compresi testo e dati protetti dalla normativa sul diritto d'autore, è opportuno che i fornitori di tali modelli elaborino e mettano a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali. Pur tenendo debitamente conto della necessità di proteggere i segreti commerciali e le informazioni commerciali riservate, la presente sintesi dovrebbe essere di respiro ampio e generale, anziché dettagliata sotto il profilo tecnico, al fine di agevolare le parti con interessi legittimi, compresi i titolari dei diritti d'autore, nell'esercitare e far rispettare i loro diritti ai sensi del diritto dell'Unione, ad esempio elencando le principali raccolte o serie di dati che sono state inserite nell'addestramento del modello, quali grandi banche dati o archivi di dati privati o pubblici, e fornendo una descrizione delle altre fonti di dati utilizzate. È opportuno che l'ufficio per l'IA fornisca un modello per la sintesi, che dovrebbe essere semplice ed efficace nonché consentire al fornitore di fornire la sintesi richiesta in forma descrittiva.

(108) In merito agli obblighi imposti ai fornitori di modelli di IA per finalità generali per quanto riguarda l'attuazione di una politica volta a rispettare la normativa dell'Unione in materia di diritto d'autore e a mettere pubblicamente a disposizione una sintesi dei contenuti utilizzati per l'addestramento, l'ufficio per l'IA dovrebbe controllare se il fornitore ha adempiuto tali obblighi senza verificare o procedere a una valutazione puntuale dei dati di addestramento in termini di conformità al diritto d'autore. Il presente regolamento non pregiudica l'applicazione delle norme sul diritto d'autore previste dal diritto dell'Unione.

(109) Il rispetto degli obblighi applicabili ai fornitori di modelli di IA per finalità generali dovrebbe essere commisurato e proporzionato al tipo di fornitore del modello, escludendo la necessità di adempimento per le persone che sviluppano o utilizzano modelli per finalità non professionali o di ricerca scientifica, le quali dovrebbero tuttavia essere incoraggiate a rispettare volontariamente tali obblighi. Fatta salva la normativa dell'Unione in materia di diritto d'autore, il rispetto di tali obblighi dovrebbe tenere debitamente conto delle dimensioni del fornitore e consentire modalità semplificate di adempimento per le PMI, comprese le start-up, che non dovrebbero comportare costi eccessivi né scoraggiare l'uso di tali modelli. In caso di modifica o perfezionamento di un modello, gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero essere limitati a tale modifica o perfezionamento, ad esempio integrando la documentazione tecnica già esistente con informazioni sulle modifiche, comprese nuove fonti di dati di addestramento, quale mezzo per adempiere gli obblighi della catena del valore di cui al presente regolamento.

(110) I modelli di IA per finalità generali potrebbero comportare rischi sistemici che includono, tra l'altro, qualsiasi effetto negativo effettivo o ragionevolmente prevedibile in relazione a incidenti gravi, perturbazioni di settori critici e serie conseguenze per la salute e la sicurezza pubbliche; eventuali effetti negativi, effettivi o ragionevolmente prevedibili, sui processi democratici e sulla sicurezza pubblica ed economica; la diffusione di contenuti illegali, mendaci o discriminatori. I rischi sistemici sono da intendersi in aumento con le capacità e la portata del modello, possono emergere durante l'intero ciclo di vita del modello e sono influenzati da condizioni di uso improprio, affidabilità, equità e sicurezza del modello, il livello di autonomia del modello, dal suo accesso agli strumenti, dalle sue modalità nuove o combinate, dalle strategie di rilascio e distribuzione, dal potenziale di rimozione delle misure protettive e da altri fattori. In particolare, gli approcci internazionali hanno finora rilevato la necessità di prestare attenzione ai rischi derivanti da potenziali usi impropri intenzionali o da involontari problemi di controllo relativi all'allineamento con l'intento umano; ai rischi chimici, biologici, radiologici e nucleari, come le modalità con cui ridurre gli ostacoli

all'accesso, anche per quanto riguarda lo sviluppo e l'uso di armi o la relativa acquisizione di progetti; alle capacità informatiche offensive, come le modalità per consentire la scoperta, lo sfruttamento o l'uso operativo delle vulnerabilità; agli effetti dell'interazione e dell'uso di strumenti, compresa, ad esempio, la capacità di controllare i sistemi fisici e di interferire con infrastrutture critiche; ai rischi derivanti da modelli che realizzano copie di sé stessi o «autoreplicanti» o che addestrano altri modelli; alle modalità con cui i modelli possono dar luogo a dannosi pregiudizi e discriminazioni con rischi per gli individui, le comunità o le società; all'agevolazione della disinformazione o alla violazione della vita privata con minacce ai valori democratici e ai diritti umani; al rischio che un particolare evento possa provocare una reazione a catena con notevoli effetti negativi che potrebbero interessare fino a un'intera città, un intero settore o un'intera comunità.

(111) È opportuno stabilire una metodologia per la classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischi sistemici. Poiché i rischi sistemici derivano da capacità particolarmente elevate, si dovrebbe considerare che un modello di IA per finalità generali presenti rischi sistemici se ha capacità di impatto elevato, valutate sulla base di metodologie e strumenti tecnici adeguati, o se ha un impatto significativo sul mercato interno a causa della sua portata. Per capacità di impatto elevato nei modelli di IA per finalità generali si intendono capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati. L'intera gamma di capacità di un modello potrebbe essere meglio compresa dopo la sua immissione sul mercato o quando i deployer interagiscono con il modello. In base allo stato dell'arte al momento dell'entrata in vigore del presente regolamento, l'importo cumulativo del calcolo utilizzato per l'addestramento del modello di IA per finalità generali misurato in operazioni in virgola mobile è una delle approssimazioni pertinenti per le capacità del modello. L'importo cumulativo del calcolo utilizzato per l'addestramento comprende il calcolo utilizzato nelle attività e nei metodi tesi a migliorare le capacità del modello prima della diffusione, quali il pre-addestramento, la generazione di dati sintetici e il perfezionamento. È pertanto opportuno fissare una soglia iniziale di operazioni in virgola mobile che, se raggiunta da un modello di IA per finalità generali, porta a presumere che il modello sia un modello di IA per finalità generali con rischi sistemici. Tale soglia dovrebbe essere adeguata nel tempo per riflettere i cambiamenti tecnologici e industriali, quali miglioramenti algoritmici o una maggiore efficienza dell'hardware, e dovrebbe essere integrata da parametri di riferimento e indicatori per la capacità del modello. A tal fine, l'ufficio per l'IA dovrebbe dialogare con la comunità scientifica, l'industria, la società civile e altri esperti. Le soglie, nonché gli strumenti e i parametri di riferimento per la valutazione delle capacità di impatto elevato, dovrebbero essere solidi indicatori della generalità, delle capacità e del connesso rischio sistemico dei modelli di IA per finalità generali e potrebbero tenere conto delle modalità con cui il modello sarà immesso sul mercato o del numero di utenti che potrebbero esserne interessati. A integrazione di tale sistema, la Commissione dovrebbe avere la possibilità di adottare decisioni individuali per designare un modello di IA per finalità generali come modello di IA per finalità generali con rischio sistemico, qualora si accerti che tale modello abbia capacità o un impatto equivalenti a quelli rilevati dalla soglia fissata. Tale decisione dovrebbe essere adottata in base a una valutazione globale dei criteri per la designazione di un modello di IA per finalità generali con rischio sistemico di cui all'allegato del presente regolamento, come la qualità o le dimensioni del set di dati di addestramento, il numero di utenti commerciali e finali, le sue modalità di input e output, il suo livello di autonomia e scalabilità o gli strumenti a cui ha accesso. Su richiesta motivata di un fornitore il cui modello è stato designato come modello di IA per finalità generali con rischio sistemico, la Commissione dovrebbe tenere conto della richiesta e può decidere di rivalutare se si possa ancora ritenere che il modello di IA per finalità generali presenti rischi sistemici.

(112) È altresì opportuno specificare una procedura per la classificazione di un modello di IA per finalità generali con rischi sistemici. Si dovrebbe presumere che un modello di IA per finalità generali che raggiunge la soglia applicabile per le capacità di impatto elevato sia un modello di IA per finalità generali con rischio sistemico. Il fornitore dovrebbe informare l'ufficio per l'IA al più tardi due settimane dopo che i requisiti sono soddisfatti o quando viene a conoscenza del fatto che un modello di IA per finalità generali soddisferà i requisiti che portano alla suddetta presunzione. Questo assume particolare rilevanza in relazione alla soglia di operazioni in virgola mobile, dato che l'addestramento dei modelli di IA per finalità generali richiede una pianificazione considerevole, comprensiva dell'assegnazione anticipata delle risorse di calcolo, cosicché i fornitori di modelli di IA per finalità generali siano in grado di sapere se il loro modello può raggiungere la soglia prima della conclusione dell'addestramento. Nel contesto di tale notifica, il fornitore dovrebbe essere in grado di dimostrare che, a causa delle sue caratteristiche specifiche, un modello di IA per finalità generali non presenta eccezionalmente rischi sistemici e che, pertanto, non dovrebbe essere classificato come modello di IA per finalità generali con rischi sistemici. Si tratta di informazioni utili all'ufficio per l'IA per anticipare l'immissione sul mercato di modelli di IA per finalità generali con rischi sistemici e i fornitori possono iniziare a dialogare con l'ufficio per l'IA sin dalle prime fasi. Tali informazioni sono

particolarmente importanti per quanto riguarda i modelli di IA per finalità generali che si pianifica di rilasciare come open source, dato che, dopo il rilascio del modello open source, è possibile che sia più difficile attuare le misure necessarie a garantire il rispetto degli obblighi di cui al presente regolamento.

(113) La Commissione dovrebbe avere il potere di designare un modello di IA per finalità generali come modello di IA per finalità generali con rischio sistemico, se viene a conoscenza del fatto che il modello in questione soddisfa i requisiti per tale designazione e in precedenza tale fatto non era noto o il pertinente fornitore aveva omesso di notificarlo alla Commissione. Un sistema di segnalazioni qualificate dovrebbe garantire che l'ufficio per l'IA sia informato dal gruppo scientifico dei modelli di IA per finalità generali che potrebbero dover essere classificati come modelli di IA per finalità generali con rischio sistemico, in aggiunta alle attività di monitoraggio dell'ufficio per l'IA.

(114) I fornitori di modelli di IA per finalità generali che presentano rischi sistemici dovrebbero essere soggetti, oltre agli obblighi previsti per i fornitori di modelli di IA per finalità generali, agli obblighi volti a individuare e attenuare tali rischi e a garantire un livello adeguato di protezione della cibersicurezza, a prescindere dal fatto che il modello sia fornito come modello autonomo o integrato in un sistema di IA o in un prodotto. Per conseguire tali obiettivi, il presente regolamento dovrebbe imporre ai fornitori di effettuare le necessarie valutazioni dei modelli, in particolare prima della sua prima immissione sul mercato, compreso lo svolgimento e la documentazione del test contraddittorio (adversarial testing) dei modelli, anche, se del caso, mediante prove interne o esterne indipendenti. Inoltre, i fornitori di modelli di IA per finalità generali con rischi sistemici dovrebbero valutare e attenuare continuamente i rischi sistemici, ad esempio attuando politiche di gestione dei rischi, quali processi di responsabilità e governance, svolgendo il monitoraggio successivo all'immissione sul mercato, adottando misure adeguate lungo l'intero ciclo di vita del modello e cooperando con gli attori pertinenti lungo la catena del valore dell'IA.

(115) I fornitori di modelli di IA per finalità generali con rischi sistemici dovrebbero valutare e attenuare i possibili rischi sistemici. Se lo sviluppo o l'utilizzo di un modello di IA per finalità generali che potrebbe presentare rischi sistemici causa un incidente grave, nonostante gli sforzi volti a individuare e prevenire i rischi connessi a tale modello, il fornitore del modello di IA per finalità generali dovrebbe, senza indebito ritardo, tenere traccia dell'incidente e riferire alla Commissione e alle autorità nazionali competenti le informazioni pertinenti e le eventuali misure correttive. Inoltre, i fornitori dovrebbero garantire un livello adeguato di protezione della cibersicurezza per il modello e la sua infrastruttura fisica, se del caso, lungo l'intero ciclo di vita del modello. La protezione della cibersicurezza connessa ai rischi sistemici associati a uso doloso o attacchi dovrebbe tenere debitamente in considerazione model leakage accidentali, rilasci non autorizzati, elusioni delle misure di sicurezza, nonché la difesa contro gli attacchi informatici, l'accesso non autorizzato o il furto di modelli. Tale protezione potrebbe essere facilitata mettendo al sicuro pesi, algoritmi, server e set di dati relativi al modello, ad esempio attraverso misure di sicurezza operativa per la sicurezza delle informazioni, politiche specifiche in materia di cibersicurezza, soluzioni tecniche e consolidate appropriate e controlli dell'accesso informatico e fisico, che siano adeguati alle circostanze pertinenti e ai rischi connessi.

(116) L'ufficio per l'IA dovrebbe incoraggiare e agevolare l'elaborazione, il riesame e l'adeguamento dei codici di buone pratiche, tenendo conto degli approcci internazionali. Tutti i fornitori di modelli di IA per finalità generali potrebbero essere invitati a partecipare. Per garantire che i codici di buone pratiche riflettano lo stato dell'arte e tengano debitamente conto di una serie diversificata di prospettive, l'ufficio per l'IA dovrebbe collaborare con le pertinenti autorità nazionali competenti e potrebbe, se del caso, consultare le organizzazioni della società civile e altri portatori di interessi ed esperti pertinenti, compreso il gruppo di esperti scientifici, ai fini dell'elaborazione di tali codici. I codici di buone pratiche dovrebbero disciplinare gli obblighi per i fornitori di modelli di IA per finalità generali e per i fornitori di modelli di IA per finalità generali che presentano rischi sistemici. Inoltre, quanto ai rischi sistemici, i codici di buone pratiche dovrebbero contribuire a stabilire una tassonomia del tipo e della natura dei rischi sistemici a livello dell'Unione, comprese le loro fonti. I codici di buone pratiche dovrebbero inoltre concentrarsi su misure specifiche di valutazione e attenuazione dei rischi.

(117) I codici di buone pratiche dovrebbero rappresentare uno strumento essenziale per i fornitori di modelli di IA per finalità generali ai fini di un'adeguata conformità agli obblighi previsti dal presente regolamento. I fornitori dovrebbero poter fare affidamento su codici di buone pratiche per dimostrare la conformità agli obblighi. Mediante atti di esecuzione, la Commissione può decidere di approvare un codice di buone pratiche e conferire ad esso una validità generale all'interno dell'Unione o, in alternativa, di stabilire norme comuni per l'attuazione dei pertinenti obblighi, qualora un codice di buone pratiche non possa essere portato a termine o ritenuto adeguato da parte dell'ufficio per l'IA entro la data di applicazione del presente regolamento. Quando una norma armonizzata è

pubblicata e ritenuta idonea a disciplinare i pertinenti obblighi da parte dell'ufficio per l'IA, la conformità a una norma armonizzata europea dovrebbe conferire ai fornitori la presunzione di conformità. I fornitori di modelli di IA per finalità generali dovrebbero inoltre essere in grado di dimostrare la conformità utilizzando mezzi adeguati alternativi, se non sono disponibili codici di buone pratiche o norme armonizzate, oppure se tali fornitori scelgono di non fare affidamento su tali codici e norme.

(118) Il presente regolamento disciplina i sistemi di IA e i modelli di IA imponendo determinati requisiti e obblighi agli operatori del mercato pertinenti che li immettono sul mercato, li mettono in servizio o li utilizzano nell'Unione, integrando in tal modo gli obblighi per i prestatori di servizi intermediari che incorporano tali sistemi o modelli nei loro servizi disciplinati dal regolamento (UE) 2022/2065. Nella misura in cui sono integrati in piattaforme online di dimensioni molto grandi designate o motori di ricerca online di dimensioni molto grandi designati, tali sistemi o modelli sono soggetti al quadro di gestione dei rischi di cui al regolamento (UE) 2022/2065. Di conseguenza, si dovrebbe ritenere che gli obblighi corrispondenti del presente regolamento siano adempiuti, salvo se emergono e sono individuati in tali modelli dei rischi sistemici significativi non disciplinati dal regolamento (UE) 2022/2065. In tale quadro, i prestatori di piattaforme online di dimensioni molto grandi e motori di ricerca online di dimensioni molto grandi sono tenuti a valutare i potenziali rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'utilizzo dei rispettivi servizi, comprese le modalità con cui la progettazione dei sistemi algoritmici impiegati nel servizio possono contribuire a tali rischi, nonché i rischi sistemici derivanti da potenziali usi impropri. Tali prestatori sono altresì tenuti ad adottare misure di attenuazione adeguate nel rispetto dei diritti fondamentali.

(119) Considerando la rapidità dell'innovazione e dell'evoluzione tecnologica dei servizi digitali che rientrano nell'ambito di applicazione dei diversi strumenti previsti dal diritto dell'Unione, in particolare tenendo presente l'uso e la percezione dei loro destinatari, i sistemi di IA soggetti al presente regolamento possono essere forniti come servizi intermediari o parti di essi ai sensi del regolamento (UE) 2022/2065, da interpretarsi in modo tecnologicamente neutro. Ad esempio, i sistemi di IA possono essere utilizzati per fornire motori di ricerca online, in particolare nella misura in cui un sistema di IA, come un chatbot online, effettua ricerche, in linea di principio, su tutti i siti web, incorpora i risultati nelle sue conoscenze esistenti e si avvale delle conoscenze aggiornate per generare un unico output che combina diverse fonti di informazione.

(120) Inoltre, gli obblighi imposti dal presente regolamento ai fornitori e ai deployer di taluni sistemi di IA, volti a consentire il rilevamento e la divulgazione del fatto che gli output di tali sistemi siano generati o manipolati artificialmente, sono molto importanti per contribuire all'efficace attuazione del regolamento (UE) 2022/2065. Ciò si applica specialmente agli obblighi per i fornitori di piattaforme online di dimensioni molto grandi o motori di ricerca online di dimensioni molto grandi di individuare e attenuare i rischi sistemici che possono derivare dalla diffusione di contenuti generati o manipolati artificialmente, in particolare il rischio di impatti negativi effettivi o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, anche mediante la disinformazione.

(121) La normazione dovrebbe svolgere un ruolo fondamentale nel fornire soluzioni tecniche ai fornitori per garantire la conformità al presente regolamento, in linea con lo stato dell'arte, e promuovere l'innovazione, la competitività e la crescita nel mercato unico. La conformità alle norme armonizzate quali definite all'articolo 2, punto 1, lettera c), del regolamento (UE) n, 1025/2012 del Parlamento europeo e del Consiglio ([41]), le quali normalmente dovrebbero rispecchiare lo stato dell'arte, dovrebbe essere un modo per i fornitori di dimostrare la conformità ai requisiti del presente regolamento. È pertanto opportuno incoraggiare una rappresentanza equilibrata degli interessi che coinvolga tutti i portatori di interessi pertinenti nell'elaborazione delle norme, in particolare le PMI, le organizzazioni dei consumatori e i portatori di interessi in materia sociale e ambientale conformemente agli articoli 5 e 6 del regolamento (UE) n, 1025/2012. Al fine di agevolare l'adempimento, le richieste di normazione dovrebbero essere presentate dalla Commissione senza indebito ritardo. In sede di elaborazione della richiesta di normazione, la Commissione dovrebbe consultare il forum consultivo e il consiglio per l'IA al fine di ottenere le competenze pertinenti. Tuttavia, in assenza di riferimenti pertinenti a norme armonizzate, la Commissione dovrebbe poter stabilire, mediante atti di esecuzione e previa consultazione del forum consultivo, specifiche comuni per determinati requisiti previsti del presente regolamento. La specifica comune dovrebbe costituire una soluzione eccezionale di ripiego per agevolare l'obbligo del fornitore di conformarsi ai requisiti del presente regolamento, quando la richiesta di normazione non è stata accettata da alcuna delle organizzazioni europee di normazione, quando le pertinenti norme armonizzate non tengono sufficientemente conto delle preoccupazioni in materia di diritti fondamentali, quando le norme armonizzate non sono conformi alla richiesta o quando vi sono ritardi

([41]) 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).

nell'adozione di una norma armonizzata appropriata. Qualora tale ritardo nell'adozione di una norma armonizzata sia dovuto alla complessità tecnica di tale norma, la Commissione dovrebbe tenerne conto prima di prendere in considerazione la definizione di specifiche comuni. Nell'elaborare specifiche comuni, la Commissione è incoraggiata a cooperare con i partner internazionali e gli organismi internazionali di normazione.

(122) È opportuno che, fatto salvo il ricorso a norme armonizzate e specifiche comuni, i fornitori di un sistema di IA ad alto rischio che è stato addestrato e sottoposto a prova con dati che rispecchiano il contesto geografico, comportamentale, contestuale o funzionale specifico all'interno del quale il sistema di IA è destinato a essere usato si presumano conformi alla misura pertinente prevista dal requisito in materia di governance dei dati di cui al presente regolamento. Fatti salvi i requisiti relativi alla robustezza e all'accuratezza di cui al presente regolamento, conformemente all'articolo 54, paragrafo 3, del regolamento (UE) 2019/881, i sistemi di IA ad alto rischio certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersicurezza a norma di tale regolamento e i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione* europea dovrebbero essere considerati conformi al requisito di cibersicurezza di cui al presente regolamento nella misura in cui il certificato di cibersicurezza o la dichiarazione di conformità o parti di essi contemplino il requisito di cibersicurezza di cui al presente regolamento. Ciò lascia impregiudicata la natura volontaria di tale sistema di cibersicurezza.

(123) 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.

(124) 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 basata sul 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, la metodologia o la struttura generale specifiche della valutazione della conformità a norma della pertinente normativa di armonizzazione dell'Unione.

(125) Data la complessità dei sistemi di IA ad alto rischio e i rischi ad essi associati, è importante sviluppare un'adeguata procedura di valutazione della conformità per quanto riguarda i sistemi di IA ad alto rischio che coinvolgono organismi notificati, la cosiddetta valutazione della conformità da parte di terzi. Tuttavia, in considerazione dell'attuale 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 generalmente effettuata dal fornitore sotto la propria responsabilità, con la sola eccezione dei sistemi di IA destinati a essere utilizzati per la biometrica.

(126) Ai fini delle valutazioni della conformità da parte di terzi, laddove richieste, è opportuno che le autorità nazionali competenti notifichino gli organismi notificati a norma del presente regolamento, a condizione che tali organismi soddisfino una serie di requisiti, in particolare in materia di indipendenza, competenza, assenza di conflitti di interesse e requisiti idonei di cibersicurezza. La notifica di tali organismi dovrebbe essere trasmessa dalle autorità nazionali competenti alla Commissione e agli altri Stati membri mediante lo strumento elettronico di notifica elaborato e gestito dalla Commissione a norma dell'allegato I, articolo R23, della decisione n, 768/2008/CE.

(127) In linea con gli impegni assunti dall'Unione nell'ambito dell'accordo dell'Organizzazione mondiale del commercio sugli ostacoli tecnici agli scambi, è opportuno agevolare il riconoscimento reciproco dei risultati della valutazione della conformità prodotti da organismi di valutazione della conformità competenti, indipendentemente dal luogo in cui siano stabiliti, purché tali organismi di valutazione della conformità istituiti a norma del diritto di un paese terzo soddisfino i requisiti applicabili del presente regolamento e l'Unione abbia concluso un accordo in tal senso. In questo contesto, la Commissione dovrebbe esplorare attivamente possibili strumenti internazionali a tale scopo e, in particolare, perseguire la conclusione di accordi di riconoscimento reciproco con i paesi terzi.

(128) In linea con la nozione generalmente riconosciuta di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, è opportuno che ogniqualvolta intervenga una modifica che possa incidere sulla conformità del sistema di IA ad alto rischio al presente regolamento (ad esempio, la modifica del sistema operativo o dell'architettura del software), oppure quando viene modificata la finalità prevista del sistema, tale sistema di IA sia considerato un nuovo sistema di IA che dovrebbe essere sottoposto a una nuova valutazione della conformità. Tuttavia, le modifiche apportate all'algoritmo e alle prestazioni dei sistemi di IA che proseguono il loro «apprendimento» dopo essere stati immessi sul mercato o messi in servizio, in particolare adattando automaticamente le modalità di svolgimento delle funzioni, non dovrebbero costituire una modifica sostanziale, a condizione che tali modifiche siano state predeterminate dal fornitore e valutate al momento della valutazione della conformità.

(129) 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. Per i sistemi di IA ad alto rischio integrati in un prodotto, dovrebbe essere apposta una marcatura CE fisica, integrabile con una marcatura CE digitale. Per i sistemi di IA ad alto rischio forniti solo digitalmente, dovrebbe essere utilizzata una marcatura CE digitale. 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.

(130) La disponibilità in tempi rapidi di tecnologie innovative può, a determinate condizioni, essere fondamentale per la salute e la sicurezza delle persone, per la tutela dell'ambiente e la protezione dai cambiamenti climatici 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, di tutela dell'ambiente nonché di protezione dei principali beni industriali e infrastrutturali, le autorità di vigilanza del mercato 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. In situazioni debitamente giustificate come previsto dal presente regolamento, le autorità di contrasto o le autorità di protezione civile possono mettere in servizio uno specifico sistema di IA ad alto rischio senza l'autorizzazione dell'autorità di vigilanza del mercato, a condizione che tale autorizzazione sia richiesta durante o dopo l'uso senza indebito ritardo.

(131) Al fine di agevolare il lavoro della Commissione e degli Stati membri nel settore dell'IA 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, nonché i fornitori che ritengono che, in base a una deroga, il sistema di IA elencato tra i casi ad alto rischio nell'allegato del presente regolamento non sia ad alto rischio, siano tenuti a registrarsi e a registrare informazioni sul loro sistema di IA in una banca dati dell'UE, che sarà istituita e gestita dalla Commissione. Prima di utilizzare un sistema di IA elencato tra i casi ad alto rischio nell'allegato del presente regolamento, i deployer di sistemi di IA ad alto rischio che sono autorità, agenzie o organismi pubblici dovrebbero registrarsi in tale banca dati e selezionare il sistema che intendono utilizzare. Gli altri deployer dovrebbero essere autorizzati a farlo su base volontaria. Questa sezione della banca dati dell'UE dovrebbe essere accessibile al pubblico gratuitamente e le informazioni dovrebbero essere di facile consultazione, comprensibili e leggibili meccanicamente. La banca dati dell'UE dovrebbe inoltre essere di facile utilizzo, ad esempio tramite la fornitura di funzionalità di ricerca, anche attraverso parole chiave, che consentano al pubblico di reperire informazioni pertinenti da presentare al momento della registrazione dei sistemi di IA ad alto rischio e riguardanti l'uso di sistemi di IA ad alto rischio, elencati in allegato al presente regolamento, a cui corrispondono i sistemi di IA ad alto rischio. Qualsiasi modifica sostanziale dei sistemi di IA ad alto rischio dovrebbe essere registrata anche nella banca dati dell'UE. Per i sistemi di IA ad alto rischio nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, gli obblighi di registrazione dovrebbero essere adempiuti in una sezione non pubblica sicura della banca dati dell'UE. L'accesso alla sezione non pubblica sicura dovrebbe essere strettamente limitato alla Commissione e alle autorità di vigilanza del mercato per quanto riguarda la rispettiva sezione nazionale di tale banca dati. I sistemi di IA ad alto rischio nel settore delle infrastrutture critiche dovrebbero essere registrati solo a livello nazionale. È opportuno che la Commissione sia la titolare del trattamento di tale banca dati dell'UE conformemente al regolamento (UE) 2018/1725. Al fine di garantire la piena funzionalità della banca dati dell'UE, 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. Nello svolgimento dei suoi compiti di titolare del trattamento dei dati nella banca dati dell'UE, la Commissione dovrebbe tenere conto dei rischi legati alla cibersicurezza. Onde massimizzare la disponibilità e l'uso della banca dati dell'UE da parte del pubblico, la banca dati dell'UE, comprese le informazioni ivi messe a disposizione, dovrebbe essere conforme ai requisiti di cui alla direttiva (UE) 2019/882.

(132) 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, e soggetto ad eccezioni mirate per tenere conto delle particolari esigenze delle attività di contrasto. 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 dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. Nell'attuare tale obbligo, le caratteristiche delle persone fisiche appartenenti a gruppi vulnerabili a causa della loro età o disabilità dovrebbero essere prese in considerazione nella misura in cui il sistema di IA sia destinato a interagire anche con tali gruppi. È inoltre opportuno che le persone fisiche ricevano una notifica quando sono esposte a sistemi di IA che, nel trattamento dei loro dati biometrici, possono identificare o inferire le emozioni o intenzioni di tali persone o assegnarle a categorie specifiche. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti personali, l'origine etnica, le preferenze e gli interessi personali. Tali informazioni e notifiche dovrebbero essere fornite in formati accessibili alle persone con disabilità.

(133) Diversi sistemi di IA possono generare grandi quantità di contenuti sintetici, che per gli esseri umani è divenuto sempre più difficile distinguere dai contenuti autentici e generati da esseri umani. L'ampia disponibilità e l'aumento delle capacità di tali sistemi hanno un impatto significativo sull'integrità e sulla fiducia nell'ecosistema dell'informazione, aumentando i nuovi rischi di cattiva informazione e manipolazione su vasta scala, frode, impersonificazione e inganno dei consumatori. Alla luce di tali impatti, della rapida evoluzione tecnologica e della necessità di nuovi metodi e tecniche per risalire all'origine delle informazioni, è opportuno imporre ai fornitori di tali sistemi di integrare soluzioni tecniche che consentano agli output di essere marcati in un formato leggibile meccanicamente e di essere rilevabili come generati o manipolati da un sistema di IA e non da esseri umani. Tali tecniche e metodi dovrebbero essere sufficientemente affidabili, interoperabili, efficaci e solidi nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle tecniche disponibili o di una combinazione di tali tecniche, quali filigrane, identificazioni di metadati, metodi crittografici per dimostrare la provenienza e l'autenticità dei contenuti, metodi di registrazione, impronte digitali o altre tecniche, a seconda dei casi. Nell'attuare tale obbligo, i fornitori dovrebbero tenere conto anche delle specificità e dei limiti dei diversi tipi di contenuti e dei pertinenti sviluppi tecnologici e di mercato nel settore, come rispecchia lo stato dell'arte generalmente riconosciuto. Tali tecniche e metodi possono essere attuati a livello di sistema di IA o a livello di modello di IA, compresi i modelli di IA per finalità generali che generano contenuti, facilitando in tal modo l'adempimento di tale obbligo da parte del fornitore a valle del sistema di IA. Per continuare a essere proporzionato, è opportuno prevedere che tale obbligo di marcatura non debba riguardare i sistemi di IA che svolgono principalmente una funzione di assistenza per l'editing standard o i sistemi di IA che non modificano in modo sostanziale i dati di input forniti dal deployer o la rispettiva semantica.

(134) Oltre alle soluzioni tecniche utilizzate dai fornitori del sistema di IA, i deployer che utilizzano un sistema di IA per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi, entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri a una persona (deep fake), dovrebbero anche rendere noto in modo chiaro e distinto che il contenuto è stato creato o manipolato artificialmente etichettando di conseguenza gli output dell'IA e rivelandone l'origine artificiale. L'adempimento di tale obbligo di trasparenza non dovrebbe essere interpretato nel senso che l'uso del sistema di IA o dei suoi output ostacola il diritto alla libertà di espressione e il diritto alla libertà delle arti e delle scienze garantito dalla Carta, in particolare quando il contenuto fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico, fittizio, o analogo fatte salve le tutele adeguate per i diritti e le libertà dei terzi. In tali casi, l'obbligo di trasparenza per i deep fake di cui al presente regolamento si limita alla rivelazione dell'esistenza di tali contenuti generati o manipolati in modo adeguato che non ostacoli l'esposizione o il godimento dell'opera, compresi il suo normale sfruttamento e utilizzo, mantenendo nel contempo l'utilità e la qualità dell'opera. È inoltre opportuno prevedere un obbligo di divulgazione analogo in relazione al testo generato o manipolato dall'IA nella misura in cui è pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico, a meno che il contenuto generato dall'IA sia stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica abbia la responsabilità editoriale della pubblicazione del contenuto.

(135) Fatta salva la natura obbligatoria e la piena applicabilità degli obblighi di trasparenza, la Commissione può altresì incoraggiare e agevolare l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi in materia di rilevazione ed etichettatura dei contenuti generati o manipolati artificialmente, anche per sostenere modalità pratiche per rendere accessibili, se del caso, i meccanismi di rilevazione e favorire la cooperazione con altri attori lungo la catena del valore, diffondere contenuti o verificarne l'autenticità e la provenienza onde consentire al pubblico di distinguere efficacemente i contenuti generati dall'IA.

(136) Gli obblighi imposti dal presente regolamento ai fornitori e ai deployer di taluni sistemi di IA, volti a consentire il rilevamento e la divulgazione del fatto che gli output di tali sistemi siano generati o manipolati artificialmente, sono molto importanti per contribuire all'efficace attuazione del regolamento (UE) 2022/2065. Ciò si applica specialmente agli obblighi per i fornitori di piattaforme online di dimensioni molto grandi o motori di ricerca online di dimensioni molto grandi di individuare e attenuare i rischi sistemici che possono derivare dalla diffusione di contenuti generati o manipolati artificialmente, in particolare il rischio di impatti negativi effettivi o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, anche mediante la disinformazione. L'obbligo di etichettare i contenuti generati dai sistemi di IA a norma del presente regolamento lascia impregiudicato l'obbligo di cui all'articolo 16, paragrafo 6, del regolamento (UE) 2022/2065 per i prestatori di servizi di memorizzazione di informazioni di trattare le segnalazioni di contenuti illegali ricevute a norma dell'articolo 16, paragrafo 1, di tale regolamento e non dovrebbe influenzare la valutazione e la decisione in merito all'illegalità del contenuto specifico. Tale valutazione dovrebbe essere effettuata solo con riferimento alle norme che disciplinano la legalità dei contenuti.

(137) La conformità agli obblighi di trasparenza per i sistemi di IA disciplinati dal presente regolamento non dovrebbe essere interpretata nel senso che l'uso del sistema di IA o dei suoi output è lecito ai sensi del presente regolamento o di altre disposizioni del diritto dell'Unione e degli Stati membri e dovrebbe lasciare impregiudicati gli altri obblighi di trasparenza per i deployer dei sistemi di IA stabiliti dal diritto dell'Unione o nazionale.

(138) L'IA è una famiglia di tecnologie in rapida evoluzione che richiede sorveglianza regolamentare e uno spazio sicuro e controllato 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 che promuova l'innovazione, sia adeguato alle esigenze future e resiliente alle perturbazioni, gli Stati membri dovrebbero garantire che le rispettive autorità nazionali competenti istituiscano almeno uno spazio di sperimentazione normativa in materia di IA a livello nazionale 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. Gli Stati membri potrebbero inoltre adempiere tale obbligo partecipando a spazi di sperimentazione normativa già esistenti o istituendo congiuntamente uno spazio di sperimentazione con le autorità competenti di uno o più Stati membri, nella misura in cui tale partecipazione fornisca un livello equivalente di copertura nazionale per gli Stati membri partecipanti. Gli spazi di sperimentazione normativa per l'IA potrebbero essere istituiti in forma fisica, digitale o ibrida e potrebbero accogliere prodotti sia fisici che digitali. Le autorità costituenti dovrebbero altresì garantire che gli spazi di sperimentazione normativa per l'IA dispongano delle risorse adeguate per il loro funzionamento, comprese risorse finanziarie e umane.

(139) Gli obiettivi degli spazi di sperimentazione normativa per l'IA 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 pertinenti disposizioni di diritto dell'Unione e nazionale. Inoltre, gli spazi di sperimentazione normativa per l'IA dovrebbero avere come obiettivo 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, l'agevolazione dell'apprendimento normativo per le autorità e le imprese, anche in vista del futuro adeguamento del quadro giuridico, il sostegno alla cooperazione e la condivisione delle migliori pratiche con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA, nonché l'accelerazione dell'accesso ai mercati, anche mediante l'eliminazione degli ostacoli per le PMI, comprese le start-up. Gli spazi di sperimentazione normativa per l'IA dovrebbero essere ampiamente disponibili in tutta l'Unione e si dovrebbe prestare particolare attenzione alla loro accessibilità per le PMI, comprese le start-up. La partecipazione allo spazio di sperimentazione normativa per l'IA dovrebbe concentrarsi su questioni che creano incertezza giuridica rendendo difficoltoso per i fornitori e i potenziali fornitori innovare, sperimentare l'IA nell'Unione e contribuire all'apprendimento normativo basato su dati concreti. La supervisione dei sistemi di IA nello spazio di sperimentazione normativa per l'IA dovrebbe pertanto riguardare il relativo sviluppo, addestramento, prova e convalida prima che i sistemi siano immessi sul mercato o messi in servizio, nonché la nozione e il verificarsi di modifiche sostanziali che possono richiedere una nuova procedura di valutazione della conformità. Qualsiasi rischio significativo individuato durante lo sviluppo e le prove di tali sistemi di IA dovrebbe comportare l'adozione di adeguate misure di attenuazione e, in mancanza di ciò, la sospensione del processo di sviluppo e di prova. Se del caso, le autorità nazionali competenti che istituiscono spazi di sperimentazione normativa per l'IA dovrebbero cooperare con altre autorità pertinenti, comprese quelle che vigilano sulla protezione dei diritti fondamentali, e potrebbero consentire il coinvolgimento di altri attori all'interno dell'ecosistema dell'IA, quali organizzazioni di normazione nazionali o europee, organismi notificati, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione, poli europei dell'innovazione digitale e pertinenti portatori di interessi e organizzazioni della società civile. Al fine di garantire un'attuazione uniforme in tutta l'Unione e le economie di scala, è opportuno stabilire regole comuni per l'attuazione degli spazi di sperimentazione normativa per l'IA e un quadro per la cooperazione tra le autorità competenti coinvolte nel controllo degli spazi di sperimentazione. Gli spazi di sperimentazione normativa per l'IA istituiti a norma del presente regolamento non dovrebbero pregiudicare altre disposizioni che consentono la creazione di altri spazi di sperimentazione volti a garantire la conformità a disposizioni del diritto diverse dal presente regolamento. Se del caso, le pertinenti autorità competenti responsabili di tali altri spazi di sperimentazione normativa dovrebbero considerare i vantaggi derivanti dall'utilizzo di tali spazi di sperimentazione anche al fine di garantire la conformità dei sistemi di IA al presente regolamento. Previo accordo tra le autorità nazionali competenti e i partecipanti allo spazio di sperimentazione normativa per l'IA, anche le prove in condizioni reali possono essere gestite e supervisionate nel quadro dello spazio di sperimentazione normativa per l'IA.

(140) Il presente regolamento dovrebbe fornire la base giuridica ai fornitori e ai potenziali fornitori nello spazio di sperimentazione normativa per l'IA per utilizzare i 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, solo a specifiche condizioni, conformemente all'articolo 6, paragrafo 4, e all'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679, e agli articoli 5, 6 e 10 del regolamento (UE) 2018/1725, e fatti salvi l'articolo 4, paragrafo 2, e l'articolo 10 della direttiva (UE) 2016/680. Tutti gli altri obblighi dei titolari del trattamento e i diritti degli interessati ai sensi del regolamento (UE) 2016/679, del regolamento (UE) 2018/1725 e della direttiva (UE) 2016/680 restano applicabili. In particolare, il presente regolamento non dovrebbe costituire una base giuridica ai sensi dell'articolo 22, paragrafo 2, lettera b), del regolamento (UE) 2016/679 e dell'articolo 24, paragrafo 2, lettera b), del regolamento (UE) 2018/1725. I fornitori e i potenziali fornitori nello spazio di sperimentazione normativa per l'IA dovrebbero fornire garanzie adeguate e cooperare con le autorità competenti, anche seguendo

i loro orientamenti e agendo rapidamente e in buona fede per attenuare adeguatamente eventuali rischi significativi individuati per la sicurezza, la salute e i diritti fondamentali che possono emergere durante lo sviluppo, le prove e la sperimentazione in tale spazio.

(141) Al fine di accelerare il processo di sviluppo e immissione sul mercato dei sistemi di IA ad alto rischio elencati in un allegato del presente regolamento, è importante che anche i fornitori o i potenziali fornitori di tali sistemi possano beneficiare di un regime specifico per sottoporre a prova tali sistemi in condizioni reali, senza partecipare a uno spazio di sperimentazione normativa per l'IA. Tuttavia, in tali casi, e tenendo conto delle possibili conseguenze di tali prove sulle persone, è opportuno garantire che il presente regolamento introduca garanzie e condizioni adeguate e sufficienti per i fornitori o potenziali fornitori. Tali garanzie dovrebbero includere, tra l'altro, la richiesta del consenso informato delle persone fisiche a partecipare a prove in condizioni reali, ad eccezione delle autorità di contrasto quando la richiesta di consenso informato impedirebbe di sottoporre a prova il sistema di IA. Il consenso dei soggetti a partecipare a tali prove a norma del presente regolamento è distinto e non pregiudica il consenso degli interessati al trattamento dei loro dati personali ai sensi della pertinente normativa in materia di protezione dei dati. È inoltre importante ridurre al minimo i rischi e consentire la sorveglianza da parte delle autorità competenti e richiedere pertanto ai potenziali fornitori di disporre di un piano di prova in condizioni reali presentato all'autorità di vigilanza del mercato competente, di registrare le prove in sezioni dedicate della banca dati dell'UE, fatte salve alcune limitate eccezioni, di fissare limiti al periodo nel quale possono essere effettuate le prove e di richiedere tutele aggiuntive per le persone appartenenti a certi gruppi vulnerabili, nonché un accordo scritto che definisca i ruoli e le responsabilità dei potenziali fornitori e dei deployer e una sorveglianza efficace da parte del personale competente coinvolto nelle prove in condizioni reali. È inoltre opportuno prevedere tutele aggiuntive per garantire che le previsioni, le raccomandazioni o le decisioni del sistema di IA possano essere efficacemente ribaltate e ignorate e che i dati personali siano protetti e cancellati quando i soggetti hanno revocato il loro consenso a partecipare alle prove, fatti salvi i loro diritti in qualità di interessati ai sensi della normativa dell'Unione in materia di protezione dei dati. Per quanto riguarda il trasferimento dei dati, è inoltre opportuno prevedere che i dati raccolti e trattati ai fini delle prove in condizioni reali siano trasferiti a paesi terzi solo se sono attuate tutele adeguate e applicabili ai sensi del diritto dell'Unione, in particolare conformemente alle basi per il trasferimento di dati personali ai sensi del diritto dell'Unione in materia di protezione dei dati, mentre per i dati non personali sono poste in essere tutele adeguate conformemente al diritto dell'Unione, quali il regolamento (UE) 2022/868 ([42]) e il regolamento (UE) 2023/2854 ([43]) del Parlamento europeo e del Consiglio.

(142) Per garantire che l'IA porti a risultati vantaggiosi sul piano sociale e ambientale, gli Stati membri sono incoraggiati a sostenere e promuovere la ricerca e lo sviluppo di soluzioni di IA a sostegno di risultati vantaggiosi dal punto di vista sociale e ambientale, come le soluzioni basate sull'IA per aumentare l'accessibilità per le persone con disabilità, affrontare le disuguaglianze socioeconomiche o conseguire obiettivi in materia di ambiente, assegnando risorse sufficienti, compresi i finanziamenti pubblici e dell'Unione, e, se del caso e a condizione che siano soddisfatti i criteri di ammissibilità e selezione, prendendo in considerazione soprattutto i progetti che perseguono tali obiettivi. Tali progetti dovrebbero basarsi sul principio della cooperazione interdisciplinare tra sviluppatori dell'IA, esperti in materia di disuguaglianza e non discriminazione, accessibilità e diritti ambientali, digitali e dei consumatori, nonché personalità accademiche.

(143) Al fine di promuovere e proteggere l'innovazione, è importante che siano tenuti in particolare considerazione gli interessi delle PMI, comprese le start-up, che sono fornitrici o deployer 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. Gli Stati membri dovrebbero fornire alle PMI, comprese le start-up, con sede legale o una filiale nell'Unione, un accesso prioritario agli spazi di sperimentazione normativa per l'IA, purché soddisfino le condizioni di ammissibilità e i criteri di selezione e senza precludere ad altri fornitori e potenziali fornitori l'accesso agli spazi di sperimentazione, a condizione che siano soddisfatti gli stessi criteri e le stesse condizioni. Gli Stati membri dovrebbero utilizzare i canali esistenti e, ove opportuno, istituiscono nuovi canali dedicati per la comunicazione con le PMI, comprese le start-up, i deployer, altri innovatori e, se del caso, le autorità pubbliche locali, al fine di sostenere le PMI nel loro percorso di sviluppo fornendo orientamenti e rispondendo alle domande sull'attuazione del presente regolamento. Se del caso, tali canali dovrebbero collaborare per creare sinergie e garantire l'omogeneità dei loro orientamenti per le PMI, comprese le start-up, e i deployer. Inoltre, gli Stati membri dovrebbero agevolare la partecipazione delle PMI e di altri portatori di interessi pertinenti ai processi di sviluppo della normazione. Gli organismi notificati, nel fissare le tariffe per la valutazione della conformità, dovrebbero tenere in considerazione gli

([42]) Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati) (GU L 152 del 3.6.2022, pag. 1).

([43]) Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati) (GU L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

interessi e le esigenze specifici dei fornitori che sono PMI, comprese le start-up. La Commissione dovrebbe valutare periodicamente i costi di certificazione e di conformità per le PMI, comprese le start-up, attraverso consultazioni trasparenti e dovrebbe collaborare con gli Stati membri per ridurre tali costi. Ad esempio, 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 deployer transfrontalieri. Al fine di rispondere alle esigenze specifiche delle PMI, comprese le start-up, la Commissione dovrebbe fornire modelli standardizzati per i settori disciplinati dal presente regolamento, su richiesta del consiglio per l'IA. Inoltre, la Commissione dovrebbe integrare gli sforzi degli Stati membri fornendo a tutti i fornitori e i deployer una piattaforma unica di informazioni di facile utilizzo in relazione al presente regolamento, organizzando adeguate campagne di comunicazione per sensibilizzare in merito agli obblighi derivanti dal presente regolamento e valutando e promuovendo la convergenza delle migliori pratiche nelle procedure di appalto pubblico in relazione ai sistemi di IA. Le imprese che di recente sono passate dalla categoria delle piccole imprese a quella delle medie imprese ai sensi dell'allegato della raccomandazione 2003/361/CE ([44]) della Commissione dovrebbero avere accesso a tali misure di sostegno, in quanto queste nuove imprese di medie dimensioni possono talvolta non disporre delle risorse giuridiche e della formazione necessarie per garantire una corretta comprensione del presente regolamento e la conformità ad esso.

(144) Al fine di promuovere e proteggere l'innovazione, la piattaforma di IA on demand e tutti i pertinenti programmi e progetti di finanziamento dell'Unione, quali il programma Europa digitale e Orizzonte Europa, attuati dalla Commissione e dagli Stati membri a livello dell'Unione o nazionale, a seconda dei casi, dovrebbero contribuire al conseguimento degli obiettivi del presente regolamento.

(145) 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, in particolare le PMI, comprese le start-up, 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 gli impianti di prova e sperimentazione istituiti dalla Commissione e dagli Stati membri a livello dell'Unione o nazionale contribuiscano all'attuazione del presente regolamento. Nell'ambito delle rispettive missioni e dei rispettivi settori di competenza, la piattaforma di IA on demand, i poli europei dell'innovazione digitale e gli impianti di prova e sperimentazione sono in grado di fornire, in particolare, sostegno tecnico e scientifico ai fornitori e agli organismi notificati.

(146) Inoltre, alla luce delle dimensioni molto ridotte di alcuni operatori e al fine di garantire la proporzionalità rispetto ai costi dell'innovazione, è opportuno consentire alle microimprese di adempiere a uno degli obblighi più dispendiosi, vale a dire l'istituzione di un sistema di gestione della qualità, in un modo semplificato che ridurrebbe gli oneri amministrativi e i costi a carico di tali imprese senza incidere sul livello di protezione e sulla necessità di rispettare i requisiti per i sistemi di IA ad alto rischio. La Commissione dovrebbe elaborare orientamenti per specificare gli elementi del sistema di gestione della qualità che le microimprese devono soddisfare in tale modo semplificato.

(147) È opportuno che la Commissione agevoli, nella misura del possibile, l'accesso agli impianti di prova e sperimentazione di organismi, gruppi o laboratori istituiti o accreditati a norma di qualsiasi pertinente normativa di armonizzazione dell'Unione che assolvono compiti nel contesto della valutazione della conformità di prodotti o dispositivi contemplati da tale normativa di armonizzazione dell'Unione. Ciò vale in particolare per quanto riguarda i gruppi di esperti, i laboratori specializzati e i laboratori di riferimento nel settore dei dispositivi medici a norma dei regolamenti (UE) 2017/745 e (UE) 2017/746.

(148) Il presente regolamento dovrebbe istituire un quadro di governance che consenta di coordinare e sostenere l'applicazione dello stesso a livello nazionale, nonché di sviluppare capacità a livello dell'Unione e integrare i portatori di interessi nel settore dell'IA. L'attuazione e l'esecuzione efficaci del presente regolamento richiedono un quadro di governance che consenta di coordinare e sviluppare competenze centrali a livello dell'Unione. L'ufficio per l'IA è stato istituito con decisione della Commissione ([45]) e ha la missione di sviluppare competenze e capacità dell'Unione nel settore dell'IA e di contribuire all'attuazione del diritto dell'Unione in materia di IA. Gli Stati membri dovrebbero facilitare i compiti dell'ufficio per l'IA al fine di sostenere lo sviluppo di competenze e capacità dell'Unione a livello dell'Unione e di rafforzare il funzionamento del mercato unico digitale. È inoltre opportuno istituire un consiglio per l'IA composto da rappresentanti degli Stati membri, un gruppo di esperti scientifici volto a integrare la comunità scientifica e un forum consultivo per raccogliere il contributo dei portatori di interessi all'attuazione del presente regolamento, a livello dell'Unione e nazionale. Lo sviluppo delle competenze e delle

([44]) 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).

([45]) Decisione della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale C (2024) 390.

capacità dell'Unione dovrebbe includere anche l'utilizzo delle risorse e delle competenze esistenti, in particolare grazie a sinergie con le strutture create nel contesto dell'esecuzione a livello dell'Unione di altre disposizioni e a sinergie con le iniziative correlate a livello dell'Unione, quali l'impresa comune EuroHPC e gli impianti di prova e sperimentazione dell'IA nell'ambito del programma Europa digitale.

(149) Al fine di facilitare un'attuazione agevole, efficace e armonizzata del presente regolamento, è opportuno istituire un consiglio per l'IA. Il consiglio per l'IA dovrebbe riflettere i vari interessi dell'ecosistema dell'IA ed essere composto da rappresentanti degli Stati membri. Il consiglio per l'IA dovrebbe essere responsabile di una serie di compiti consultivi, tra cui l'emanazione di pareri, raccomandazioni, consulenze o il contributo all'emanazione di orientamenti su questioni relative all'attuazione del presente regolamento, comprese le questioni relative all'esecuzione, le specifiche tecniche o le norme esistenti per quanto riguarda i requisiti stabiliti nel presente regolamento, e la fornitura di consulenza alla Commissione, agli Stati membri e alle rispettive autorità nazionali competenti su questioni specifiche connesse all'IA. Al fine di offrire una certa flessibilità agli Stati membri nella designazione dei loro rappresentanti all'interno del consiglio per l'IA, tali rappresentanti possono essere persone appartenenti a entità pubbliche dotate delle competenze e dei poteri pertinenti per facilitare il coordinamento a livello nazionale e contribuire all'adempimento dei compiti del consiglio per l'IA. Il consiglio per l'IA dovrebbe istituire due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e le autorità di notifica su questioni relative, rispettivamente, alla vigilanza del mercato e agli organismi notificati. Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per il presente regolamento ai sensi dell'articolo 30 del regolamento (UE) 2019/1020. In conformità dell'articolo 33 di tale regolamento, la Commissione dovrebbe sostenere le attività del sottogruppo permanente per la vigilanza del mercato effettuando valutazioni o studi di mercato, in particolare al fine di individuare gli aspetti del presente regolamento che richiedono un coordinamento specifico e urgente tra le autorità di vigilanza del mercato. Il consiglio per l'IA può istituire altri sottogruppi permanenti o temporanei, se del caso, ai fini dell'esame di questioni specifiche. Il consiglio per l'IA dovrebbe inoltre cooperare, se del caso, con i pertinenti organismi, gruppi di esperti e reti dell'Unione attivi nel contesto del pertinente diritto dell'Unione, compresi in particolare quelli attivi a norma del pertinente diritto dell'Unione sui dati, i prodotti e i servizi digitali.

(150) Al fine di garantire il coinvolgimento dei portatori di interessi nell'attuazione e nell'applicazione del presente regolamento, è opportuno istituire un forum consultivo per fornire consulenza e competenze tecniche al consiglio per l'IA e alla Commissione. Al fine di garantire una rappresentanza diversificata ed equilibrata dei portatori di interessi che tenga conto di interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, con riferimento alle PMI e alle altre imprese, il forum consultivo dovrebbe comprendere, tra l'altro, l'industria, le start-up, le PMI, il mondo accademico, la società civile, comprese le parti sociali, nonché l'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo delle norme di telecomunicazione (ETSI).

(151) Al fine di sostenere l'attuazione e l'esecuzione del presente regolamento, in particolare le attività di monitoraggio dell'ufficio per l'IA per quanto riguarda i modelli di IA per finalità generali, è opportuno istituire un gruppo di esperti scientifici indipendenti. Gli esperti indipendenti che costituiscono il gruppo dovrebbero essere selezionati sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'IA e dovrebbero svolgere i loro compiti con imparzialità e obiettività e garantire la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività. Per consentire il potenziamento delle capacità nazionali necessarie per l'efficace esecuzione del presente regolamento, gli Stati membri dovrebbero essere in grado di chiedere il sostegno della riserva di esperti che costituisce il gruppo di esperti scientifici per le loro attività di esecuzione.

(152) Al fine di sostenere un'esecuzione adeguata per quanto riguarda i sistemi di IA e rafforzare le capacità degli Stati membri, è opportuno istituire e mettere a disposizione degli Stati membri strutture di sostegno dell'Unione per la prova dell'IA.

(153) Gli Stati membri svolgono un ruolo chiave nell'applicare ed eseguire il presente regolamento. A tale riguardo, è opportuno che ciascuno Stato membro designi almeno una autorità di notifica e almeno una autorità di vigilanza del mercato come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del presente regolamento. Gli Stati membri possono decidere di nominare qualsiasi tipo di entità pubblica per svolgere i compiti delle autorità nazionali competenti ai sensi del presente regolamento, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali. Al fine di incrementare l'efficienza organizzativa da parte degli Stati membri e di istituire un punto di contatto unico nei confronti del pubblico e di altre controparti sia a livello di Stati membri sia a livello di Unione, è opportuno che ciascuno Stato membro designi un'autorità di vigilanza del mercato come punto di contatto unico.

(154) Le autorità nazionali competenti dovrebbero esercitare i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità dovrebbero astenersi da qualsiasi atto incompatibile con le loro funzioni e dovrebbero essere soggetti alle norme in materia di riservatezza ai sensi del presente regolamento.

(155) 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. Se del caso, il monitoraggio successivo all'immissione sul mercato dovrebbe includere un'analisi dell'interazione con altri sistemi di IA, compresi altri dispositivi e software. Il monitoraggio successivo all'immissione sul mercato non dovrebbe riguardare i dati operativi sensibili dei deployer che sono autorità di contrasto. 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 derivanti dall'uso dei loro sistemi di IA, vale a dire incidenti o malfunzionamenti che comportano il decesso o gravi danni alla salute, perturbazioni gravi e irreversibili della gestione o del funzionamento delle infrastrutture critiche, violazioni degli obblighi ai sensi del diritto dell'Unione intesi a proteggere i diritti fondamentali o gravi danni alle cose o all'ambiente.

(156) Al fine di garantire un'esecuzione 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. Le autorità di vigilanza del mercato designate a norma del presente regolamento dovrebbero disporre di tutti i poteri di esecuzione di cui al presente regolamento e al regolamento (UE) 2019/1020 e dovrebbero esercitare i loro poteri e svolgere le loro funzioni in modo indipendente, imparziale e senza pregiudizi. Sebbene la maggior parte dei sistemi di IA non sia soggetta a requisiti e obblighi specifici a norma del presente regolamento, le autorità di vigilanza del mercato possono adottare misure in relazione a tutti i sistemi di IA che presentino un rischio conformemente al presente regolamento. Data la natura specifica delle istituzioni, degli organi e degli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento, è opportuno designare il Garante europeo della protezione dei dati quale autorità di vigilanza del mercato per essi competente. Ciò non dovrebbe pregiudicare la designazione di autorità nazionali competenti da parte degli Stati membri. Le attività di vigilanza del mercato non dovrebbero pregiudicare la capacità delle entità sottoposte a vigilanza di svolgere i loro compiti in modo indipendente, qualora tale indipendenza sia richiesta dal diritto dell'Unione.

(157) Il presente regolamento non pregiudica le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione del diritto dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati. Ove necessario per il loro mandato, è opportuno che tali autorità od organismi pubblici nazionali abbiano altresì accesso alla documentazione creata a norma del presente regolamento. È opportuno istituire una procedura di salvaguardia specifica per garantire un'esecuzione adeguata e tempestiva rispetto ai sistemi di IA che presentano un rischio per la salute, la sicurezza e i diritti fondamentali. La procedura per siffatti sistemi di IA che presentano un rischio dovrebbe essere applicata ai sistemi di IA ad alto rischio che presentano un rischio, ai sistemi vietati che sono stati immessi sul mercato, messi in servizio o utilizzati in violazione dei divieti riguardanti le pratiche di cui al presente regolamento e ai sistemi di IA che sono stati messi a disposizione in violazione dei requisiti di trasparenza di cui al presente regolamento e che presentano un rischio.

(158) Il diritto 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'esecuzione degli obblighi previsti dal presente regolamento e delle regole e dei requisiti pertinenti degli atti giuridici dell'Unione in materia di servizi finanziari, è opportuno che le autorità competenti del controllo e dell'esecuzione di tali atti giuridici, in particolare le autorità competenti quali definite al regolamento (UE) n, 575/2013 del Parlamento europeo e del Consiglio ([46]) e alle direttive 2008/48/CE ([47]), 2009/138/CE ([48]), 2013/36/UE ([49]), 2014/17/UE ([50])

([46]) Regolamento (UE) n, 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n, 648/2012 (GU L 176 del 27.6.2013, pag. 1).

([47]) 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE (GU L 133 del 22.5.2008, pag. 66).

([48]) Direttiva 2009/138/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

([49]) 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).

([50]) Direttiva 2014/17/UE del Parlamento europeo e del Consiglio, del 4 febbraio 2014, in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali e recante modifica delle direttive 2008/48/CE e 2013/36/UE e del regolamento (UE) n, 1093/2010 (GU L 60 del 28.2.2014, pag. 34).

e (UE) 2016/97 ([51]) del Parlamento europeo e del Consiglio, siano designate, nell'ambito delle rispettive competenze, quali 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, a meno che gli Stati membri non decidano di designare un'altra autorità per svolgere tali compiti di vigilanza del mercato. Tali autorità competenti dovrebbero disporre di tutti i poteri a norma del presente regolamento e del regolamento (UE) 2019/1020 per far rispettare i requisiti e gli obblighi del presente regolamento, compresi i poteri per svolgere attività di vigilanza del mercato *ex post* che possono essere integrate, se del caso, nei rispettivi meccanismi e nelle rispettive procedure di vigilanza esistenti a norma del pertinente diritto dell'Unione in materia di servizi finanziari. È opportuno prevedere che, quando agiscono in qualità di autorità di vigilanza del mercato a norma del presente regolamento, le autorità nazionali responsabili della vigilanza degli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento (UE) n, 1024/2013 del Consiglio ([52]), comunichino senza ritardo alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento. Per migliorare ulteriormente la coerenza tra il presente regolamento e le regole applicabili agli enti creditizi disciplinati dalla direttiva 2013/36/UE, è altresì opportuno integrare negli obblighi e nelle procedure esistenti a norma di tale direttiva alcuni degli obblighi procedurali dei fornitori in materia di gestione dei rischi, monitoraggio successivo all'immissione sul mercato 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 ai deployer dei sistemi di IA ad alto rischio nella misura in cui si applicano agli enti creditizi disciplinati dalla direttiva 2013/36/UE. Lo stesso regime dovrebbe applicarsi alle imprese di assicurazione e di riassicurazione e alle società di partecipazione assicurativa ai sensi della direttiva 2009/138/CE nonché agli intermediari assicurativi ai sensi della direttiva (UE) 2016/97 e ad altri tipi di istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del pertinente diritto dell'Unione in materia di servizi finanziari per garantire coerenza e parità di trattamento nel settore finanziario.

(159) Ciascuna autorità di vigilanza del mercato per i sistemi di IA ad alto rischio nel settore della biometria elencati in un allegato del presente regolamento nella misura in cui tali sistemi siano utilizzati a fini di contrasto, migrazione, asilo e gestione del controllo delle frontiere, o per l'amministrazione della giustizia e dei processi democratici, dovrebbe disporre di poteri di indagine e correttivi efficaci, tra cui almeno il potere di ottenere l'accesso a tutti i dati personali trattati e a tutte le informazioni necessarie per lo svolgimento dei suoi compiti. Le autorità di vigilanza del mercato dovrebbero poter esercitare i loro poteri agendo in piena indipendenza. Qualsiasi limitazione del loro accesso ai dati operativi sensibili a norma del presente regolamento dovrebbe lasciare impregiudicati i poteri loro conferiti dalla direttiva (UE) 2016/680. Nessuna esclusione relativa alla divulgazione dei dati alle autorità nazionali per la protezione dei dati a norma del presente regolamento dovrebbe incidere sui poteri attuali o futuri di tali autorità al di là dell'ambito di applicazione del presente regolamento.

(160) Le autorità di vigilanza del mercato e la Commissione dovrebbero poter proporre attività congiunte, comprese indagini congiunte, che dovrebbero essere condotte dalle autorità di vigilanza del mercato o dalle autorità di vigilanza del mercato di concerto con la Commissione, al fine di promuovere la conformità, individuare casi di non conformità, sensibilizzare e fornire orientamenti in relazione al presente regolamento riguardo a specifiche categorie di sistemi di IA ad alto rischio che si rileva presentino un rischio grave in due o più Stati membri. Le attività congiunte volte a promuovere la conformità dovrebbero essere svolte conformemente all'articolo 9 del regolamento (UE) 2019/1020. L'ufficio per l'IA dovrebbe fornire sostegno di coordinamento per le indagini congiunte.

(161) È necessario chiarire le responsabilità e le competenze a livello dell'Unione e nazionale per quanto riguarda i sistemi di IA basati su modelli di IA per finalità generali. Per evitare sovrapposizioni di competenze, qualora un sistema di IA si basi su un modello di IA per finalità generali e il modello e il sistema siano forniti dallo stesso fornitore, la

([51]) Direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio, del 20 gennaio 2016, sulla distribuzione assicurativa (GU L 26 del 2.2.2016, pag. 19).

([52]) Regolamento (UE) n, 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi (GU L 287 del 29.10.2013, pag. 63).

supervisione dovrebbe avere luogo a livello dell'Unione attraverso l'ufficio per l'IA, che dovrebbe disporre a tal fine dei poteri di un'autorità di vigilanza del mercato ai sensi del regolamento (UE) 2019/1020. In tutti gli altri casi, le autorità nazionali di vigilanza del mercato restano responsabili della supervisione dei sistemi di IA. Tuttavia, per i sistemi di IA per finalità generali che possono essere utilizzati direttamente dai deployer per almeno una finalità classificata come ad alto rischio, le autorità di vigilanza del mercato dovrebbero cooperare con l'ufficio per l'IA per effettuare valutazioni della conformità e informare di conseguenza il consiglio per l'IA e le altre autorità di vigilanza del mercato. Inoltre, qualsiasi autorità di vigilanza del mercato dovrebbero poter chiedere assistenza all'ufficio per l'IA qualora non sia in grado di concludere un'indagine su un sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali su cui è costruito il sistema di IA ad alto rischio. In tali casi, dovrebbe applicarsi mutatis mutandis la procedura relativa all'assistenza reciproca nei casi transfrontalieri di cui al capo VI del regolamento (UE) 2019/1020.

(162) Per sfruttare al meglio le competenze centralizzate dell'Unione e le sinergie a livello dell'Unione, i poteri di controllo ed esecuzione degli obblighi dei fornitori di modelli di IA per finalità generali dovrebbero essere di competenza della Commissione. L'ufficio per l'IA dovrebbe essere in grado di svolgere tutte le attività necessarie per monitorare l'efficace attuazione del presente regolamento per quanto riguarda i modelli di IA per finalità generali. Dovrebbe essere in grado di svolgere indagini su eventuali violazioni delle norme applicabili ai fornitori di modelli di IA per finalità generali sia di propria iniziativa, a seguito dei risultati delle sue attività di monitoraggio, sia su richiesta delle autorità di vigilanza del mercato in linea con le condizioni stabilite nel presente regolamento. Per sostenere un monitoraggio efficace dell'ufficio per l'IA, esso dovrebbe prevedere la possibilità che i fornitori a valle presentino reclami in merito a possibili violazioni delle norme applicabili ai fornitori di modelli e sistemi di IA per finalità generali.

(163) Al fine di integrare i sistemi di governance per i modelli di IA per finalità generali, il gruppo di esperti scientifici dovrebbe sostenere le attività di monitoraggio dell'ufficio per l'IA e può, in alcuni casi, fornire segnalazioni qualificate all'ufficio per l'IA che avviano attività di follow-up quali indagini. Ciò dovrebbe valere quando il gruppo di esperti scientifici ha motivo di sospettare che un modello di IA per finalità generali rappresenti un rischio concreto e identificabile a livello dell'Unione. Inoltre, ciò dovrebbe verificarsi nel caso in cui il gruppo di esperti scientifici abbia motivo di sospettare che un modello di IA per finalità generali soddisfa i criteri che comporterebbero una classificazione come modello di IA per finalità generali con rischio sistemico. Per dotare il gruppo di esperti scientifici delle informazioni necessarie per lo svolgimento di tali compiti, è opportuno prevedere un meccanismo in base al quale il gruppo di esperti scientifici può chiedere alla Commissione di esigere da un fornitore documentazione o informazioni.

(164) L'ufficio per l'IA dovrebbe essere in grado di adottare le misure necessarie per monitorare l'efficace attuazione e il rispetto degli obblighi dei fornitori di modelli di IA per finalità generali di cui al presente regolamento. L'ufficio per l'IA dovrebbe essere in grado di svolgere indagini su possibili violazioni conformemente ai poteri previsti dal presente regolamento, anche richiedendo documentazione e informazioni, effettuando valutazioni ed esigendo l'adozione di misure da parte dei fornitori di modelli di IA per finalità generali. Nell'effettuare le valutazioni, al fine di avvalersi di competenze indipendenti, l'ufficio per l'IA dovrebbe potersi rivolgere a esperti indipendenti che svolgano le valutazioni per suo conto. Il rispetto degli obblighi dovrebbe essere reso esecutivo, tra l'altro, mediante richieste di adottare misure adeguate, comprese misure di attenuazione dei rischi nel caso di rischi sistemici individuati, nonché limitando la messa a disposizione sul mercato, ritirando o richiamando il modello. A titolo di salvaguardia, ove ciò sia necessario al di là dei diritti procedurali di cui al presente regolamento, i fornitori di modelli di IA per finalità generali dovrebbero godere dei diritti procedurali di cui all'articolo 18 del regolamento (UE) 2019/1020, che dovrebbero applicarsi mutatis mutandis, fatti salvi i diritti procedurali più specifici previsti dal presente regolamento.

(165) Lo sviluppo di sistemi di IA diversi dai sistemi di IA ad alto rischio in conformità dei requisiti del presente regolamento può portare a una più ampia adozione nell'Unione di un'IA etica e affidabile. I fornitori di sistemi di IA non ad alto rischio dovrebbero essere incoraggiati a creare codici di condotta, che includano meccanismi di governance connessi, volti a promuovere l'applicazione volontaria di alcuni o tutti i requisiti obbligatori applicabili ai sistemi di IA ad alto rischio, adattati in funzione della finalità prevista dei sistemi e del minor rischio connesso e tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore, come modelli e schede dati. I fornitori e, se del caso, i deployer di tutti i sistemi di IA, ad alto rischio o meno, e modelli di IA dovrebbero inoltre essere incoraggiati ad applicare su base volontaria requisiti supplementari relativi, ad esempio, agli elementi degli orientamenti etici dell'Unione per un'IA affidabile, alla sostenibilità ambientale, alle misure di alfabetizzazione in

materia di IA, alla progettazione e allo sviluppo inclusivi e diversificati dei sistemi di IA, anche prestando attenzione alle persone vulnerabili e all'accessibilità per le persone con disabilità, la partecipazione dei portatori di interessi, con il coinvolgimento, se del caso, dei portatori di interessi pertinenti quali le organizzazioni imprenditoriali e della società civile, il mondo accademico, le organizzazioni di ricerca, i sindacati e le organizzazioni per la tutela dei consumatori nella progettazione e nello sviluppo dei sistemi di IA, e alla diversità dei gruppi di sviluppo, compreso l'equilibrio di genere. Per essere efficaci, i codici di condotta volontari dovrebbero basarsi su obiettivi chiari e indicatori chiave di prestazione che consentano di misurare il conseguimento di tali obiettivi. Essi dovrebbero inoltre essere elaborati in modo inclusivo, se del caso, con il coinvolgimento dei portatori di interessi pertinenti, quali le organizzazioni imprenditoriali e della società civile, il mondo accademico, le organizzazioni di ricerca, i sindacati e le organizzazioni per la tutela dei consumatori. 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.

(166) È importante che i sistemi di IA collegati a prodotti che non sono ad alto rischio in conformità del presente regolamento e che pertanto non sono tenuti a rispettare i requisiti stabiliti per i sistemi di IA ad alto rischio 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 il regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio ([53]).

(167) Al fine di garantire una cooperazione affidabile e costruttiva delle autorità competenti a livello dell'Unione e nazionale, 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, in conformità del diritto dell'Unione o nazionale. Dovrebbero svolgere i loro compiti e le loro attività in modo da proteggere, in particolare, i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali, l'efficace attuazione del presente regolamento, gli interessi pubblici e di sicurezza nazionale, l'integrità del procedimento penale o amministrativo e l'integrità delle informazioni classificate.

(168) Il rispetto del presente regolamento dovrebbe essere reso esecutivo mediante l'imposizione di sanzioni e di altre misure di esecuzione. 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, anche nel rispetto del principio ne bis in idem. Al fine di rafforzare e armonizzare le sanzioni amministrative in caso di violazione del presente regolamento, è opportuno stabilire limiti massimi per la fissazione delle sanzioni amministrative pecuniarie per talune violazioni specifiche. Nel valutare l'importo delle sanzioni amministrative pecuniarie, gli Stati membri dovrebbero, in ogni singolo caso, tenere conto di tutte le circostanze pertinenti della situazione specifica, in particolare, della natura, della gravità e della durata della violazione e delle sue conseguenze e delle dimensioni del fornitore, in particolare se si tratta di una PMI, compresa una start-up. 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.

(169) Il rispetto degli obblighi imposti ai fornitori di modelli di IA per finalità generali a norma del presente regolamento dovrebbe essere reso esecutivo, tra l'altro, mediante sanzioni pecuniarie. A tal fine è opportuno stabilire livelli adeguati di sanzioni pecuniarie anche in caso di violazione di tali obblighi, tra cui il mancato rispetto delle misure richieste dalla Commissione a norma del presente regolamento, fatti salvi adeguati termini di prescrizione conformemente al principio di proporzionalità. Tutte le decisioni prese dalla Commissione a norma del presente regolamento sono soggette al controllo della Corte di giustizia dell'Unione europea conformemente al TFUE, compresa la giurisdizione, anche di merito, della Corte di giustizia riguardo alle sanzioni ai sensi dell'articolo 261 TFUE

(170) Il diritto dell'Unione e nazionale prevedono già mezzi di ricorso efficaci per le persone fisiche e giuridiche sui cui diritti e sulle cui libertà incide negativamente l'uso dei sistemi di IA. Fatti salvi tali mezzi di ricorso, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione del presente regolamento dovrebbe avere il diritto di presentare un reclamo alla pertinente autorità di vigilanza del mercato.

(171) Le persone interessate dovrebbero avere il diritto di ottenere una spiegazione qualora la decisione di un deployer si basi principalmente sugli output di determinati sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento e qualora tale decisione produca effetti giuridici o in modo analogo incida

([53]) Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n, 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio (GU L 135 del 23.5.2023, pag. 1).

significativamente su tali persone in un modo che esse ritengano avere un impatto negativo sulla loro salute, sicurezza o sui loro diritti fondamentali. Tale spiegazione dovrebbe essere chiara e significativa e fornire una base su cui le persone interessate possano esercitare i loro diritti. Il diritto di ottenere una spiegazione non dovrebbe applicarsi all'uso di sistemi di IA per i quali il diritto dell'Unione o nazionale prevede eccezioni o restrizioni e dovrebbe applicarsi solo nella misura in cui tale diritto non sia già previsto dal diritto dell'Unione.

(172) Le persone che agiscono in qualità di informatori in merito alle violazioni del presente regolamento dovrebbero essere protette a norma del diritto dell'Unione. La direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio ([54]) dovrebbe pertanto applicarsi alla segnalazione di violazioni del presente regolamento e alla protezione delle persone che segnalano tali violazioni.

(173) 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 condizioni alle quali un sistema di IA non dovrebbe essere considerato ad alto rischio, l'elenco dei sistemi di IA ad alto rischio, le disposizioni relative alla documentazione tecnica, il contenuto della dichiarazione di conformità UE, le disposizioni relative alle procedure di valutazione della conformità, 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, la soglia, i parametri di riferimento e gli indicatori, anche integrando tali parametri di riferimento e indicatori, nelle regole per la classificazione di un modello di IA per finalità generali con rischio sistemico, i criteri per la designazione dei modelli di IA per finalità generali con rischio sistemico, la documentazione tecnica per i fornitori di modelli di IA per finalità generali e le informazioni sulla trasparenza per i fornitori di modelli di IA per finalità generali. 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 ([55]). 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.

(174) Dati i rapidi sviluppi tecnologici e le competenze tecniche necessarie per l'efficace applicazione del presente regolamento, la Commissione dovrebbe valutare e riesaminare il presente regolamento entro il 2 agosto 2029 e successivamente ogni quattro anni e presentare una relazione al Parlamento europeo e al Consiglio. Inoltre, tenuto conto delle implicazioni per l'ambito di applicazione del presente regolamento, la Commissione dovrebbe effettuare, una volta all'anno, una valutazione della necessità di modificare l'elenco dei sistemi di IA ad alto rischio e l'elenco delle pratiche vietate. Inoltre, entro il 2 agosto 2028 e successivamente ogni quattro anni, la Commissione dovrebbe valutare la necessità di modificare l'elenco delle rubriche dei settori ad alto rischio di cui all'allegato del presente regolamento, i sistemi di IA che rientrano nell'ambito di applicazione degli obblighi di trasparenza, l'efficacia del sistema di supervisione e governance e i progressi compiuti riguardo allo sviluppo di prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico di modelli di IA per finalità generali, compresa la necessità di ulteriori misure o azioni, e riferire al Parlamento europeo e al Consiglio in merito. Entro il 2 agosto 2028 e successivamente ogni tre anni la Commissione dovrebbe valutare l'impatto e l'efficacia dei codici di condotta volontari per la promozione dell'applicazione dei requisiti previsti per i sistemi di IA ad alto rischio nel caso di sistemi di IA diversi dai sistemi di IA ad alto rischio ed eventualmente di altri requisiti supplementari per tali sistemi di IA.

(175) 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 ([56]).

(176) Poiché l'obiettivo del presente regolamento, vale a dire migliorare il funzionamento del mercato interno e promuovere la diffusione di un'IA antropocentrica e affidabile, garantendo nel contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e promuovendo

([54]) Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (GU L 305 del 26.11.2019, pag. 17).
([55]) GU L 123 del 12.5.2016, pag. 1.
([56]) 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).

l'innovazione, non può essere conseguito in misura sufficiente dagli Stati membri ma, 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.

(177) Al fine di garantire la certezza del diritto, assicurare un adeguato periodo di adattamento per gli operatori ed evitare perturbazioni del mercato, anche garantendo la continuità dell'uso dei sistemi di IA, è opportuno che il presente regolamento si applichi ai sistemi di IA ad alto rischio che sono stati immessi sul mercato o messi in servizio prima della data generale di applicazione dello stesso, solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione o finalità prevista. È opportuno precisare che, a tale riguardo, il concetto di modifica significativa dovrebbe essere inteso come equivalente nella sostanza alla nozione di modifica sostanziale, utilizzata solo per i sistemi di IA ad alto rischio a norma del presente regolamento. In via eccezionale e alla luce della responsabilità pubblica, gli operatori di sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati in un allegato del presente regolamento e gli operatori di sistemi di IA ad alto rischio destinati a essere utilizzati dalle autorità pubbliche dovrebbero adottare le misure necessarie per conformarsi ai requisiti del presente regolamento, rispettivamente, entro la fine del 2030 ed entro il 2 agosto 2030.

(178) I fornitori di sistemi di IA ad alto rischio sono incoraggiati a iniziare a rispettare, su base volontaria, i pertinenti obblighi del presente regolamento già durante il periodo transitorio.

(179) Il presente regolamento si dovrebbe applicare a decorrere dal 2 agosto 2026. Tuttavia, tenuto conto del rischio inaccettabile associato all'uso dell'IA in determinati modi, i divieti nonché le disposizioni generali del presente regolamento dovrebbero applicarsi già a decorrere dal 2 febbraio 2025. Sebbene la piena efficacia di tali divieti discenda dall'istituzione della governance e dall'esecuzione del presente regolamento, è importante anticipare l'applicazione di detti divieti per tenere conto dei rischi inaccettabili e avere un effetto su altre procedure, ad esempio nel diritto civile. È inoltre opportuno che l'infrastruttura relativa alla governance e al sistema di valutazione della conformità sia operativa prima del 2 agosto 2026, pertanto le disposizioni sugli organismi notificati e sulla struttura di governance dovrebbero applicarsi a decorrere dal 2 agosto 2025. In considerazione del rapido ritmo dello sviluppo tecnologico e dell'adozione di modelli di IA per finalità generali, gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero applicarsi a decorrere dal 2 agosto 2025. I codici di buone pratiche dovrebbero essere pronti entro 2 agosto 2025 al fine d consentire ai fornitori di dimostrare la conformità «in tempo utile». L'ufficio per l'IA dovrebbe garantire che le norme e le procedure di classificazione siano aggiornate alla luce degli sviluppi tecnologici. 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 2 agosto 2025.

(180) Conformemente all'articolo 42, paragrafi 1 e 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 congiunto il 18 giugno 2021,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

1. Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione.

2. Il presente regolamento stabilisce:

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

b) divieti di talune pratiche di IA;

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

d) regole di trasparenza armonizzate per determinati sistemi di IA;

e) regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali;

f) regole in materia di monitoraggio del mercato, vigilanza del mercato, governance ed esecuzione;

g) misure a sostegno dell'innovazione, con particolare attenzione alle PMI, comprese le start-up.

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 o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo;

b) ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione;

c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione;

d) agli importatori e ai distributori di sistemi di IA;

e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio;

f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione;

g) alle persone interessate che si trovano nell'Unione.

2. Ai sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, relativo a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, si applicano unicamente l'articolo 6, paragrafo 1, gli articoli da 102 a 109 e l'articolo 112. L'articolo 57 si applica solo nella misura in cui i requisiti per i sistemi di IA ad alto rischio a norma del presente regolamento siano stati integrati in tale normativa di armonizzazione dell'Unione.

3. Il presente regolamento non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze.

Il presente regolamento non si applica ai sistemi di IA se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

Il presente regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

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 della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri, a condizione che tale paese terzo o organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone.

5. Il presente regolamento non pregiudica l'applicazione delle disposizioni sulla responsabilità dei prestatori di servizi intermediari di cui al capo II del regolamento (UE) 2022/2065.

6. Il presente regolamento non si applica ai sistemi di IA o modelli di IA, ivi compresi i loro output, specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici.

7. Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento.

8. Il presente regolamento non si applica alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio. Tali attività sono svolte in conformità del diritto dell'Unione applicabile. Le prove in condizioni reali non rientrano in tale esclusione.

9. Il presente regolamento lascia impregiudicate le norme stabilite da altri atti giuridici dell'Unione in materia di protezione dei consumatori e di sicurezza dei prodotti.

10. Il presente regolamento non si applica agli obblighi dei deployer che sono persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale.

11. Il presente regolamento non osta a che l'Unione o gli Stati membri mantengano o introducano disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso dei sistemi di IA da parte dei datori di lavoro, o incoraggino o consentano l'applicazione di contratti collettivi più favorevoli ai lavoratori.

12. Il presente regolamento non si applica ai sistemi di IA rilasciati con licenza libera e open source, a meno che non siano immessi sul mercato o messi in servizio come sistemi di IA ad alto rischio o come sistema di IA rientrante nell'ambito di applicazione dell'articolo 5 o 50.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «sistema di IA»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

2) «rischio»: la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso;

3) «fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;

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

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

6) «importatore»: una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo;

7) «distributore»: una 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;

8) «operatore»: un fornitore, un fabbricante del prodotto, un deployer, un rappresentante autorizzato, un importatore o un distributore;

9) «immissione sul mercato»: la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione;

10) «messa a disposizione sul mercato»: la fornitura di un sistema di IA o di un modello di IA per finalità generali 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 al deployer per il primo uso o per uso proprio nell'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, ivi compresi altri sistemi di IA, ragionevolmente prevedibile;

14) «componente di sicurezza»: un componente di un prodotto o di un sistema di IA che svolge una funzione di sicurezza per tale prodotto o sistema di IA 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 il deployer in particolare della finalità prevista e dell'uso corretto di un sistema di IA;

16) «richiamo di un sistema di IA»: qualsiasi misura volta a ottenere la restituzione al fornitore, la messa fuori servizio o la disabilitazione dell'uso di un sistema di IA messo a disposizione dei deployer;

17) «ritiro di un sistema di IA»: qualsiasi misura volta a impedire che un sistema di IA nella catena di approvvigionamento sia messo a disposizione sul mercato;

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 dimostrare se i requisiti di cui al capo III, sezione 2, relativi a un sistema di IA ad alto rischio 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 notificato in conformità del presente regolamento e di altre pertinenti normative di armonizzazione dell'Unione;

23) «modifica sostanziale»: una modifica di un sistema di IA a seguito della sua immissione sul mercato o messa in servizio che non è prevista o programmata nella valutazione iniziale della conformità effettuata dal fornitore e che ha l'effetto di incidere sulla conformità del sistema di IA ai requisiti di cui al capo III, sezione 2, o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato;

24) «marcatura CE»: una marcatura mediante la quale un fornitore indica che un sistema di IA è conforme ai requisiti stabiliti al capo III, sezione 2, e in altre normative di armonizzazione dell'Unione applicabili e che ne prevedono l'apposizione;

25) «sistema di monitoraggio successivo all'immissione sul mercato»: tutte le attività svolte dai fornitori di sistemi di IA al fine diraccogliere e analizzare 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 armonizzata di cui all'articolo 2, punto 1), lettera c), del regolamento (UE) n, 1025/2012;

28) «specifiche comuni»: un insieme di specifiche tecniche quali definite all'articolo 2, punto 4), del regolamento (UE) n, 1025/2012, che forniscono i mezzi persoddisfare determinati requisitistabiliti a norma del presente regolamento;

29) «dati di addestramento»: i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere;

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 tra l'altro di evitare lo scarso (underfitting) o l'eccessivo (overfitting) adattamento ai dati di addestramento;

31) «set di dati di convalida»: un set di dati distinto o costituito da una partizione fissa o variabile del set di dati di addestramento;

32) «dati di prova»: i dati utilizzati per fornire una valutazione indipendente delsistema di IA al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;

33) «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;

34) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica,quali le immagini facciali o i dati dattiloscopici;

35) «identificazione biometrica»: il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati;

36) «verifica biometrica»: la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza;

37) «categorie particolari di dati personali»: le categorie 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;

38) «dati operativi sensibili»: dati operativi relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali;

39) «sistema di riconoscimento delle emozioni»: un sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;

40) «sistema di categorizzazione biometrica»: un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive;

41) «sistema di identificazione biometrica remota»: un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento;

42) «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, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione;

43) «sistema di identificazione biometrica remota a posteriori»: un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota «in tempo reale»;

44) «spazio accessibile al pubblico»: qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che possano applicarsi determinate condizioni di accesso e indipendentemente dalle potenziali restrizioni di capacità;

45) «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; oppure

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;

46) «attività di contrasto»: le attività svolte dalle autorità di contrasto o per loro conto 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;

47) «ufficio per l'IA»: la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA prevista dalla decisione della Commissione del 24 gennaio 2024. I riferimenti all'ufficio per l'IA contenuti nel presente regolamento si intendono fatti alla Commissione;

48) «autorità nazionale competente»: un'autorità di notifica o un'autorità di vigilanza del mercato; per quanto riguarda i sistemi di IA messi in servizio o utilizzati da istituzioni, organi e organismi dell'Unione, i riferimenti alle autorità nazionali competenti o alle autorità di vigilanza del mercato contenuti nel presente regolamento si intendono fatti al Garante europeo della protezione dei dati;

49) «incidente grave»: un incidente o malfunzionamento di un sistema di IA che, direttamente o indirettamente, causa una delle conseguenze seguenti:

a) il decesso di una persona o gravi danni alla salute di una persona;

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

c) la violazione degli obblighi a norma del diritto dell'Unione intesi a proteggere i diritti fondamentali;

d) gravi danni alle cose o all'ambiente;

50) «dati personali»: i dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;

51) «dati non personali»: dati diversi dai dati personali di cui all'articolo 4, punto 1), del regolamento (UE) 2016/679;

52) «profilazione»: la profilazione quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679;

53) «piano di prova in condizioni reali»: un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali;

54) «piano dello spazio di sperimentazione»: un documento concordato tra il fornitore partecipante e l'autorità competente in cui sono descritti gli obiettivi, le condizioni, il calendario, la metodologia e i requisiti relativamente alle attività svolte all'interno dello spazio di sperimentazione;

55) «spazio di sperimentazione normativa per l'IA»: un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare;

56) «alfabetizzazione in materia di IA»: le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare;

57) «prova in condizioni reali»: la prova temporanea di un sistema di IA per la sua finalità prevista in condizioni reali al di fuori di un laboratorio o di un ambiente altrimenti simulato al fine di raccogliere dati affidabili e solidi e di valutare e verificare la conformità del sistema di IA ai requisiti del presente regolamento e che non è considerata immissione sul mercato o messa in servizio del sistema di IA ai sensi del presente regolamento, purché siano soddisfatte tutte le condizioni di cui all'articolo 57 o 60;

58) «soggetto»: ai fini della prova in condizioni reali, una persona fisica che partecipa a prove in condizioni reali;

59) «consenso informato»: l'espressione libera, specifica, inequivocabile e volontaria di un soggetto della propria disponibilità a partecipare a una determinata prova in condizioni reali, dopo essere stato informato di tutti gli aspetti della prova rilevanti per la sua decisione di partecipare;

60) «deep fake»: un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona;

61) «infrazione diffusa»: qualsiasi azione od omissione contraria al diritto dell'Unione che tutela gli interessi delle persone:

a) che abbia arrecato o possa arrecare un danno agli interessi collettivi di persone che risiedono in almeno due Stati membri diversi dallo Stato membro in cui:

i) ha avuto origine o si è verificato l'azione o l'omissione in questione;

ii) è ubicato o stabilito il fornitore interessato o, se del caso, il suo rappresentante autorizzato; oppure

iii) è stabilito il deployer, quando la violazione è commessa dal deployer;

b) che abbia arrecato, arrechi o possa arrecare un danno agli interessi collettivi di persone e che presenti caratteristiche comuni, compresa la stessa pratica illecita e lo stesso interesse leso e che si verifichi simultaneamente, commessa dal medesimo operatore, in almeno tre Stati membri;

62) «infrastruttura critica»: infrastruttura critica quale definita all'articolo 2, punto 4), della direttiva (UE) 2022/2557;

63) «modello di IA per finalità generali»: un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

64) «capacità di impatto elevato»: capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati;

65) «rischio sistemico»: un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore;

66) «sistema di IA per finalità generali»: un sistema di IA basato su un modello di IA per finalità generali e che ha la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA;

67) «operazione in virgola mobile»: qualsiasi operazione o assegnazione matematica che comporta numeri in virgola mobile, un sottoinsieme dei numeri reali generalmente rappresentati sui computer mediante un numero intero con precisione fissa avente come fattore di scala un esponente intero di una base fissa;

68) «fornitore a valle»: un fornitore di un sistema di IA, compreso un sistema di IA per finalità generali, che integra un modello di IA, indipendentemente dal fatto che il modello di IA sia fornito dallo stesso e integrato verticalmente o fornito da un'altra entità sulla base di relazioni contrattuali.

Articolo 4

Alfabetizzazione in materia di IA

I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.

CAPO II

PRATICHE DI IA VIETATE

Articolo 5

Pratiche di IA vietate

1. Sono vietate le pratiche di IA 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 o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo;

b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo;

c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IAper la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:

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

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

d) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa;

e) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;

f) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza;

g) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto;

h) l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrastoa meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:

i) la ricerca mirata di specifichevittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;

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

iii) lalocalizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

La lettera h) del primo comma lascia impregiudicato l'articolo 9 del regolamento (UE) 2016/679 per quanto riguarda il trattamento dei dati biometrici a fini diversi dall'attività di contrasto.

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, primo comma, lettera h), è applicato ai fini di cui a tale lettera, solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti:

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

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

L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), del presente articolo rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali. L'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico è autorizzato solo se l'autorità di contrasto ha completato una valutazione d'impatto sui diritti fondamentali come previsto all'articolo 27 e ha registrato il sistema nella banca dati UE conformemente all'articolo 49. Tuttavia, in situazioni di urgenza debitamente giustificate, è possibile iniziare a usare tali sistemi senza la registrazione nella banca dati dell'UE, a condizione che tale registrazione sia completata senza indebito ritardo.

3. Ai fini del paragrafo 1, primo comma, lettera h), e del paragrafo 2, ogniuso 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 oda un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità delle regole dettagliate del diritto nazionale di cui al paragrafo 5. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati.

L'autorità giudiziaria competente o un'autorità amministrativa indipendente la cui decisione è vincolante rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota «in tempo reale» in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, primo comma, lettera h), come indicato nella richiesta e, in

particolare, rimane limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale. Nel decidere in merito alla richiesta, tale autorità tiene conto degli elementi di cui al paragrafo 2. Nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota «in tempo reale».

4. Fatto salvo il paragrafo 3, ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è notificato alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati conformemente alle regole nazionali di cui al paragrafo 5. La notifica contiene almeno le informazioni di cui al paragrafo 6 e non include dati operativi sensibili.

5. 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, primo comma, lettera h), e ai paragrafi 2 e 3. Gli Stati membri interessati stabiliscono 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 e comunicazione ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, primo comma, lettera h), compresi i reati di cui alla lettera h), punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto. Gli Stati membri notificano tali regole alla Commissione al più tardi 30 giorni dopo la loro adozione. Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota.

6. Le autorità nazionali di vigilanza del mercato e le autorità nazionali per la protezione dei dati degli Stati membri cui è stato notificato l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a norma del paragrafo 4, presentano alla Commissione relazioni annuali su tale uso. A tal fine, la Commissione fornisce agli Stati membri e alle autorità nazionali di vigilanza del mercato e di protezione dei dati un modello comprendente informazioni sul numero di decisioni che le autorità giudiziarie competenti, o un'autorità amministrativa indipendente la cui decisione è vincolante, hanno adottato in risposta alle richieste di autorizzazione a norma del paragrafo 3 e il loro esito.

7. La Commissione pubblica relazioni annuali sull'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, fondate sui dati aggregati negli Stati membri sulla base delle relazioni annuali di cui al paragrafo 6. Tali relazioni annuali non includono dati operativi sensibili delle relative attività di contrasto.

8. Il presente articolo lascia impregiudicati i divieti che si applicano qualora una pratica di IA violi altre disposizioni di diritto dell'Unione.

CAPO III

SISTEMI DI IA AD ALTO RISCHIO

SEZIONE 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 indipendentemente dai 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 il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

b) il prodotto, il cui componente di sicurezza a norma della lettera a) 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 I.

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.

3. In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.

Il primo comma si applica quando è soddisfatta almeno una qualsiasi delle condizioni seguenti:

a) il sistema di IA è destinato a eseguire un compito procedurale limitato;

b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata;

c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o

d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

Fatto salvo il primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.

4. Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione.

5. Dopo aver consultato il consiglio europeo per l'intelligenza artificiale («consiglio per l'IA»), ed entro il 2 febbraio 2026, la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo in linea con l'articolo 96, insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio.

6. Alla Commissione è conferito il potere di adottare atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo aggiungendo nuove condizioni a quelle ivi stabilite, oppure modificandole, qualora vi siano prove concrete e affidabili dell'esistenza di sistemi di IA che rientrano nell'ambito di applicazione dell'allegato III ma non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

7. La Commissione adotta atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo sopprimendo qualsiasi condizione ivi stabilita, qualora vi siano prove concrete e affidabili che è necessario al fine di mantenere il livello di protezione della salute, della sicurezza e dei diritti fondamentali previsto dal presente regolamento.

8. Eventuali modifiche alle condizioni di cui al paragrafo 3, secondo comma, adottate in conformità dei paragrafi 6 e 7 del presente articolo non riducono il livello globale di protezione della salute, della sicurezza e dei diritti fondamentali nell'Unione previsto dal presente regolamento e garantiscono la coerenza con gli atti delegati adottati a norma dell'articolo 7, paragrafo 1, e tengono conto degli sviluppi tecnologici e del mercato.

Articolo 7

Modifiche dell'allegato III

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato III aggiungendo o modificando i casi d'uso dei 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 nell'allegato III;

b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali, e tale rischio è 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 la condizione di cui al paragrafo 1, lettera b), 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 natura e la quantità di dati trattati e utilizzati dal sistema di IA, in particolare l'eventualità che siano trattate categorie particolari di dati personali;

d) la misura in cui il sistema di IA agisce autonomamente e la possibilità che un essere umano annulli una decisione o una raccomandazione che potrebbe causare un danno potenziale;

e) la misura in cui l'uso di un sistema di IA ha già causato un danno alla salute e alla sicurezza, ha avuto un impatto negativo sui diritti fondamentali o ha suscitato gravi preoccupazioni in relazione alla probabilità di tale danno o impatto negativo, come dimostrato, ad esempio, da relazioni o da prove documentate presentate alle autorità nazionali competenti o da altre relazioni, a seconda dei casi;

f) la portata potenziale di tale danno o di tale impatto negativo, in particolare in termini di intensità e capacità di incidere su più persone o di incidere in modo sproporzionato su un particolare gruppo di persone;

g) 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 in ragione del fatto che per motivi pratici o giuridici non è ragionevolmente possibile sottrarsi a tale risultato;

h) la misura in cui esiste uno squilibrio di potere o le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto al deployer di un sistema di IA, in particolare a causa della condizione, dell'autorità, della conoscenza, della situazione economica o sociale o dell'età;

i) la misura in cui il risultato prodotto con il coinvolgimento di un sistema di IA è facilmente correggibile o reversibile, tenendo conto delle soluzioni tecniche disponibili per correggerlo o ribaltarlo, considerando non facilmente correggibili o reversibili i risultati che hanno un impatto negativo sulla salute, sulla sicurezza o sui diritti fondamentali;

j) l'entità e la probabilità dei benefici derivanti dalla diffusione del sistema di IA per le persone, i gruppi o la società in generale, compresi i possibili miglioramenti della sicurezza del prodotto;

k) la misura in cui il vigente diritto 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.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'elenco di cui all'allegato III rimuovendo sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) il sistema di IA ad alto rischio interessato non pone più rischi significativi per i diritti fondamentali, la salute o la sicurezza, tenendo conto dei criteri elencati al paragrafo 2;

b) la soppressione non riduce il livello generale di protezione della salute, della sicurezza e dei diritti fondamentali a norma del diritto dell'Unione.

SEZIONE 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 nella presente sezione, tenendo conto delle loro previste finalità nonché dello stato dell'arte generalmente riconosciuto in materia di IA e di tecnologie correlate all'IA. Nel garantire conformità a tali requisiti si tiene conto del sistema di gestione dei rischi di cui all'articolo 9.

2. Se un prodotto contiene un sistema di IA cui si applicano i requisiti del presente regolamento e i requisiti della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, i fornitori sono responsabili di garantire che il loro prodotto sia pienamente conforme a tutti i requisiti applicabili previsti dalla normativa di armonizzazione dell'Unione applicabile. Nel garantire la conformità dei sistemi di IA ad alto rischio di cui al paragrafo 1 ai requisiti di cui alla presente sezione e al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari processi di prova e di comunicazione nonché le informazioni e la documentazione che forniscono relativamente al loro prodotto nella documentazione e nelle procedure esistenti e richieste in conformità della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A.

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 inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. Esso comprende le fasi seguenti:

a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista;

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 72;

d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lettera a).

3. I rischi di cui al presente articolo riguardano solo quelli che possono essere ragionevolmente attenuati o eliminati attraverso lo sviluppo o la progettazione del sistema di IA ad alto rischio o la fornitura di informazioni tecniche adeguate.

4. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), tengono in debita considerazione gli effetti e la possibile interazione derivanti dall'applicazione combinata dei requisiti di cui alla presente sezione, al fine di ridurre al minimo i rischi con maggiore efficacia e raggiungere nel contempo un equilibrio adeguato nell'attuazione delle misure volte a soddisfare tali requisiti.

5. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili.

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

a) l'eliminazione o la riduzione dei rischi individuati e valutati a norma del paragrafo 2, per quanto possibile dal punto di vista tecnico attraverso un'adeguata progettazione e fabbricazione del sistema di IA ad alto rischio;

b) ove opportuno, l'attuazione di adeguate misure di attenuazione e di controllo nell'affrontare i rischi che non possono essere eliminati;

c) la fornitura delle informazioni richieste a norma dell'articolo 13 e, ove opportuno, la formazione dei deployer.

Al fine di 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 dal deployer e il contesto presumibile in cui il sistema è destinato ad essere usato.

6. I sistemi di IA ad alto rischio sono sottoposti a prova al fine di individuare le misure di gestione dei rischi più appropriate e mirate. 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 alla presente sezione.

7. Le procedure di prova possono comprendere prove in condizioni reali conformemente all'articolo 60.

8. 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 della loro immissione sul mercato o messa in servizio. Le prove sono effettuate sulla base di metriche e soglie probabilistiche definite precedentemente e adeguate alla finalità prevista perseguita dal sistema di IA ad alto rischio.

9. Nell'attuare il sistema di gestione dei rischi di cui ai paragrafi da 1 a 7, i fornitori prestano attenzione, nell'ottica della sua finalità prevista, all'eventualità che il sistema di IA ad alto rischio possa avere un impatto negativo sulle persone di età inferiore a 18 anni o, a seconda dei casi, su altri gruppi vulnerabili.

10. Per i fornitori di sistemi di IA ad alto rischio soggetti ai requisiti relativi ai processi interni di gestione dei rischi a norma di altre disposizioni pertinenti del diritto dell'Unione, gli aspetti di cui ai paragrafi da 1 a 9 possono far parte delle procedure di gestione dei rischi stabilite a norma di tale diritto oppure essere combinati con le stesse.

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 di IA 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 ogniqualvolta siano utilizzati tali set di dati.

2. I set di dati di addestramento, convalida e prova sono soggetti a pratiche di governance e gestione dei dati adeguate alla finalità prevista del sistema di IA ad alto rischio. Tali pratiche riguardano in particolare:

a) le scelte progettuali pertinenti;

b) i processi di raccolta dei dati e l'origine dei dati, nonché la finalità originaria della raccolta nel caso di dati personali;

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

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

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

f) un esame atto a valutare le possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future;

g) le misure adeguate per individuare, prevenire e attenuare le possibili distorsioni individuate conformemente alla lettera f);

h) l'individuazione di lacune o carenze pertinenti nei dati tali da pregiudicare il rispetto del presente regolamento e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova sono pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista. Essi possiedono le proprietà statistiche appropriate anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone relativamente ai 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 a livello di una combinazione degli stessi.

4. I set di dati tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico ambito geografico, contestuale, 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 garantireil rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio in conformità del paragrafo 2, lettere f) e g), del presente articolo, i fornitori di tali sistemi possono eccezionalmente trattare categorie particolari di dati personali, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche. Oltre alle disposizioni di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680 devono essere soddisfatte, affinché tale trattamento avvenga, tutte le condizioni seguenti:

a) il rilevamento e la correzione delle distorsioni non possono essere realizzati efficacemente mediante il trattamento di altri dati, compresi i dati sintetici o anonimizzati;

b) le categorie particolari di dati personali sono soggette a limitazioni tecniche relative al riutilizzo dei dati personali, nonché a misure più avanzate di sicurezza e di tutela della vita privata, compresa la pseudonimizzazione;

c) le categorie particolari di dati personali sono soggette a misure tese a garantire che i dati personali trattati siano resi sicuri e protetti nonché soggetti a garanzie adeguate, ivi compresi controlli e documentazione rigorosi dell'accesso, al fine di evitare abusi e garantire che solo le persone autorizzate e sottostanti a opportuni obblighi di riservatezza abbiano accesso a tali dati personali;

d) le categorie particolari di dati personali non devono essere trasmesse, trasferite o altrimenti consultate da terzi;

e) le categorie particolari di dati personali vengono cancellate dopo che la distorsione è stata corretta oppure i dati personali hanno raggiunto la fine del loro periodo di conservazione, a seconda di quale delle due condizioni si verifica per prima;

f) i registri delle attività di trattamento a norma dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680 comprendono i motivi per cui il trattamento delle categorie particolari di dati personali era strettamente necessario per rilevare e correggere distorsioni e i motivi per cui tale obiettivo non poteva essere raggiunto mediante il trattamento di altri dati.

6. Per lo sviluppo di sistemi di IA ad alto rischio che non utilizzano tecniche che prevedono l'addestramento di modelli di IA, i paragrafi da 2 a 5 si applicano solo ai set di dati di prova.

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 alla presente sezione e da fornire alle autorità nazionali competenti e agli organismi notificati, in forma chiara e comprensibile, le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. Essa contiene almeno gli elementi di cui all'allegato IV. Le PMI, comprese le start-up, possono fornire in modo semplificato gli elementi della documentazione tecnica specificati nell'allegato IV. A tal fine la Commissione definisce un modulo di documentazione tecnica semplificata che risponda alle esigenze delle piccole imprese e delle microimprese. Qualora una PMI, compresa una start-up, decida di fornire in modo semplificato le informazioni richieste nell'allegato IV, utilizza il modulo di cui al presente paragrafo. Gli organismi notificati accettano il modulo ai fini della valutazione della conformità.

2. Se è immesso sul mercato o messo in servizio un sistema di IA ad alto rischio connesso a un prodotto contemplato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, si redige un'unica documentazione tecnica contenente tutte le informazioni di cui al paragrafo 1 e le informazioni necessarie a norma di tali atti giuridici.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 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 alla presente sezione.

Articolo 12

Conservazione delle registrazioni

1. I sistemi di IA ad alto rischio consentono a livello tecnico la registrazione automatica degli eventi («log») per la durata del ciclo di vita del sistema.

2. Al fine di garantire un livello di tracciabilità del funzionamento del sistema di IA ad alto rischio adeguato alla finalità prevista del sistema, le capacità di registrazione consentono la registrazione di eventi pertinenti per:

a) l'individuazione di situazioni che possono far sì che il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, o determinare una modifica sostanziale;

b) l'agevolazione del monitoraggio successivo all'immissione sul mercato di cui all'articolo 72; e

c) il monitoraggio del funzionamento dei sistemi di IA ad alto rischio di cui all'articolo 26, paragrafo 5.

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

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 utilizzata dal sistema per verificare 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 ai deployer

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 ai deployer 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 del fornitore e del deployer di cui alla sezione 3.

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

3. Le istruzioni per l'uso contengono almeno le informazioni seguenti:

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 che ci si può attendere, comprese le metriche, di 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 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 della 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 di cui all'articolo 9, paragrafo 2;

iv) se del caso, le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output;

v) ove opportuno, le sue prestazioni per quanto riguarda le persone o i gruppi di persone specifici sui quali il sistema è destinato a essere utilizzato;

vi) 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 ad alto rischio;

vii) se del caso, informazioni che consentano ai deployer di interpretare l'output del sistema di IA ad alto rischio e di usarlo in modo opportuno;

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 ad alto rischio da parte dei deployer;

e) le risorse computazionali e di hardware necessarie, la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura, compresa la relativa frequenza, necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software;

f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai deployer di raccogliere, conservare e interpretare correttamente i log in conformità dell'articolo 12.

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 sono 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 qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione.

3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti:

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 dal deployer.

4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al deployer in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di:

a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese;

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 in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche;

c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;

d) 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) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.

5. In aggiunta, per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 del presente articolo sono tali da garantire che il deployer non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità.

Il requisito di una verifica separata da parte di almeno due persone fisiche non si applica ai sistemi di IA ad alto rischio utilizzati a fini di contrasto, migrazione, controllo delle frontiere o asilo, qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito.

Articolo 15

Accuratezza, robustezza e cibersicurezza

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire 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. Al fine di affrontare gli aspetti tecnici relativi alle modalità di misurazione degli adeguati livelli di accuratezza e robustezza di cui al paragrafo 1 e altre metriche di prestazione pertinenti, la Commissione, in cooperazione con i portatori di interessi e le organizzazioni pertinenti, quali le autorità di metrologia e di analisi comparativa, incoraggia, se del caso, lo sviluppo di parametri di riferimento e metodologie di misurazione.

3. 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.

4. I sistemi di IA ad alto rischio sono il più resilienti possibile 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. A tale riguardo sono adottate misure tecniche e organizzative.

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 eliminare o ridurre il più possibile il rischio di output potenzialmente distorti che influenzano gli input per operazioni future (feedback loops - «circuiti di feedback») e garantire che tali circuiti di feedback siano oggetto di adeguate misure di attenuazione.

5. I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso, gli output 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, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (data poisoning - «avvelenamento dei dati») o i componenti preaddestrati utilizzati nell'addestramento (model poisoning - «avvelenamento dei modelli»), gli input progettati in modo da far sì che il modello di IA commetta un errore (adversarial examples - «esempi antagonistici», o model evasion, - «evasione dal modello»), gli attacchi alla riservatezza o i difetti del modello.

SEZIONE 3

Obblighi dei fornitori e dei deployer 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 alla sezione 2;

b) indicano sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento, a seconda dei casi, il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati;

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

d) conservano la documentazione di cui all'articolo 18;

e) quando sono sotto il loro controllo, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio di cui all'articolo 19;

f) garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità di cui all'articolo 43 prima che sia immesso sul mercato o messo in servizio;

g) elaborano una dichiarazione di conformità UE a norma dell'articolo 47;

h) appongono la marcatura CE sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento per indicare la conformità al presente regolamento a norma dell'articolo 48;

i) rispettano gli obblighi di registrazione di cui all'articolo 49, paragrafo 1;

j) adottano le necessarie misure correttive e forniscono le informazioni necessarie in conformità dell'articolo 20;

k) su richiesta motivata di un'autorità nazionale competente, dimostrano la conformità del sistema di IA ad alto rischio ai requisiti di cui alla sezione 2;

l) garantiscono che il sistema di IA ad alto rischio sia conforme ai requisiti di accessibilità in conformità delle direttive (UE) 2016/2102 e (UE) 2019/882.

Articolo 17

Sistema di gestione della qualità

1. I fornitori di sistemi di IA ad alto rischio istituiscono 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 gli aspetti seguenti:

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, o non includano tutti i requisiti pertinenti di cui alla sezione 2, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme a tali requisiti;

f) i sistemi e le procedure per la gestione dei dati, compresa l'acquisizione, 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 72;

i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 73;

j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, comprese quelle 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. I fornitori rispettano, in ogni caso, il grado di rigore e il livello di protezione necessari per garantire la conformità dei loro sistemi di IA ad alto rischio al presente regolamento.

3. I fornitori di sistemi di IA ad alto rischio soggetti agli obblighi relativi ai sistemi di gestione della qualità o a una funzione equivalente a norma del pertinente diritto settoriale dell'Unione possono includere gli aspetti elencati al paragrafo 1 nell'ambito dei sistemi di gestione della qualità stabiliti a norma di tale diritto.

4. Per i fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di istituire un sistema di gestione della qualità, ad eccezione del paragrafo 1, lettere g), h) e i), del presente articolo, si considera soddisfatto se sono soddisfatte le regole sui dispositivi o i processi di governance interna a norma del pertinente diritto dell'Unione in materia di servizi finanziari. A tal fine, si tiene conto delle norme armonizzate di cui all'articolo 40.

Articolo 18

Conservazione dei documenti

1. Il fornitore, per un periodo che termina 10 anni dopo che il sistema di IA ad alto rischio 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 47.

2. Ciascuno Stato membro stabilisce le condizioni alle quali la documentazione di cui al paragrafo 1 resta a disposizione delle autorità nazionali competenti per il periodo indicato in tale paragrafo nel caso in cui il prestatore o il rappresentante autorizzato stabilito nel suo territorio fallisca o cessi la sua attività prima della fine di tale periodo.

3. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, conservano la documentazione tecnica nell'ambito della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari.

Articolo 19

Log generati automaticamente

1. I fornitori di sistemi di IA ad alto rischio conservano i log di cui all'articolo 12, paragrafo 1, generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo. Fatto salvo il diritto dell'Unione o nazionale applicabile, i log sono conservati per un periodo adeguato alla finalità prevista del sistema di IA ad alto rischio, della durata di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.

2. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, a dispositivi o a processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio nell'ambito della documentazione conservata a norma del pertinente diritto in materia di servizi finanziari.

Articolo 20

Misure correttive e dovere di informazione

1. 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, disabilitarlo o richiamarlo, a seconda dei casi. Essi informano di conseguenza i distributori del sistema di IA ad alto rischio interessato e, ove applicabile, i deployer, il rappresentante autorizzato e gli importatori.

2. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, e il fornitore ne venga a conoscenza, tale fornitore indaga immediatamente sulle cause, in collaborazione con il deployer che ha effettuato la segnalazione, se del caso, e ne informa le autorità di vigilanza del mercato competenti per il sistema di IA ad alto rischio interessato e, ove applicabile, l'organismo notificato che ha rilasciato un certificato per il sistema di IA ad alto rischio in conformità dell'articolo 44, in particolare in merito alla natura della non conformità e all'eventuale misura correttiva pertinente adottata.

Articolo 21

Cooperazione con le autorità competenti

1. I fornitori di sistemi di IA ad alto rischio, su richiesta motivata di un'autoritàcompetente, 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 alla sezione 2, in una lingua che può essere compresa facilmente dall'autorità in una delle lingue ufficiali delle istituzioni dell'Unione indicata dallo Stato membro interessato.

2. Su richiesta motivata di un'autorità competente, i fornitori concedono inoltre all'autorità competente richiedente, a seconda dei casi, l'accesso ai log generati automaticamente del sistema di IA ad alto rischio di cui all'articolo 12, paragrafo 1, nella misura in cui tali log sono sotto il loro controllo.

3. Qualsiasi informazione ottenuta da un'autorità competente a norma del presente articolo è trattata in conformità degli obblighi di riservatezza di cui all'articolo 78.

Articolo 22

Rappresentanti autorizzati dei fornitori dei sistemi di IA ad alto rischio

1. Prima di mettere a disposizione i sistemi di IA ad alto rischio sul mercato dell'Unione, i fornitori stabiliti in paesi terzi nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

2. Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore.

3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fornitore. Fornisce una copia del mandato alle autorità di vigilanza del mercato, su richiesta, in una delle lingue ufficiali delle istituzioni dell'Unione indicata dall'autorità competente. Ai fini del presente regolamento, il mandato consente al rappresentante autorizzato di eseguire i compiti seguenti:

a) verificare che la dichiarazione di conformità UE di cui all'articolo 47 e la documentazione tecnica di cui all'articolo 11 siano state redatte e che il fornitore abbia eseguito un'appropriata procedura di valutazione della conformità;

b) tenere a disposizione delle autorità competenti e delle autorità o degli organismi nazionali di cui all'articolo 74, paragrafo 10, per un periodo di 10 anni dopo la data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, i dati di contatto del fornitore che ha nominato il rappresentante autorizzato, una copia della dichiarazione di conformità UE di cui all'articolo 47, la documentazione tecnica e, se del caso, il certificato rilasciato dall'organismo notificato;

c) fornire all'autorità competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui alla lettera b) del presente comma, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, compreso l'accesso ai log, di cui all'articolo 12, paragrafo 1, generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore;

d) cooperare con le autoritàcompetenti, su richiesta motivata, in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio, in particolare per ridurre e attenuare i rischi posti dal sistema di IA ad alto rischio;

e) ove applicabile, rispettare gli obblighi di registrazione di cui all'articolo 49, paragrafo 1, o, se la registrazione è effettuata dal fornitore stesso, garantire la correttezza delle informazioni di cui all'allegato VIII, sezione A, punto 3.

Il mandato consente al rappresentante autorizzato di fare da interlocutore, in aggiunta o in sostituzione del fornitore, con le autorità competenti per tutte le questioni relative al rispetto del presente regolamento.

4. Il rappresentante autorizzato pone fine al mandato se ritiene o ha motivi per ritenere che il fornitore agisca in contrasto con i propri obblighi a norma del presente regolamento. In tal caso, comunica immediatamente alla pertinente autorità di vigilanza del mercato, nonché, se del caso, all'organismo notificato pertinente, la cessazione del mandato e i relativi motivi.

Articolo 23

Obblighi degli importatori

1. Prima di immettere sul mercato un sistema di IA ad alto rischio, gli importatori garantiscono che il sistema sia conforme al presente regolamento verificando che:

a) il fornitore di tale sistema di IA ad alto rischio abbia eseguito la pertinente procedura di valutazione della conformità di cui all'articolo 43;

b) il fornitore abbia redatto la documentazione tecnica conformemente all'articolo 11 e all'allegato IV;

c) il sistema rechi la necessaria marcatura CE e sia accompagnato dalla dichiarazione di conformità UE di cui all'articolo 47 e dalle istruzioni per l'uso;

d) il fornitore abbia nominato un rappresentante autorizzato conformemente all'articolo 22, paragrafo 1.

2. Qualora abbia motivo sufficiente di ritenere che un sistema di IA ad alto rischio non sia conforme al presente regolamento, ovvero sia falsificato o sia accompagnato da una documentazione falsificata, un importatore non lo immette sul mercato fino a quando non sia stato reso conforme. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, l'importatore ne informa il fornitore del sistema, i rappresentanti autorizzati 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 e sul suo imballaggio o in un documento di accompagnamento, ove applicabile.

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 alla sezione 2.

5. Gli importatori conservano, per un periodo di 10 anni dalla data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, una copia del certificato rilasciato dall'organismo notificato, se del caso, delle istruzioni per l'uso e della dichiarazione di conformità UE di cui all'articolo 47.

6. Gli importatori forniscono alla pertinente autorità competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui al paragrafo 5, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2 in una lingua che può essere compresa facilmente da tale autorità nazionale competente. A tal fine garantiscono altresì che la documentazione tecnica possa essere messa a disposizione di tale autorità.

7. Gli importatori cooperano con le pertinenti autorità competenti in qualsiasi azione intrapresa da tali autorità in relazione a un sistema di IA ad alto rischio immesso sul mercato dagli importatori, in particolare per ridurre e attenuare i rischi che esso comporta.

Articolo 24

Obblighi dei distributori

1. Prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che esso rechi la necessaria marcatura CE, che sia accompagnato da una copia della dichiarazione di conformità UE di cui all'articolo 47 e dalle istruzioni per l'uso e che il fornitore e l'importatore di tale sistema, a seconda dei casi, abbiano rispettato i loro rispettivi obblighi di cui all'articolo 16, lettere b) e c), e all'articolo 23, paragrafo 3.

2. Qualora ritenga o abbia motivo di ritenere, sulla base delle informazioni in suo possesso, che un sistema di IA ad alto rischio non sia conforme ai requisiti di cui alla sezione 2, 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 di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, 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 alla sezione 2.

4. Un distributore che ritiene o ha motivo di ritenere, sulla base delle informazioni in suo possesso, che un sistema di IA ad alto rischio che ha messo a disposizione sul mercato non sia conforme ai requisiti di cui alla sezione 2, 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 79, paragrafo 1, il distributore ne informa immediatamente il fornitore o l'importatore del sistema e le autorità competenti per il sistema di IA ad alto rischio interessate fornendo in particolare informazioni precise sulla non conformità e sulle eventuali misure correttive adottate.

5. Su richiesta motivata di una pertinente autorità competente, i distributori di un sistema di IA ad alto rischio forniscono a tale autorità tutte le informazioni e la documentazione concernenti le sue azioni a norma dei paragrafi da 1 a 4 necessarie per dimostrare la conformità di tale sistema ai requisiti di cui alla sezione 2.

6. I distributori cooperano con le pertinenti autorità competenti in qualsiasi azione intrapresa da tali autorità in relazione a un sistema di IA ad alto rischio messo a disposizione sul mercato dai distributori, in particolare per ridurre e attenuare il rischio che esso comporta.

Articolo 25

Responsabilità lungo la catena del valore dell'IA

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

a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo;

b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6;

c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6.

2. Qualora si verifichino le circostanze di cui al paragrafo 1, il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA non è più considerato fornitore di quel determinato sistema di IA ai fini del presente regolamento. Tale fornitore iniziale coopera strettamente con i nuovi fornitori e mette a disposizione le informazioni necessarie nonché fornisce l'accesso tecnico ragionevolmente atteso e qualsiasi altra forma di assistenza che sono richiesti per l'adempimento degli obblighi di cui al presente regolamento, in particolare per quanto riguarda la conformità alla valutazione della conformità dei sistemi di IA ad alto rischio. Il presente paragrafo non si applica nei casi in cui il fornitore iniziale abbia chiaramente specificato che il suo sistema di IA non deve essere trasformato in un sistema di IA ad alto rischio e pertanto non sia soggetto all'obbligo di consegnare la documentazione.

3. Nel caso dei sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fabbricante del prodotto è considerato il fornitore del sistema di IA ad alto rischio ed è soggetto agli obblighi di cui all'articolo 16, in una delle circostanze seguenti:

a) se il sistema di IA ad alto rischio è immesso sul mercato insieme al prodotto con il nome o il marchio del fabbricante del prodotto;

b) se il sistema di IA ad alto rischio è messo in servizio con il nome o il marchio del fabbricante del prodotto dopo che il prodotto è stato immesso sul mercato.

4. Il fornitore di un sistema di IA ad alto rischio e il terzo che fornisce un sistema di IA, strumenti, servizi, componenti o processi utilizzati o integrati in un sistema di IA ad alto rischio precisano, mediante accordo scritto, le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari, sulla base dello stato dell'arte generalmente riconosciuto per permettere al fornitore del sistema di IA ad alto rischio di adempiere pienamente agli obblighi di cui al presente regolamento. Il presente paragrafo non si applica ai terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti, diversi dai modelli di IA per finalità generali, con licenza libera e open source.

L'ufficio per l'IA può elaborare e raccomandare clausole contrattuali tipo volontarie tra i fornitori di sistemi di IA ad alto rischio e i terzi che forniscono strumenti, servizi, componenti o processi utilizzati o integrati in sistemi di IA ad alto rischio. Nell'elaborare tali clausole contrattuali tipo volontarie, l'ufficio per l'IA tiene conto dei possibili requisiti contrattuali applicabili in determinati settori o casi commerciali. Le clausole contrattuali tipo volontarie sono pubblicati e disponibili gratuitamente in un formato elettronico facilmente utilizzabile.

5. I paragrafi 2 e 3 lasciano impregiudicata la necessità di rispettare e proteggere i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali conformemente al diritto dell'Unione e nazionale.

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

1. I deployer di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 3 e 6.

2. I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.

3. Gli obblighi di cui ai paragrafi 1 e 2 lasciano impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale e la libertà del deployer di organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore.

4. Fatti salvi i paragrafi 1 e 2, nella misura in cui esercita il controllo sui dati di input, il deployer garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio.

5. I deployer monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informano i fornitori a tale riguardo conformemente all'articolo 72. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio ai sensi dell'articolo 79, paragrafo 1, i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il deployer non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 73. Tale obbligo non riguarda i dati operativi sensibili dei deployer dei sistemi di IA che sono autorità di contrasto.

Per i deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di monitoraggio di cui al primo comma si considera soddisfatto se sono soddisfatte le regole sui dispositivi, sui processi e sui meccanismi di governance interna a norma del pertinente diritto in materia di servizi finanziari.

6. I deployer di sistemi di IA ad alto rischio conservano i log generati automaticamente da tale sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per un periodo adeguato alla prevista finalità del sistema di IA ad alto rischio, di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.

I deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari conservano i log come parte della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari.

7. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti.

8. I deployer di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione rispettano gli obblighi di registrazione di cui all'articolo 49. Ove accertino che il sistema di IA ad alto rischio che intendono utilizzare non è stato registrato nella banca dati dell'UE di cui all'articolo 71, tali deployer non utilizzano tale sistema e ne informano il fornitore o il distributore.

9. Se del caso, i deployer di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 del presente regolamento 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.

10. Fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, *ex ante* o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato. Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato.

Se l'autorizzazione richiesta a norma del primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati.

In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa. Occorre garantire che nessuna decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'output di tali sistemi di identificazione biometrica remota a posteriori.

Il presente paragrafo lascia impregiudicati l'articolo 9 del regolamento (UE) 2016/679 e l'articolo 10 della direttiva (UE) 2016/680 riguardo al trattamento dei dati biometrici.

Indipendentemente dalla finalità o dal deployer, ciascun uso di tali sistemi di IA ad alto rischio è documentato nel pertinente fascicolo di polizia e messo a disposizione della pertinente autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati, su richiesta, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Il presente comma lascia impregiudicati i poteri conferiti alle autorità di controllo dalla direttiva (UE) 2016/680.

I deployer presentano alle pertinenti autorità di vigilanza del mercato e alle autorità nazionali per la protezione dei dati relazioni annuali sul loro uso di sistemi di identificazione biometrica remota a posteriori, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Le relazioni possono essere aggregate per coprire più di un utilizzo.

Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota a posteriori.

11. Fatto salvo l'articolo 50, del presente regolamento i deployer dei sistemi di IA ad alto rischio di cui all'allegato III che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche informano queste ultime che sono soggette all'uso del sistema di IA ad alto rischio. Per i sistemi di IA ad alto rischio utilizzati a fini di contrasto si applica l'articolo 13 della direttiva (UE) 2016/680.

12. I deployer cooperano con le pertinenti autorità competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione al sistema di IA ad alto rischio ai fini dell'attuazione del presente regolamento.

Articolo 27

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

1. Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i deployer effettuano una valutazione che comprende gli elementi seguenti:

a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;

b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;

c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico;

d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;

e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso;

f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

2. L'obbligo di cui al paragrafo 1 si applica al primo uso del sistema di IA ad alto rischio. Il deployer può, in casi analoghi, basarsi su valutazioni d'impatto sui diritti fondamentali effettuate in precedenza o su valutazioni d'impatto esistenti effettuate da un fornitore. Se, durante l'uso del sistema di IA ad alto rischio, ritiene che uno qualsiasi degli elementi elencati al paragrafo 1 sia cambiato o non sia più aggiornato, il deployer adotta le misure necessarie per aggiornare le informazioni.

3. Una volta effettuata la valutazione di cui al paragrafo 1 del presente articolo, il deployer notifica all'autorità di vigilanza del mercato i suoi risultati, presentando il modello compilato di cui al paragrafo 5 del presente articolo nell'ambito della notifica. Nel caso di cui all'articolo 46, paragrafo 1, i deployer possono essere esentati da tale obbligo di notifica.

4. Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati.

5. L'ufficio per l'IA elabora un modello di questionario, anche attraverso uno strumento automatizzato, per agevolare i deployer nell'adempimento dei loro obblighi a norma del presente articolo in modo semplificato.

SEZIONE 4

Autorità di notifica e organismi notificati

Articolo 28

Autorità di notifica

1. Ciascuno Stato membro designa o istituisce almeno 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. Tali procedure sono sviluppate nell'ambito della collaborazione tra le autorità di notifica di tutti gli Stati membri.

2. Gli Stati membri possono decidere che la valutazione e il monitoraggio di cui al paragrafo 1 siano eseguiti da un organismo nazionale di accreditamento ai sensi e in conformità del 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 alcuna delle attività eseguite dagli organismi di valutazione della conformità, né servizi di consulenza su base commerciale o concorrenziale.

6. Le autorità di notifica salvaguardano la riservatezza delle informazioni che ottengono conformemente all'articolo 78.

7. Le autorità di notifica dispongono di un numero adeguato di dipendenti competenti per l'adeguata esecuzione dei relativi compiti. I dipendenti competenti dispongono, se del caso, delle competenze necessarie per svolgere le proprie funzioni in settori quali le tecnologie dell'informazione, l'IA e il diritto, compreso il controllo dei diritti fondamentali.

Articolo 29

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 dei tipi di sistemi di IA per i 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 31.

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 tutte le prove documentali necessarie per la verifica, il riconoscimento e il monitoraggio periodico della sua conformità ai requisiti di cui all'articolo 31.

4. 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. L'organismo notificato aggiorna la documentazione di cui ai paragrafi 2 e 3 del presente articolo ogni volta che si verificano cambiamenti di rilievo, al fine di consentire all'autorità responsabile degli organismi notificati di monitorare e verificare il continuo rispetto di tutte le prescrizioni di cui all'articolo 31.

Articolo 30

Procedura di notifica

1. Le autorità di notifica possononotificare solo gli organismi di valutazione della conformità che siano conformi alle prescrizioni di cui all'articolo 31.

2. Le autorità di notifica notificano alla Commissione e agli altri Stati membri, utilizzando lo strumento elettronico di notifica elaborato e gestito dalla Commissione, ogni organismo di valutazione della conformità di cui al paragrafo 1.

3. La notifica di cui al paragrafo 2 del presente articolo include tutti i dettagli riguardanti le attività di valutazione della conformità, il modulo o i moduli di valutazione della conformità, i tipi di sistemi di IA interessati, nonché la relativa attestazione di competenza. Qualora una notifica non sia basata su un certificato di accreditamento di cui all'articolo 29, paragrafo 2, l'autorità di notifica fornisce alla Commissione e agli altri Stati membri le prove documentali che attestino la competenza dell'organismo di valutazione della conformità nonché le misure predisposte per fare in modo che tale organismo sia monitorato periodicamente e continui a soddisfare i requisiti di cui all'articolo 31.

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 due settimane dalla notifica da parte di un'autorità di notifica, qualora essa includa un certificato di accreditamento di cui all'articolo 29, paragrafo 2, o entro due mesi dalla notifica da parte dell'autorità di notifica, qualora essa includa le prove documentali di cui all'articolo 29, paragrafo 3.

5. Se sono sollevate obiezioni, la Commissione avvia senza ritardo consultazioni con gli Stati membri pertinenti e l'organismo di valutazione della conformità. Tenutone debito conto, la Commissione decide se l'autorizzazione è giustificata. La Commissione trasmette la propria decisione allo Stato membro interessato e all'organismo di valutazione della conformità pertinente.

Articolo 31

Requisiti relativi agli organismi notificati

1. Un organismo notificato è istituito a norma del diritto nazionale di uno Stato membro e ha personalità giuridica.

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 nonché i requisiti idonei di cibersicurezza.

3. La struttura organizzativa, l'assegnazione delle responsabilità, le linee di riporto e il funzionamento degli organismi notificati garantiscono la fiducia nelle loro prestazioni 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 nei sistemi di IA ad alto rischio oggetto della valutazione, nonché da eventuali concorrenti del fornitore. Ciò non preclude l'uso dei sistemi di IA ad alto rischio oggetto della valutazione che sono necessari per il funzionamento dell'organismo di valutazione della conformità o l'uso di tali sistemi di IA ad alto rischio per scopi privati.

5. L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale incaricato di svolgere i compiti di valutazione della conformità non intervengono direttamente nella progettazione, nello sviluppo, nella commercializzazione o nell'utilizzo di sistemi di IA ad alto rischio, né rappresentano i soggetti impegnati in tali attività. Essi non intraprendono alcuna attività che possa essere in conflitto con la loro indipendenza di giudizio o la loro integrità per quanto riguarda le attività di valutazione della conformità per le quali sono notificati. Ciò vale in particolare per i servizi di consulenza.

6. 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.

7. Gli organismi notificati dispongono di procedure documentate per garantire che il loro personale, i loro comitati, le affiliate, i subappaltatori e qualsiasi altra organizzazione associata o il personale di organismi esterni mantengano, conformemente all'articolo 78, la riservatezza delle informazioni di cui vengono in possesso nello svolgimento delle attività di valutazione della conformità, salvo quando la normativa 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 propri compiti a norma del presente regolamento, tranne che nei confronti delle autorità di notifica dello Stato membro in cui svolge le proprie attività.

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

9. Gli organismi notificati sottoscrivono un'adeguata assicurazione di responsabilità per le loro attività di valutazione della conformità, a meno che lo Stato membro in cui sono stabiliti non si assuma tale responsabilità a norma del diritto nazionale o non sia esso stesso direttamente responsabile della valutazione della conformità.

10. 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.

11. Gli organismi notificati dispongono di sufficienti competenze interne per poter valutare efficacemente i compiti svolti da parti esterne per loro conto.Gli organismi notificati dispongono permanentemente di sufficiente personale amministrativo, tecnico, giuridico e scientifico dotato di esperienza e conoscenze relative ai tipi di sistemi di IA, ai dati, al calcolo dei dati pertinenti, nonché ai requisiti di cui alla sezione 2.

12. 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.

Articolo 32

Presunzione di conformità ai requisiti relativi agli organismi notificati

Qualora dimostri la propria conformità ai criteri stabiliti nelle pertinenti norme armonizzate o in parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, l'organismo di valutazione della conformità è considerato conforme ai requisiti di cui all'articolo 31 nella misura in cui le norme armonizzate applicabili coprano tali requisiti.

Articolo 33

Affiliate degli organismi notificati e subappaltatori

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 31 e ne informa l'autorità di notifica.

2. Gli organismi notificati si assumono la completa responsabilità dei compiti eseguiti da eventuali subappaltatori o affiliate.

3. Le attività possono essere subappaltate o eseguite da un'affiliata solo con il consenso del fornitore. Gli organismi notificati mettono a disposizione del pubblico un elenco delle loro affiliate.

4. I documenti pertinenti riguardanti la valutazione delle qualifiche del subappaltatore o dell'affiliata e il lavoro da essi eseguito a norma del presente regolamento sono tenuti a disposizione dell'autorità di notifica per un periodo di cinque anni a decorrere dalla data in cui termina il contratto di subappalto.

Articolo 34

Obblighi operativi degli organismi notificati

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

2. Gli organismi notificati evitano oneri inutili per i fornitori nello svolgimento delle loro attività e tengono debitamente conto delle dimensioni del fornitore, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA ad alto rischio interessato, in particolare al fine di ridurre al minimo gli oneri amministrativi e i costi di conformità per le microimprese e le piccole imprese ai sensi della raccomandazione 2003/361/CE. L'organismo notificato rispetta tuttavia il grado di rigore e il livello di tutela necessari per la conformità del sistema di IA ad alto rischio rispetto ai requisiti del presente regolamento.

3. 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 28 per consentirle di svolgere le proprie attività di valutazione, designazione, notifica e monitoraggio e per agevolare la valutazione di cui alla presente sezione.

Articolo 35

Numeri di identificazione ed elenchi di organismi notificati

1. La Commissione assegna un numero di identificazione unico a ciascun organismo notificato, anche se un organismo è notificato a norma di più atti dell'Unione.

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

Articolo 36

Modifiche delle notifiche

1. L'autorità di notifica informa la Commissione e gli altri Stati membri di ogni pertinente modifica della notifica di un organismo notificato tramite lo strumento elettronico di notifica di cui all'articolo 30, paragrafo 2.

2. Le procedure di cui agli articoli 29 e 30 si applicano alle estensioni della portata della notifica.

In caso di modifiche della notifica diverse dalle estensioni della sua portata, si applicano le procedure stabilite nei paragrafi da 3 a 9.

3. Qualora decida di cessare le attività di valutazione della conformità, un organismo notificato ne informa l'autorità di notifica e i fornitori interessati quanto prima possibile e almeno un anno prima della cessazione delle attività qualora la cessazione sia stata programmata. I certificati dell'organismo notificato possono restare validi per un periodo di nove mesi dopo la cessazione delle attività dell'organismo notificato purché un altro organismo notificato abbia confermato per iscritto che assumerà la responsabilità per i sistemi di IA ad alto rischio coperti da tale certificato. Quest'ultimo organismo notificato completa una valutazione integrale dei sistemi di IA ad alto rischio coinvolti entro la fine del periodo di nove mesi indicato prima di rilasciare nuovi certificati per gli stessi sistemi. Qualora l'organismo notificato abbia cessato le proprie attività, l'autorità di notifica ritira la designazione.

4. Qualora un'autorità di notifica abbia motivo sufficiente di ritenere che un organismo notificato non soddisfa più i requisiti di cui all'articolo 31 o non adempie i suoi obblighi, l'autorità di notifica 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 non soddisfa più i requisiti di cui all'articolo 31 o non adempie i suoi obblighi, tale autorità limita, sospende o ritira ladesignazione, a seconda dei casi, in funzione della gravità del mancato rispetto di tali requisiti o dell'inadempimento di tali obblighi. Essa informa immediatamente la Commissione e gli altri Stati membri.

5. Qualora la sua designazione sia stata sospesa, limitata oppure ritirata interamente o in parte, l'organismo notificato informa i fornitori interessati al più tardi entro 10 giorni.

6. In caso di limitazione, sospensione o ritiro di una designazione, l'autorità di notifica adotta le misure appropriate per far sì che i fascicoli dell'organismo notificato interessato siano conservati e messi a disposizione delle autorità di notifica in altri Stati membri nonché delle autorità di vigilanza del mercato, su richiesta.

7. In caso di limitazione, sospensione o ritiro di una designazione, l'autorità di notifica:

a) valuta l'impatto sui certificati rilasciati dall'organismo notificato;

b) entro tre mesi dalla comunicazione delle modifiche della designazione, presenta alla Commissione e agli altri Stati membri una relazione sulle proprie constatazioni;

c) impone all'organismo notificato di sospendere o ritirare, entro un periodo di tempo ragionevole stabilito dall'autorità, i certificati rilasciati indebitamente al fine di garantire la continua conformità dei sistemi di IA ad alto rischio sul mercato;

d) informa la Commissione e gli Stati membri in merito ai certificati di cui ha richiesto la sospensione o il ritiro;

e) fornisce alle autorità nazionali competenti dello Stato membro in cui ha sede il fornitore tutte le informazioni pertinenti sui certificati di cui ha richiesto la sospensione o il ritiro; tale autorità adotta le misure appropriate, laddove necessario, per evitare un rischio potenziale per la salute, la sicurezza o i diritti fondamentali.

8. Ad eccezione dei certificati rilasciati indebitamente, e ove la designazione sia stata sospesa o limitata, i certificati restano validi in uno dei casi seguenti:

a) l'autorità di notifica ha confermato, entro un mese dalla sospensione o dalla limitazione, che sotto il profilo della salute, della sicurezza o dei diritti fondamentali non sussistono rischi per quanto riguarda i certificati oggetto di sospensione o limitazione e l'autorità di notifica ha predisposto un calendario di azioni al fine di porre rimedio alla sospensione o alla limitazione; oppure

b) l'autorità di notifica ha confermato che durante il periodo di sospensione o di limitazione non saranno rilasciati, modificati o rinnovati certificati attinenti alla sospensione e indica se l'organismo notificato è in grado di continuare a svolgere il monitoraggio e rimanere responsabile dei certificati esistenti rilasciati durante il periodo della sospensione o della limitazione; nel caso in cui l'autorità di notifica stabilisca che l'organismo notificato non è in grado di sostenere i certificati in vigore, il fornitore del sistema coperto dal certificato conferma per iscritto alle autorità nazionali competenti dello Stato membro in cui ha la propria sede, entro tre mesi dalla sospensione o dalla limitazione, che un altro organismo notificato qualificato assume temporaneamente le funzioni dell'organismo notificato di svolgere il monitoraggio e assume la responsabilità dei certificati durante il periodo di sospensione o limitazione.

9. Ad eccezione dei certificati rilasciati indebitamente, e ove la designazione sia stata ritirata, i certificati restano validi per un periodo di nove mesi nei casi seguenti:

a) l'autorità nazionale competente dello Stato membro in cui il fornitore del sistema di IA ad alto rischio coperto dal certificato ha la propria sede ha confermato che sotto il profilo della salute, della sicurezza o dei diritti fondamentali non sussistono rischi per quanto riguarda i sistemi di IA ad alto rischio interessati; e

b) un altro organismo notificato ha confermato per iscritto che assume immediatamente la responsabilità per tali sistemi di IA e completa la sua valutazione entro 12 mesi dal ritiro della designazione.

Nei casi di cui al primo comma, l'autorità nazionale competente dello Stato membro in cui il fornitore del sistema coperto dal certificato ha la propria sede può prorogare la validità temporanea dei certificati di ulteriori periodi di tre mesi, per un totale non superiore a dodici mesi.

L'autorità nazionale competente o l'organismo notificato che assume le funzioni dell'organismo notificato interessato dalla modifica della designazione informa immediatamente la Commissione, gli altri Stati membri e gli altri organismi notificati.

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 competenza di un organismo notificato o della continuità dell'ottemperanza di un organismo notificato ai requisiti di cui all'articolo 31 e alle sue responsabilità applicabili.

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

3. La Commissione provvede affinché tutte le informazioni sensibili ottenute nel corso delle sue indagini a norma del presente articolo siano trattate in maniera riservata in conformità dell'articolo 78.

4. La Commissione, qualora accerti che un organismo notificato non soddisfa, o non soddisfa più, i requisiti per la sua notifica, informa di conseguenza lo Stato membro notificante e gli chiede di adottare le misure correttive necessarie compresa la sospensione o il ritiro della notifica. Se lo Stato membro non adotta le misure correttive necessarie, la Commissione può, mediante atto di esecuzione, sospendere, limitare o ritirare la designazione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Articolo 38

Coordinamento degli organismi notificati

1. La Commissione garantisce che, per quanto riguarda i sistemi di IA ad alto rischio, siano istituiti e funzionino correttamente, in forma di gruppo settoriale di organismi notificati, un coordinamento e una cooperazione adeguati tra gli organismi notificati che partecipano alle procedure di valutazione della conformità a norma del presente regolamento.

2. Ciascuna autorità di notifica garantisce che gli organismi da essa notificati partecipino al lavoro di un gruppo di cui al paragrafo 1, direttamente o mediante rappresentanti designati.

3. La Commissione provvede allo scambio di conoscenze e migliori pratiche tra le autorità di notifica.

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, a condizione che soddisfino i requisiti stabiliti all'articolo 31 o garantiscano un livello di conformità equivalente.

SEZIONE 5

Norme, valutazione della conformità, certificati, registrazione

Articolo 40

Norme armonizzate e prodotti della normazione

1. I sistemi di IA ad alto rischio o i modelli di IA per finalità generali che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n, 1025/2012 si presumono conformi ai requisiti di cui alla sezione 2 del presente capo o, se del caso, agli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento, nella misura in cui tali requisiti o obblighi sono contemplati da tali norme.

2. In conformità dell'articolo 10 del regolamento (UE) n, 1025/2012, la Commissione presenta senza indebito ritardo richieste di normazione riguardanti tutti i requisiti di cui alla sezione 2 del presente capo e, se del caso, richieste di normazione riguardanti gli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento. La richiesta di normazione chiede inoltre prodotti relativi a processi di comunicazione e documentazione intesi a migliorare le prestazioni dei sistemi di IA in termini di risorse, come la riduzione del consumo di energia e di altre risorse del sistema di IA ad alto rischio durante il suo ciclo di vita, e allo sviluppo efficiente sotto il profilo energetico dei modelli di IA per finalità generali. Nel preparare una richiesta di normazione, la Commissione consulta il consiglio per l'IA e i pertinenti portatori di interessi, compreso il forum consultivo.

Nel presentare una richiesta di normazione alle organizzazioni europee di normazione, la Commissione specifica che le norme devono essere chiare, coerenti, anche con le norme elaborate nei vari settori per i prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione elencata nell'allegato I, e volte a garantire che i sistemi di IA ad alto rischio o i modelli di IA per finalità generali immessi sul mercato o messi in servizio nell'Unione soddisfino i pertinenti requisiti od obblighi di cui al presente regolamento.

La Commissione chiede alle organizzazioni europee di normazione di dimostrare che si adoperano al massimo per conseguire gli obiettivi di cui al primo e al secondo comma del presente paragrafo conformemente all'articolo 24 del regolamento (UE) n, 1025/2012.

3. I partecipanti al processo di normazione cercano di promuovere gli investimenti e l'innovazione nell'IA, anche mediante una maggiore certezza del diritto, nonché la competitività e la crescita del mercato dell'Unione, di contribuire a rafforzare la cooperazione globale in materia di normazione e a tener conto delle norme internazionali esistenti nel settore dell'IA che sono coerenti con i valori, i diritti fondamentali e gli interessi dell'Unione, e di rafforzare la governance multipartecipativa garantendo una rappresentanza equilibrata degli interessi e l'effettiva partecipazione di tutti i portatori di interessi pertinenti conformemente agli articoli 5, 6 e 7 del regolamento (UE) n, 1025/2012.

Articolo 41

Specifiche comuni

1. La Commissione può adottare atti di esecuzione che stabiliscano specifiche comuni per i requisiti di cui alla sezione 2 del presente capo o, se del caso, per gli obblighi di cui al capo V, sezioni 2 e 3, se sono soddisfatte le condizioni seguenti:

a) a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n, 1025/2012, la Commissione ha chiesto a una o più organizzazioni europee di normazione di elaborare una norma armonizzata per i requisiti di cui alla sezione 2 del presente capo, o ove applicabile, per gli obblighi di cui al capo V, sezioni 2 e 3, e:

   i) la richiesta non è stata accettata da nessuna delle organizzazioni europee di normazione; o

ii) le norme armonizzate relative a tale richiesta non vengono presentate entro il termine fissato a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n, 1025/2012; o

iii) le pertinenti norme armonizzate non tengono sufficientemente conto delle preoccupazioni in materia di diritti fondamentali; o

iv) le norme armonizzate non sono conformi alla richiesta; e

b) nessun riferimento a norme armonizzate, che contemplino i requisiti di cui alla sezione 2 del presente capo o, ove applicabile, gli obblighi di cui al capo V, sezioni 2 e 3, è stato pubblicato nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n, 1025/2012 e non si prevede che un tale riferimento sia pubblicato entro un termine ragionevole.

Nel redigere le specifiche comuni, la Commissione consulta il forum consultivo di cui all'articolo 67.

Gli atti di esecuzione di cui al primo comma sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

2. Prima di preparare un progetto di atto di esecuzione, la Commissione informa il comitato di cui all'articolo 22 del regolamento (UE) n, 1025/2012 del fatto che ritiene soddisfatte le condizioni di cui al paragrafo 1 del presente articolo.

3. I sistemi di IA ad alto rischio o i modelli di IA per finalità generali conformi alle specifiche comuni di cui al paragrafo 1, o a parti di tali specifiche, si presumono conformi ai requisiti di cui alla sezione 2 del presente capo o, ove applicabile, agli obblighi di cui al capo V, sezioni 2 e 3 nella misura in cui tali requisiti o tali obblighi sono contemplati da tali specifiche comuni.

4. Qualora una norma armonizzata sia adottata da un organismo europeo di normazione e proposta alla Commissione per la pubblicazione del suo riferimento nella *Gazzetta ufficiale dell'Unione europea*, la Commissione valuta la norma armonizzata conformemente al regolamento (UE) n, 1025/2012. Quando un riferimento a una norma armonizzata è pubblicato nella *Gazzetta ufficiale dell'Unione europea*, la Commissione abroga gli atti di esecuzione di cui al paragrafo 1 o le parti di tali atti che riguardano gli stessi requisiti di cui alla sezione 2 del presente capo o, ove applicabile, gli obblighi di cui al capo V, sezioni 2 e 3.

5. Qualora non rispettino le specifiche comuni di cui al paragrafo 1, i fornitori di sistemi di IA ad alto rischio o di modelli di IA per finalità generali adottano soluzioni tecniche debitamente motivate che soddisfano i requisiti di cui alla sezione 2 del presente capo o, ove applicabile, gli obblighi di cui al capo V, sezioni 2 e 3, a un livello almeno equivalente.

6. Se uno Stato membro ritiene che una specifica comune non soddisfi interamente i requisiti di cui alla sezione 2 o, ove applicabile, non rispetti gli obblighi di cui al capo V, sezioni 2 e 3, ne informa la Commissione fornendo una spiegazione dettagliata. La Commissione valuta tali informazioni e, ove necessario, modifica l'atto di esecuzione che stabilisce la specifica comune interessata.

Articolo 42

Presunzione di conformità a determinati requisiti

1. I sistemi di IA ad alto rischio che sono stati addestrati e sottoposti a prova con dati che rispecchiano il contesto geografico, comportamentale, contestuale o funzionale specifico all'interno del quale sono destinati a essere usati si presumono conformi ai pertinenti requisiti 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 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 alla sezione 2, il fornitore sceglie una delle seguenti procedure di valutazione della conformità basate sugli elementi qui di seguito:

a) il controllo interno di cui all'allegato VI; oppure

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

Nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, il fornitore segue la procedura di valutazione della conformità di cui all'allegato VII se:

a) non esistono le norme armonizzate di cui all'articolo 40 e non sono disponibili le specifiche comuni di cui all'articolo 41;

b) il fornitore non ha applicato la norma armonizzata o ne ha applicato solo una parte;

c) esistono le specifiche comuni di cui alla lettera a), ma il fornitore non le ha applicate;

d) una o più norme armonizzate di cui alla lettera a) sono state pubblicate con una limitazione e soltanto sulla parte della norma che è oggetto di limitazione.

Ai fini della procedura di valutazione della conformità di cui all'allegato VII, il fornitore può scegliere uno qualsiasi degli organismi notificati. Tuttavia, se il sistema di IA ad alto rischio è destinato ad essere messo in servizio dalle autorità competenti in materia di contrasto, di immigrazione o di asilo, nonché da istituzioni, organi o organismi dell'Unione, l'autorità di vigilanza del mercato di cui all'articolo 74, paragrafo 8 o 9, a seconda dei casi, agisce in qualità di organismo notificato.

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.

3. Per i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fornitore segue la pertinente procedura di valutazione della conformità prevista da tali atti giuridici. I requisiti di cui alla sezione 2 del presente capo 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 alla sezione 2, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 31, paragrafi 4, 10 e 11, sia stata valutata nel contesto della procedura di notifica a norma di tali atti giuridici.

Qualora un atto giuridico elencato nell'allegato I, sezione A, consenta 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 tutti i requisiti di cui alla sezione 2 del presente capo.

4. I sistemi di IA ad alto rischio che sono già stati oggetto di una procedura di valutazione della conformità sono sottoposti a una nuova procedura di valutazione della conformità nel caso di una modifica sostanziale, indipendentemente dal fatto che il sistema modificato sia destinato a essere ulteriormente distribuito o continui a essere usato dal deployer 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 97 al fine di modificare gli allegati VI e VII aggiornandoli alla luce del progresso tecnico.

6. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 che modificano i paragrafi 1 e 2 del presente articolo 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 lingua che può essere facilmente compresa dalle autorità pertinenti dello Stato membro in cui è stabilito l'organismo notificato.

2. I certificati sono validi per il periodo da essi indicato che non supera i cinque anni per i sistemi di IA disciplinati dall'allegato I e i quattro anni per i sistemi di IA disciplinati dall'allegato III. Su domanda del fornitore, la validità di un certificato può essere prorogata per ulteriori periodi, ciascuno non superiore a cinque anni per i sistemi di IA disciplinati dall'allegato I e a quattro anni per i sistemi di IA disciplinati dall'allegato III, sulla base di una nuova valutazione secondo le procedure di valutazione della conformità applicabili. Ogni supplemento del certificato rimane valido purché sia valido il certificato cui si riferisce.

3. Qualora constati che il sistema di IA non soddisfa più i requisiti di cui alla sezione 2, 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.

È disponibile una procedura di ricorso contro le decisioni degli organismi notificati, anche sui certificati di conformità rilasciati.

Articolo 45

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 dei 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 dei requisiti dell'allegato VII;

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

d) qualsiasi richiesta di informazioni che abbiano 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'Unione 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 gli stessi tipi di sistemi di IA informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, positivi della valutazione della conformità.

4. Gli organismi notificati tutelano la riservatezza delle informazioni che ottengono in conformità dell'articolo 78.

Articolo 46

Deroga alla procedura di valutazione della conformità

1. In deroga all'articolo 43 e su richiesta debitamente giustificata, 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 o dei principali beni industriali e infrastrutturali. Tale autorizzazione è valida per un periodo limitato, mentre sono in corso le necessarie procedure di valutazione della conformità, tenendo conto dei motivi eccezionali che giustificano la deroga. Il completamento di tali procedure è effettuato senza indebito ritardo.

2. In una situazione di urgenza debitamente giustificata per motivi eccezionali di sicurezza pubblica o in caso di minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche, le autorità di contrasto o le autorità di protezione civile possono mettere in servizio uno specifico sistema di IA ad alto rischio senza l'autorizzazione di cui al paragrafo 1, a condizione che tale autorizzazione sia richiesta durante o dopo l'uso senza indebito ritardo. Se l'autorizzazione di cui al paragrafo 1 è rifiutata, l'uso del sistema di IA ad alto rischio è interrotto con effetto immediato e tutti i risultati e gli output di tale uso sono immediatamente eliminati.

3. 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 alla sezione 2. L'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri di eventuali autorizzazioni rilasciate a norma dei paragrafi 1 e 2. Tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità di contrasto.

4. Se, entro 15 giorni di calendario dal ricevimento dell'informazione di cui al paragrafo 3, 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 del paragrafo 1, tale autorizzazione è considerata giustificata.

5. Se, entro 15 giorni di calendario dal ricevimento della notifica di cui al paragrafo 3, 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 3 sia infondata, la Commissione avvia senza ritardo consultazioni con lo Stato membro interessato. Gli operatori interessati sono consultati e hanno la possibilità di esprimere il loro parere. Tenuto conto di ciò, la Commissione decide se l'autorizzazione è giustificata. La Commissione trasmette la propria decisione allo Stato membro interessato e agli operatori pertinenti.

6. Se la Commissione ritiene l'autorizzazione ingiustificata, essa è ritirata dall'autorità di vigilanza del mercato dello Stato membro interessato.

7. Per i sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, si applicano solo le deroghe alla valutazione della conformità stabilite in tale normativa di armonizzazione dell'Unione.

Articolo 47

Dichiarazione di conformità UE

1. Il fornitore compila una dichiarazione scritta di conformità UE leggibile meccanicamente, firmata a mano o elettronicamente, per ciascun sistema di IA ad alto rischio e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio. La dichiarazione di conformità UE identifica il sistema di IA ad alto rischio per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è presentata alle pertinenti autorità nazionali competenti.

2. La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio interessato soddisfa i requisiti di cui alla sezione 2. La dichiarazione di conformità UE riporta le informazioni di cui all'allegato V ed è tradotta in una lingua che può essere facilmente compresa dalle autorità nazionali competenti degli Stati membri nei quali il sistema di IA ad alto rischio è immesso sul mercato o messo a disposizione.

3. Qualora i sistemi di IA ad alto rischio siano soggetti ad altra normativa di armonizzazione dell'Unione che richieda anch'essa 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 alla sezione 2. Il fornitore tiene opportunamente aggiornata la dichiarazione di conformità UE.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato V aggiornando il contenuto della dichiarazione di conformità UE di cui a tale allegato per introdurre elementi che si rendano necessari alla luce del progresso tecnico.

Articolo 48

Marcatura CE

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

2. Per i sistemi di IA ad alto rischio forniti digitalmente è utilizzata una marcatura CE digitale soltanto se è facilmente accessibile attraverso l'interfaccia da cui si accede a tale sistema o tramite un codice leggibile meccanicamente o altri mezzi elettronici facilmente accessibili.

3. 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.

4. 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 di identificazione dell'organismo notificato è apposto dall'organismo stesso o, in base alle istruzioni di quest'ultimo, dal fornitore o dal rappresentante autorizzato del fornitore. 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.

5. Se i sistemi di IA ad alto rischio sono disciplinati da altre disposizioni del diritto dell'Unione che prevedono anch'esse l'apposizione della marcatura CE, quest'ultima indica che i sistemi di IA ad alto rischio soddisfano anche i requisiti delle altre normative in questione.

Articolo 49

Registrazione

1. Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, il fornitore o, ove applicabile, il rappresentante autorizzato si registra e registra il suo sistema nella banca dati dell'UE di cui all'articolo 71.

2. Prima di immettere sul mercato o mettere in servizio un sistema di IA che il fornitore ha concluso non essere ad alto rischio a norma dell'articolo 6, paragrafo 3, il fornitore o, ove applicabile, il rappresentante autorizzato si registra o registra tale sistema nella banca dati dell'UE di cui all'articolo 71.

3. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio elencati nel punto 2 dell'allegato III, i deployer che sono autorità pubbliche, istituzioni, organi e organismi dell'Unione o persone che agiscono per loro conto si registrano, selezionano il sistema e ne registrano l'uso nella banca dati dell'UE di cui all'articolo 71.

4. Per i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, la registrazione di cui ai paragrafi 1, 2 e 3 del presente articolo si trova in una sezione sicura non pubblica della banca dati dell'UE di cui all'articolo 71 e comprende, a seconda dei casi, solo le informazioni seguenti di cui:

a) all'allegato VIII, sezione A, punti da 1 a 5 e punti 8 e 9;

b) all'allegato VIII, sezione B, punti da 1 a 5 e punti 8 e 9;

c) all'allegato VIII, sezione C, punti da 1 a 3;

d) all'allegato IX, punti 1, 2, 3 e 5.

Solo la Commissione e le autorità nazionali di cui all'articolo 74, paragrafo 8, hanno accesso alle rispettive sezioni riservate della banca dati dell'UE elencate al primo comma del presente paragrafo.

5. I sistemi di IA ad alto rischio di cui all'allegato III, punto 2, sono registrati a livello nazionale.

CAPO IV

OBBLIGHI DI TRASPARENZA PER I FORNITORI E I DEPLOYER DI DETERMINATI SISTEMI DI IA

Articolo 50

Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA

1. I fornitori garantiscono che i sistemi di IA destinati a interagire direttamente con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

2. I fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, garantiscono che gli output del sistema di IA siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente. I fornitori garantiscono che le loro soluzioni tecniche siano efficaci, interoperabili, solide e affidabili nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle specificità e dei limiti dei vari tipi di contenuti, dei costi di attuazione e dello stato dell'arte generalmente riconosciuto, come eventualmente indicato nelle pertinenti norme tecniche. Tale obbligo non si applica se i sistemi di IA svolgono una funzione di assistenza per l'editing standard o non modificano in modo sostanziale i dati di input forniti dal deployer o la rispettiva semantica, o se autorizzati dalla legge ad accertare, prevenire, indagare o perseguire reati.

3. I deployer 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 e trattano i dati personali in conformità dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680, a seconda dei casi. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica e il riconoscimento delle emozioni autorizzati dalla legge per accertare, prevenire o indagare reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi e conformemente al diritto dell'Unione.

4. I deployer di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un «deep fake» rendono noto che il contenuto è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati. Qualora il contenuto faccia parte di un'analoga opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera.

I deployer di un sistema di IA che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati o se il contenuto generato dall'IA è stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.

5. Le informazioni di cui ai paragrafi da 1 a 4 sono fornite alle persone fisiche interessate in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione. Le informazioni devono essere conformi ai requisiti di accessibilità applicabili.

6. I paragrafi da 1 a 4 lasciano impregiudicati i requisiti e gli obblighi di cui al capo III, così come gli altri obblighi di trasparenza stabiliti dal diritto dell'Unione o nazionale per i deployer dei sistemi di IA.

7. L'ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei contenuti generati o manipolati artificialmente. La Commissione può adottare atti di esecuzione per approvare tali codici di buone pratiche secondo la procedura di cui all'articolo 56, paragrafo 6. Se ritiene che il codice non sia adeguato, la Commissione può adottare un atto di esecuzione che specifichi norme comuni per l'attuazione di tali obblighi secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

CAPO V

MODELLI DI IA PER FINALITÀ GENERALI

SEZIONE 1

Regole di classificazione

Articolo 51

Classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischio sistemico

1. Un modello di IA per finalità generali è classificato come modello di IA per finalità generali con rischio sistemico se soddisfa una delle condizioni seguenti:

a) presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento;

b) sulla base di una decisione della Commissione, *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XIII.

2. Si presume che un modello di IA per finalità generali abbia capacità di impatto elevato a norma del paragrafo 1, lettera a), quando la quantità cumulativa di calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 10^{25}.

3. La Commissione adotta atti delegati a norma dell'articolo 97 per modificare le soglie di cui ai paragrafi 1 e 2 del presente articolo, nonché per integrare parametri di riferimento e indicatori alla luce degli sviluppi tecnologici in evoluzione, quali miglioramenti algoritmici o una maggiore efficienza dell'hardware, ove necessario, affinché tali soglie riflettano lo stato dell'arte.

Articolo 52

Procedura

1. Se un modello di IA per finalità generali soddisfa la condizione di cui all'articolo 51, paragrafo 1, lettera a), il fornitore pertinente informa la Commissione senza ritardo e in ogni caso entro due settimane dal soddisfacimento di tale requisito o dal momento in cui viene a conoscenza che tale requisito sarà soddisfatto. Tale notifica comprende le informazioni necessarie a dimostrare che il requisito in questione è stato soddisfatto. Se la Commissione viene a conoscenza di un modello di IA per finalità generali che presenta rischi sistemici di cui non è stata informata, può decidere di designarlo come modello con rischio sistemico.

2. Il fornitore di un modello di IA per finalità generali che soddisfa la condizione di cui all'articolo 51, paragrafo 1, lettera a), può presentare, unitamente alla sua notifica, argomentazioni sufficientemente fondate per dimostrare che, in via eccezionale, sebbene soddisfi tale requisito, il modello di IA per finalità generali non presenta, a causa delle sue caratteristiche specifiche, rischi sistemici e non dovrebbe essere pertanto classificato come modello di IA per finalità generali con rischio sistemico.

3. Se la Commissione conclude che le argomentazioni presentate a norma del paragrafo 2 non sono sufficientemente fondate e il fornitore in questione non è stato in grado di dimostrare che il modello di IA per finalità generali non presenta, per le sue caratteristiche specifiche, rischi sistemici, essa respinge tali argomentazioni e il modello di IA per finalità generali è considerato un modello di IA per finalità generali con rischio sistemico.

4. La Commissione può designare un modello di IA per finalità generali come modello che presenta rischi sistemici, *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici a norma dell'articolo 90, paragrafo 1, lettera a), sulla base dei criteri di cui all'allegato XIII.

Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 97 per modificare l'allegato XIII specificando e aggiornando i criteri di cui a tale allegato.

5. Su richiesta motivata di un fornitore il cui modello è stato designato come modello di IA per finalità generali con rischio sistemico a norma del paragrafo 4, la Commissione, tenendo conto della richiesta, può decidere di valutare nuovamente se si possa ancora ritenere che il modello di IA per finalità generali presenti rischi sistemici sulla base dei criteri di cui all'allegato XIII. Tale richiesta contiene motivi oggettivi, dettagliati e nuovi emersi dopo la decisione di designazione. I fornitori possono chiedere una nuova valutazione non prima di sei mesi dopo la decisione di designazione. Se la Commissione, a seguito della nuova valutazione, decide di mantenere la designazione come modello di IA per finalità generali con rischio sistemico, i fornitori possono chiedere una nuova valutazione non prima di sei mesi dopo tale decisione.

6. La Commissione garantisce che sia pubblicato un elenco di modelli di IA per finalità generali con rischio sistemico e lo mantiene aggiornato, fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale.

SEZIONE 2

Obblighi dei fornitori di modelli di IA per finalità generali

Articolo 53

Obblighi dei fornitori di modelli di IA per finalità generali

1. I fornitori di modelli di IA per finalità generali:

a) redigono e mantengono aggiornata la documentazione tecnica del modello, compresi il processo di addestramento e prova e i risultati della sua valutazione, che contiene almeno le informazioni di cui all'allegato XI affinché possa essere trasmessa, su richiesta, all'ufficio per l'IA e alle autorità nazionali competenti;

b) elaborano, mantengono aggiornate e mettono a disposizione informazioni e documentazione per i fornitori di sistemi di IA che intendono integrare il modello di IA per finalità generali nei loro sistemi di IA. Fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale, le informazioni e la documentazione:

   i) consentono ai fornitori di sistemi di IA di avere una buona comprensione delle capacità e dei limiti del modello di IA per finalità generali e di adempiere ai loro obblighi a norma del presente regolamento; nonché

   ii) contengono almeno gli elementi di cui all'allegato XII;

c) attuano una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e diritti ad esso collegati e, in particolare, a individuare e rispettare, anche attraverso tecnologie all'avanguardia, una riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790;

d) redigono e mettono a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali, secondo un modello fornito dall'ufficio per l'IA.

2. Gli obblighi di cui al paragrafo 1, lettere a) e b), non si applicano ai fornitori di modelli di IA rilasciati con licenza libera e open source che consentono l'accesso, l'uso, la modifica e la distribuzione del modello e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici. Tale eccezione non si applica ai modelli di IA per finalità generali con rischi sistemici.

3. I fornitori di modelli di IA per finalità generali collaborano, secondo necessità, con la Commissione e le autorità nazionali competenti nell'esercizio delle loro competenze e dei loro poteri a norma del presente regolamento.

4. I fornitori di modelli di IA per finalità generali possono basarsi su codici di buone pratiche ai sensi dell'articolo 56 per dimostrare la conformità agli obblighi di cui al paragrafo 1 del presente articolo, finché non è pubblicata una norma armonizzata. La conformità alle norme armonizzate europee garantisce ai fornitori la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi. I fornitori di modelli di IA per finalità generali che non aderiscono a un codice di buone pratiche approvato dimostrano mezzi alternativi adeguati di conformità ai fini di approvazione da parte della Commissione.

5. Allo scopo di agevolare la conformità all'allegato XI, in particolare al punto 2, lettere d) ed e), alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 97 per specificare le metodologie di misurazione e di calcolo al fine di consentire che la documentazione sia comparabile e verificabile.

6. Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 97, paragrafo 2, per modificare gli allegati XI e XII alla luce degli sviluppi tecnologici in evoluzione.

7. Le informazioni o la documentazione ottenute a norma del presente articolo, compresi i segreti commerciali, sono trattate in conformità degli obblighi di riservatezza di cui all'articolo 78.

Articolo 54

Rappresentanti autorizzati dei fornitori di modelli di IA per finalità generali

1. Prima di immettere sul mercato dell'Unione un modello di IA per finalità generali, i fornitori stabiliti in paesi terzi nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

2. Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore.

3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fornitore. Fornisce una copia del mandato all'ufficio per l'IA, su richiesta, in una delle lingue ufficiali delle istituzioni dell'Unione. Ai fini del presente regolamento, il mandato consente al rappresentante autorizzato di eseguire i compiti seguenti:

a) verificare che la documentazione tecnica di cui all'allegato XI sia stata redatta e che tutti gli obblighi di cui all'articolo 53 e, se del caso, all'articolo 55 siano stati adempiuti dal fornitore;

b) tenere a disposizione dell'ufficio per l'IA e delle autorità nazionali competenti una copia della documentazione tecnica di cui all'allegato XI per un periodo di 10 anni dalla data in cui il modello di IA per finalità generali è stato immesso sul mercato e i dati di contatto del fornitore che ha nominato il rappresentante autorizzato;

c) fornire all'ufficio per l'IA, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui alla lettera b), necessarie per dimostrare la conformità agli obblighi di cui al presente capo;

d) cooperare con l'ufficio per l'IA e le autorità competenti, su richiesta motivata, in qualsiasi azione intrapresa da queste ultime in relazione al modello di IA per finalità generali, anche quando il modello è integrato nei sistemi di IA immessi sul mercato o messi in servizio nell'Unione.

4. Il mandato consente al rappresentante autorizzato di essere interlocutore, in aggiunta o in sostituzione del fornitore, nei confronti dell'ufficio per l'IA o delle autorità competenti per tutte le questioni relative al rispetto del presente regolamento.

5. Il rappresentante autorizzato pone fine al mandato se ritiene o ha motivi di ritenere che il fornitore agisca in contrasto con i propri obblighi a norma del presente regolamento. In tal caso, comunica immediatamente anche all'ufficio per l'IA la cessazione del mandato e i relativi motivi.

6. L'obbligo di cui al presente articolo non si applica ai fornitori di modelli di IA per finalità generali rilasciati con licenza libera e open source che consentono l'accesso, l'uso, la modifica e la distribuzione del modello e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici, tranne nel caso in cui i modelli di IA per finalità generali presentino rischi sistemici.

SEZIONE 3

Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico

Articolo 55

Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico

1. In aggiunta agli obblighi di cui agli articoli 53 e 54, i fornitori di modelli di IA per finalità generali con rischio sistemico:

a) effettuano una valutazione dei modelli in conformità di protocolli e strumenti standardizzati che rispecchino lo stato dell'arte, anche svolgendo e documentando il test contraddittorio (adversarial testing) del modello al fine di individuare e attenuare i rischi sistemici;

b) valutano e attenuano i possibili rischi sistemici a livello dell'Unione, comprese le loro fonti, che possono derivare dallo sviluppo, dall'immissione sul mercato o dall'uso di modelli di IA per finalità generali con rischio sistemico;

c) tengono traccia, documentano e riferiscono senza indebito ritardo all'ufficio per l'IA e, se del caso, alle autorità nazionali competenti, le informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio;

d) garantiscono un livello adeguato di protezione della cibersicurezza per quanto riguarda il modello di IA per finalità generali con rischio sistemico e l'infrastruttura fisica del modello.

2. I fornitori di modelli di IA per finalità generali con rischio sistemico possono basarsi su codici di buone pratiche ai sensi dell'articolo 56 per dimostrare la conformità agli obblighi di cui al paragrafo 1 del presente articolo, fino alla pubblicazione di una norma armonizzata. La conformità alle norme armonizzate europee garantisce ai fornitori la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi. I fornitori di modelli di IA per finalità generali con rischi sistemici che non aderiscono a un codice di buone pratiche approvato o che non si conformano alle norme armonizzate europee devono dimostrare mezzi alternativi adeguati di conformità ai fini della valutazione da parte della Commissione.

3. Le informazioni o la documentazione ottenute a norma del presente articolo, compresi i segreti commerciali, sono trattate in conformità degli obblighi di riservatezza di cui all'articolo 78.

SEZIONE 4

Codici di buone pratiche

Articolo 56

Codici di buone pratiche

1. L'ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione al fine di contribuire alla corretta applicazione del presente regolamento, tenendo conto degli approcci internazionali.

2. L'ufficio per l'IA e il comitato mirano a garantire che i codici di buone pratiche contemplino almeno gli obblighi di cui agli articoli 53 e 55, compreso quanto segue:

a) i mezzi per garantire che le informazioni di cui all'articolo 53, paragrafo 1, lettere a) e b), siano mantenute aggiornate alla luce degli sviluppi tecnologici e di mercato;

b) un adeguato livello di dettaglio nella sintesi dei contenuti utilizzati per l'addestramento;

c) l'individuazione del tipo e della natura dei rischi sistemici a livello dell'Unione, comprese le rispettive fonti, se del caso;

d) le misure, le procedure e le modalità per la valutazione e la gestione dei rischi sistemici a livello dell'Unione, compresa la relativa documentazione, che devono essere proporzionate ai rischi e tenere conto della loro gravità e probabilità e delle sfide specifiche nell'affrontare tali rischi alla luce dei modi possibili in cui tali rischi possono emergere e concretizzarsi lungo la catena del valore dell'IA.

3. L'ufficio per l'IA può invitare tutti i fornitori di modelli di IA per finalità generali, nonché le pertinenti autorità nazionali competenti, a partecipare all'elaborazione dei codici di buone pratiche. Le organizzazioni della società civile, l'industria, il mondo accademico e altri pertinenti portatori di interessi, quali i fornitori a valle e gli esperti indipendenti, possono sostenere il processo.

4. L'ufficio per l'IA e il comitato mirano a garantire che i codici di buone pratiche definiscano chiaramente i loro obiettivi specifici e contengano impegni o misure, compresi, se del caso, indicatori chiave di prestazione, volti ad assicurare il conseguimento di tali obiettivi e che tengano debitamente conto delle esigenze e degli interessi di tutte le parti interessate, anche delle persone interessate, a livello dell'Unione.

5. L'ufficio per l'IA mira a garantire che i partecipanti all'elaborazione dei codici di buone pratiche riferiscano periodicamente all'ufficio per l'IA in merito all'attuazione degli impegni, alle misure adottate e ai loro esiti, anche rispetto agli indicatori chiave di prestazione, se del caso. Gli indicatori chiave di prestazione e gli impegni di comunicazione riflettono le differenze in termini di dimensioni e capacità tra i vari partecipanti.

6. L'ufficio per l'IA e il comitato monitorano e valutano periodicamente il conseguimento degli obiettivi dei codici di buone pratiche da parte dei partecipanti e il loro contributo alla corretta applicazione del presente regolamento. L'ufficio per l'IA e il comitato valutano se i codici di buone pratiche contemplano gli obblighi di cui agli articoli 53 e 55, 4e monitorano e valutano periodicamente il conseguimento dei loro obiettivi. Essi pubblicano la loro valutazione riguardante l'adeguatezza dei codici di buone pratiche.

La Commissione può approvare, mediante atto di esecuzione, un codice di buone pratiche e conferire ad esso una validità generale all'interno dell'Unione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

7. L'ufficio per l'IA può invitare tutti i fornitori di modelli di IA per finalità generali ad aderire ai codici di buone pratiche. Per i fornitori di modelli di IA per finalità generali che non presentano rischi sistemici, tale adesione può essere limitata agli obblighi di cui all'articolo 53, a meno che essi dichiarino esplicitamente il loro interesse ad aderire al codice nella sua interezza.

8. L'ufficio per l'IA incoraggia e agevola, se del caso, anche il riesame e l'adeguamento dei codici di buone pratiche, in particolare alla luce di norme emergenti. L'ufficio per l'IA fornisce assistenza per quanto riguarda la valutazione delle norme disponibili.

9. I codici di buone pratiche sono pronti al più tardi entro il 2 maggio 2025. L'ufficio per l'IA adotta le misure necessarie, compreso l'invito ai fornitori di cui al paragrafo 7.

Qualora entro il 2 agosto 2025, un codice di buone pratiche non possa essere portato a termine, o qualora l'ufficio per l'IA lo ritenga non adeguato a seguito della valutazione di cui al paragrafo 6 del presente articolo, la Commissione può prevedere, mediante atti di esecuzione, norme comuni per l'attuazione degli obblighi di cui agli articoli 53 e 55, comprese le questioni di cui al paragrafo 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

CAPO VI

MISURE A SOSTEGNO DELL'INNOVAZIONE

Articolo 57

Spazi di sperimentazione normativa per l'IA

1. Gli Stati membri provvedono affinché le loro autorità competenti istituiscano almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sia operativo entro il 2 agosto 2026. Tale spazio di sperimentazione può essere inoltre istituito congiuntamente con le autorità competenti di altri Stati membri. La Commissione può fornire assistenza tecnica, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA.

L'obbligo di cui al primo comma può essere soddisfatto anche partecipando a uno spazio di sperimentazione esistente nella misura in cui tale partecipazione fornisca un livello equivalente di copertura nazionale per gli Stati membri partecipanti.

2. Possono essere altresì istituiti ulteriori spazi di sperimentazione normativa per l'IA a livello regionale o locale, o congiuntamente con le autorità competenti di altri Stati membri.

3. Il Garante europeo della protezione dei dati può inoltre istituire uno spazio di sperimentazione normativa per l'IA per le istituzioni, gli organi e gli organismi dell'Unione e può esercitare i ruoli e i compiti delle autorità nazionali competenti conformemente al presente capo.

4. Gli Stati membri provvedono affinché le autorità competenti di cui ai paragrafi 1 e 2 assegnino risorse sufficienti per conformarsi al presente articolo in maniera efficace e tempestiva. Se del caso, le autorità nazionali competenti cooperano con altre autorità pertinenti e possono consentire il coinvolgimento di altri attori all'interno dell'ecosistema dell'IA. Il presente articolo lascia impregiudicati gli altri spazi di sperimentazione normativa istituiti a norma del diritto dell'Unione o nazionale. Gli Stati membri garantiscono un livello adeguato di cooperazione tra le autorità che controllano tali altri spazi di sperimentazione e le autorità nazionali competenti.

5. Gli spazi di sperimentazione normativa per l'IA istituiti a norma del paragrafo 1 garantiscono un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione 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 dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e l'autorità competente. Tali spazi di sperimentazione possono comprendere prove in condizioni reali soggette a controllo nei medesimi spazi.

6. Le autorità competenti, se del caso, forniscono orientamenti e garantiscono il controllo e il sostegno nell'ambito dello spazio di sperimentazione normativa per l'IA al fine di individuare i rischi, in particolare per quanto riguarda i diritti fondamentali, la salute e la sicurezza, le prove, le misure di attenuazione e la loro efficacia, in relazione agli obblighi e ai requisiti del presente regolamento e, se del caso, di altre disposizioni del diritto dell'Unione e nazionale, la conformità ai quali è soggetta a controllo nell'ambito dello spazio di sperimentazione.

7. Le autorità competenti forniscono ai fornitori e ai potenziali fornitori che partecipano allo spazio di sperimentazione normativa per l'IA orientamenti sulle aspettative normative e sulle modalità per soddisfare i requisiti e gli obblighi di cui al presente regolamento.

Su richiesta del fornitore o del potenziale fornitore del sistema di IA, l'autorità competente fornisce una prova scritta delle attività svolte con successo nello spazio di sperimentazione. L'autorità competente fornisce inoltre una relazione di uscita che illustra in dettaglio le attività svolte nello spazio di sperimentazione e i relativi risultati e le conclusioni dell'apprendimento. I fornitori possono utilizzare tale documentazione per dimostrare la loro conformità al presente regolamento attraverso la procedura di valutazione della conformità o le pertinenti attività di vigilanza del mercato. A tale riguardo, la relazione di uscita e la prova scritta fornite dall'autorità nazionale competente sono prese favorevolmente in considerazione dalle autorità di vigilanza del mercato e dagli organismi notificati, al fine di accelerare le procedure di valutazione della conformità in misura ragionevole.

8. Fatte salve le disposizioni in materia di riservatezza di cui all'articolo 78, e con l'accordo del fornitore o del potenziale fornitore, la Commissione e il comitato sono autorizzati ad accedere alle relazioni di uscita e ne tengono conto, se del caso, nell'esercizio dei loro compiti a norma del presente regolamento. Se sia il fornitore o il potenziale fornitore sia l'autorità nazionale competente acconsentono esplicitamente, la relazione di uscita può essere messa a disposizione del pubblico attraverso la piattaforma unica di informazione di cui al presente articolo.

9. L'istituzione di spazi di sperimentazione normativa per l'IA mira a contribuire agli obiettivi seguenti:

a) migliorare la certezza del diritto al fine di conseguire la conformità normativa al presente regolamento o, se del caso, ad altre applicabili disposizioni di diritto dell'Unione e nazionale;

b) sostenere la condivisione delle migliori pratiche attraverso la cooperazione con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA;

c) promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA;

d) contribuire all'apprendimento normativo basato su dati concreti;

e) agevolare e accelerare l'accesso al mercato dell'Unione per i sistemi di IA, in particolare se forniti dalle PMI, comprese le start-up.

10. Le autorità nazionali competenti 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 o competenti siano associate al funzionamento dello spazio di sperimentazione normativa per l'IA e partecipino al controllo di tali aspetti nei limiti dei rispettivi compiti e poteri.

11. Gli spazi di sperimentazione normativa per l'IA non pregiudicano i poteri correttivi o di controllo delle autorità competenti che controllano gli spazi di sperimentazione, anche a livello regionale o locale. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi di IA comporta adeguate misure di attenuazione. Le autorità nazionali competenti hanno il potere di sospendere, in via temporanea o permanente, il processo di prova o la partecipazione allo spazio di sperimentazione, se non è possibile un'attenuazione efficace, e informano l'ufficio per l'IA di tale decisione. Le autorità nazionali competenti esercitano i loro poteri di controllo entro i limiti del pertinente diritto, utilizzando i loro poteri discrezionali nell'attuazione delle disposizioni giuridiche per quanto riguarda uno specifico progetto di spazio di sperimentazione normativa per l'IA, con l'obiettivo di promuovere l'innovazione nell'IA nell'Unione.

12. I fornitori e i potenziali fornitori partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione. Tuttavia, a condizione che i potenziali fornitori rispettino il piano specifico e i termini e le condizioni di partecipazione e seguano in buona fede gli orientamenti forniti dall'autorità nazionale competente, quest'ultima non infligge alcuna sanzione amministrativa in caso di violazione del presente regolamento. Qualora altre autorità competenti responsabili del diritto dell'Unione e nazionale abbiano partecipato attivamente al controllo del sistema di IA nello spazio di sperimentazione e abbiano fornito orientamenti ai fini della conformità, nessuna sanzione amministrativa pecuniaria è inflitta in relazione a tali disposizioni di diritto.

13. Gli spazi di sperimentazione normativa per l'IA sono progettati e attuati in modo tale da agevolare, se del caso, la cooperazione transfrontaliera tra le autorità nazionali competenti.

14. Le autorità nazionali competenti coordinano le loro attività e cooperano nel quadro del comitato.

15. Le autorità nazionali competenti informano l'ufficio per l'IA e il comitato di uno spazio di sperimentazione e possono chiedere sostegno e orientamenti. L'ufficio per l'IA mette a disposizione del pubblico l'elenco degli spazi di sperimentazione normativa pianificati ed esistenti e lo mantiene aggiornato al fine di incoraggiare una maggiore interazione negli spazi di sperimentazione e nella cooperazione transfrontaliera.

16. Le autorità nazionali competenti presentano relazioni annuali all'ufficio per l'IA e al comitato a decorrere dall'anno successivo all'istituzione dello spazio di sperimentazione normativa per l'IA e successivamente ogni anno fino alla sua cessazione, nonché una relazione definitiva. Tali relazioni contengono informazioni sui progressi e sui risultati dell'attuazione di tali spazi di sperimentazione, comprese le migliori pratiche, gli incidenti, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione ed eventuale revisione del presente regolamento, inclusi i rispettivi atti delegati e di esecuzione, e sull'applicazione di altre disposizioni di diritto dell'Unione soggette a controllo da parte delle autorità competenti nell'ambito dello spazio di sperimentazione. Le autorità nazionali competenti mettono tali relazioni annuali o estratti delle stesse a disposizione del pubblico online. La Commissione tiene conto, se del caso, delle relazioni annuali nell'esercizio dei suoi compiti a norma del presente regolamento.

17. La Commissione sviluppa un'interfaccia unica e dedicata contenente tutte le informazioni pertinenti relative agli spazi di sperimentazione normativa per l'IA per permettere ai portatori di interessi di interagire con gli spazi di sperimentazione normativa per l'IA e di formulare richieste di informazioni presso le autorità competenti e di chiedere orientamenti non vincolanti sulla conformità di prodotti, servizi e modelli aziendali innovativi che integrano le tecnologie di IA, a norma dell'articolo 62, paragrafo 1, lettera c). La Commissione si coordina proattivamente con le autorità nazionali competenti, se del caso.

Articolo 58

Modalità dettagliate e funzionamento degli spazi di sperimentazione normativa per l'IA

1. Onde evitare la frammentazione nell'intera Unione, la Commissione adotta atti di esecuzione che precisano le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa per l'IA. Tali atti di esecuzione comprendono principi comuni sulle questioni seguenti:

a) criteri di ammissibilità e selezione per la partecipazione allo spazio di sperimentazione normativa per l'IA;

b) procedure per la domanda, la partecipazione, il monitoraggio, l'uscita dallo spazio di sperimentazione normativa per l'IA e la sua cessazione, compresi il piano dello spazio di sperimentazione e la relazione di uscita;

c) i termini e le condizioni applicabili ai partecipanti.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

2. Gli atti di esecuzione di cui al paragrafo 1 garantiscono:

a) che gli spazi di sperimentazione normativa per l'IA siano aperti a qualsiasi fornitore o potenziale fornitore richiedente di un sistema di IA che soddisfi criteri di ammissibilità e selezione trasparenti ed equi, e che le autorità nazionali competenti informino i richiedenti della loro decisione entro tre mesi dalla domanda;

b) che gli spazi di sperimentazione normativa consentano un accesso ampio e paritario e tengano il passo con la domanda di partecipazione; i fornitori e i potenziali fornitori possono anche presentare domande in partenariato con gli deployers e con altri terzi interessati;

c) che le modalità dettagliate e le condizioni relative agli spazi di sperimentazione normativa per l'IA sostengano la flessibilità, nella massima misura possibile, affinché le autorità nazionali competenti istituiscano e gestiscano i loro spazi di sperimentazione normativa per l'IA;

d) che l'accesso agli spazi di sperimentazione normativa per l'IA sia gratuito per le PMI, comprese le start-up, fatti salvi i costi straordinari che le autorità nazionali competenti possono recuperare in maniera equa e proporzionata;

e) che i fornitori e i potenziali fornitori siano agevolati, attraverso i risultati dell'apprendimento degli spazi di sperimentazione normativa per l'IA, a conformarsi agli obblighi di valutazione della conformità di cui al presente regolamento e all'applicazione volontaria dei codici di condotta di cui all'articolo 95;

f) che gli spazi di sperimentazione normativa per l'IA facilitino il coinvolgimento di altri attori pertinenti nell'ambito dell'ecosistema dell'IA, quali organismi notificati e organizzazioni di normazione, PMI, comprese start-up, imprese, innovatori, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione e poli europei dell'innovazione digitale, centri di eccellenza e singoli ricercatori, al fine di consentire e facilitare la cooperazione con i settori pubblico e privato;

g) che le procedure, i processi e i requisiti amministrativi per l'applicazione, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione normativa per l'IA siano semplici, facilmente intelligibili, comunicati chiaramente per agevolare la partecipazione delle PMI, comprese le start-up, con capacità giuridiche e amministrative limitate e siano razionalizzati in tutta l'Unione, al fine di evitare la frammentazione e che la partecipazione a uno spazio di sperimentazione normativa per l'IA istituito da uno Stato membro o dal Garante europeo della protezione dei dati sia reciprocamente e uniformemente riconosciuta e produca gli stessi effetti giuridici nell'intera Unione;

h) che la partecipazione allo spazio di sperimentazione normativa per l'IA sia limitata a un periodo adeguato alla complessità e alla portata del progetto, che può essere prorogato dall'autorità nazionale competente;

i) che gli spazi di sperimentazione normativa per l'IA agevolino lo sviluppo di strumenti e infrastrutture per la sperimentazione, l'analisi comparativa, la valutazione e la spiegazione delle dimensioni dei sistemi di IA pertinenti per l'apprendimento normativo, quali l'accuratezza, la robustezza e la cibersicurezza, nonché le misure per attenuare i rischi per i diritti fondamentali e la società in generale.

3. I potenziali fornitori degli spazi di sperimentazione normativa per l'IA, soprattutto le PMI e le start-up, sono indirizzati, se del caso, a servizi di pre-diffusione, quali gli orientamenti sull'attuazione del presente regolamento, ad altri servizi a valore aggiunto, quali l'assistenza per i documenti di normazione e la certificazione, gli impianti di prova e sperimentazione, i poli europei dell'innovazione digitale e i centri di eccellenza.

4. Quando valutano la possibilità di autorizzare prove in condizioni reali sottoposte a controllo nel quadro di uno spazio di sperimentazione normativa per l'IA da istituire a norma del presente articolo, le autorità nazionali competenti concordano in modo specifico con i partecipanti i termini e le condizioni di tali prove e, in particolare, le tutele adeguate al fine di proteggere i diritti fondamentali, la salute e la sicurezza. Se del caso, cooperano con altre autorità nazionali competenti al fine di garantire pratiche coerenti in tutta l'Unione.

Articolo 59

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 possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione quando sono soddisfatte tutte le condizioni seguenti:

a) i sistemi di IA sono sviluppati per salvaguardare un interesse pubblico rilevante da parte di un'autorità pubblica o di un'altra persona fisica o giuridica e in uno o più dei settori seguenti:

   i) la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari;

   ii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente, la tutela della biodiversità, la protezione contro l'inquinamento, le misure per la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi;

   iii) la sostenibilità energetica;

   iv) la sicurezza e la resilienza dei sistemi di trasporto e della mobilità, delle infrastrutture critiche e delle reti;

   v) l'efficienza e la qualità della pubblica amministrazione e dei servizi pubblici;

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

c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del regolamento (UE) 2016/679 e all'articolo 39 del regolamento (UE) 2018/1725 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 del potenziale fornitore e solo le persone autorizzate hanno accesso a tali dati;

e) i fornitori possono condividere ulteriormente i dati originariamente raccolti solo in conformità del diritto dell'Unione in materia di protezione dei dati; i dati personali creati nello spazio di sperimentazione non possono essere condivisi al di fuori dello spazio di sperimentazione;

f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati né incide sull'applicazione dei loro diritti sanciti dal diritto dell'Unione in materia di protezione dei dati personali;

g) i dati personali trattati nell'ambito dello spazio di sperimentazione sono protetti mediante adeguate misure tecniche e organizzative e 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, salvo diversa disposizione del diritto dell'Unione o nazionale;

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; tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo.

2. A fini di prevenzione, indagine, accertamento e perseguimento di reati o 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 di contrasto, il trattamento dei dati personali negli spazi di sperimentazione normativa per l'IA si basa su una specifica disposizione di diritto nazionale o dell'Unione ed è soggetto alle stesse condizioni cumulative di cui al paragrafo 1.

3. Il paragrafo 1 lascia impregiudicate le disposizioni del diritto dell'Unione o nazionale che escludono il trattamento dei dati personali per fini diversi da quelli espressamente menzionati in tali disposizioni, nonché il diritto dell'Unione o nazionale che stabilisce la base per il trattamento dei dati personali necessario ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi o qualsiasi altra base giuridica, conformemente al diritto dell'Unione in materia di protezione dei dati personali.

Articolo 60

Prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

1. Le prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA possono essere effettuate da fornitori o potenziali fornitori di sistemi di IA ad alto rischio elencati nell'allegato III, conformemente al presente articolo e al piano di prova in condizioni reali di cui al presente articolo, fatti salvi i divieti di cui all'articolo 5.

La Commissione, per mezzo di atti di esecuzione, specifica nel dettaglio gli elementi del piano di prova in condizioni reali. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Il presente paragrafo lascia impregiudicato il diritto dell'Unione o nazionale concernente le prove in condizioni reali di sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I.

2. I fornitori o potenziali fornitori possono effettuare prove dei sistemi di IA ad alto rischio di cui all'allegato III in condizioni reali in qualsiasi momento prima dell'immissione sul mercato o della messa in servizio del sistema di IA, da soli o in partenariato con uno o più deployer o potenziali deployer.

3. Le prove di sistemi di IA ad alto rischio in condizioni reali a norma del presente articolo non pregiudicano alcun esame etico che sia richiesto dal diritto dell'Unione o nazionale.

4. I fornitori o potenziali fornitori possono effettuare le prove in condizioni reali solo se sono soddisfatte tutte le condizioni seguenti:

a) il fornitore o potenziale fornitore ha elaborato un piano di prova in condizioni reali e lo ha presentato all'autorità di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali;

b) l'autorità nazionale di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali ha approvato le prove in condizioni reali e il piano di prova in condizioni reali; se l'autorità di vigilanza del mercato non ha fornito una risposta entro 30 giorni, le prove in condizioni reali e il piano di prova in condizioni reali sono da intendersi approvati; se il diritto nazionale non prevede un'approvazione tacita, le prove in condizioni reali restano soggette ad autorizzazione;

c) il fornitore o potenziale fornitore, ad eccezione dei fornitori o dei potenziali fornitori dei sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, e dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, ha registrato la prova in condizioni reali conformemente all'articolo 71, paragrafo 4, con un numero di identificazione unico a livello dell'Unione e con le informazioni di cui all'allegato IX; il fornitore o il potenziale fornitore di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori dell'attività di contrasto, della migrazione, dell'asilo e della gestione del controllo di frontiera, ha registrato la prova in condizioni reali in una sezione sicura non pubblica della banca dati UE ai sensi dell'articolo 49, paragrafo 4, lettera d), con un numero di identificazione unico a livello dell'Unione e con le informazioni ivi specificate; il fornitore o il potenziale fornitore di sistemi di IA ad alto rischio di cui all'allegato III, punto 2, ha registrato la prova in condizioni reali conformemente all'articolo 49, paragrafo 5;

d) il fornitore o potenziale fornitore che effettua le prove in condizioni reali è stabilito nell'Unione o ha nominato un rappresentante legale che è stabilito nell'Unione;

e) i dati raccolti e trattati ai fini delle prove in condizioni reali sono trasferiti a paesi terzi solo a condizione che siano poste in essere tutele adeguate e applicabili ai sensi del diritto dell'Unione;

f) le prove in condizioni reali non durano più di quanto necessario per conseguire i rispettivi obiettivi e, in ogni caso, non più di sei mesi, che possono essere prorogati per un ulteriore periodo di sei mesi, previa notifica da parte del fornitore o del potenziale fornitore all'autorità di vigilanza del mercato, corredata della motivazione relativa alla necessità di tale proroga;

g) i soggetti delle prove in condizioni reali che sono persone appartenenti a gruppi vulnerabili a causa della loro età o disabilità sono adeguatamente protetti;

h) qualora un fornitore o potenziale fornitore organizzi le prove in condizioni reali in cooperazione con uno o più deployer o potenziali deployer, questi ultimi sono stati informati di tutti gli aspetti delle prove pertinenti per la loro decisione di partecipare e hanno ricevuto le istruzioni pertinenti per l'uso del sistema di IA di cui all'articolo 13; il fornitore o potenziale fornitore e il deployer o potenziale deployer concludono un accordo che ne specifica i ruoli e le responsabilità al fine di garantire la conformità alle disposizioni relative alle prove in condizioni reali ai sensi del presente regolamento e di altre disposizioni applicabili di diritto dell'Unione e nazionale;

i) i soggetti delle prove in condizioni reali hanno dato il proprio consenso informato a norma dell'articolo 61 o, nel caso delle attività di contrasto, qualora la richiesta di consenso informato impedisca di sottoporre a prova il sistema di IA, le prove stesse e i risultati delle prove in condizioni reali non hanno alcun effetto negativo sui soggetti e i loro dati personali sono cancellati dopo lo svolgimento della prova;

j) le prove in condizioni reali sono efficacemente supervisionate dal fornitore o potenziale fornitore, nonché dai deployer o dai potenziali deployer, tramite persone adeguatamente qualificate nel settore pertinente e dotate delle capacità, della formazione e dell'autorità necessarie per svolgere i loro compiti;

k) le previsioni, le raccomandazioni o le decisioni del sistema di IA possono essere efficacemente ribaltate e ignorate.

5. Qualsiasi soggetto delle prove in condizioni reali, o il suo rappresentante legale designato, a seconda dei casi, può, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione, ritirarsi dalle prove in qualsiasi momento revocando il proprio consenso informato e può chiedere la cancellazione immediata e permanente dei propri dati personali. La revoca del consenso informato non pregiudica le attività già svolte.

6. A norma dell'articolo 75, gli Stati membri conferiscono alle loro autorità di vigilanza del mercato il potere di imporre ai fornitori e ai potenziali fornitori di fornire informazioni, di effettuare ispezioni a distanza o in loco senza preavviso e di svolgere controlli sulla conduzione delle prove in condizioni reali e sui relativi sistemi di IA ad alto rischio. Le autorità di vigilanza del mercato si avvalgono di tali poteri per garantire lo sviluppo in sicurezza delle prove in condizioni reali.

7. Qualsiasi incidente grave individuato nel corso delle prove in condizioni reali è segnalato all'autorità nazionale di vigilanza del mercato conformemente all'articolo 73. Il fornitore o potenziale fornitore adotta misure di attenuazione immediate o, in mancanza di ciò, sospende le prove in condizioni reali fino a quando tale attenuazione non abbia luogo oppure vi pone fine. Il fornitore o potenziale fornitore stabilisce una procedura per il tempestivo ritiro del sistema di IA in seguito a tale cessazione delle prove in condizioni reali.

8. I fornitori o potenziali fornitori notificano all'autorità nazionale di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali la sospensione o la cessazione delle prove in condizioni reali nonché i risultati finali.

9. Il fornitore o potenziale fornitore è responsabile ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni causati nel corso delle prove in condizioni reali.

Articolo 61

Consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

1. Ai fini delle prove in condizioni reali a norma dell'articolo 60, il consenso informato dato liberamente dai soggetti delle prove è ottenuto prima della loro partecipazione a tali prove e dopo che sono stati debitamente informati con indicazioni concise, chiare, pertinenti e comprensibili riguardanti:

a) la natura e gli obiettivi delle prove in condizioni reali e i possibili disagi che possono essere connessi alla loro partecipazione;

b) le condizioni alle quali devono essere effettuate le prove in condizioni reali, compresa la durata prevista della partecipazione del soggetto o dei soggetti;

c) i loro diritti e le garanzie riconosciute al soggetto in relazione alla loro partecipazione, in particolare il loro diritto di rifiutarsi di partecipare e il diritto di ritirarsi dalle prove in condizioni reali in qualsiasi momento, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione;

d) le modalità per richiedere che le previsioni, raccomandazioni o decisioni del sistema di IA siano ignorate o ribaltate;

e) il numero di identificazione unico a livello dell'Unione delle prove in condizioni reali conformemente all'articolo 60, paragrafo 4, lettera c), e i dati di contatto del fornitore o del suo rappresentante legale da cui è possibile ottenere ulteriori informazioni.

2. Il consenso informato è datato e documentato e una copia è consegnata ai soggetti delle prove o al loro rappresentante legale.

Articolo 62

Misure per i fornitori e i deployer, in particolare le PMI, comprese le start-up

1. Gli Stati membri intraprendono le azioni seguenti:

a) fornire alle PMI, comprese le start-up, con sede legale o una filiale nell'Unione, un accesso prioritario agli spazi di sperimentazione normativa per l'IA nella misura in cui soddisfano le condizioni di ammissibilità e i criteri di selezione; l'accesso prioritario non impedisce ad altre PMI, comprese le start-up, diverse da quelle di cui al presente paragrafo di accedere allo spazio di sperimentazione normativa per l'IA, purché soddisfino anche le condizioni di ammissibilità e i criteri di selezione;

b) organizzare specifiche attività di sensibilizzazione e formazione sull'applicazione del presente regolamento adattate alle esigenze delle PMI, comprese le start-up, dei deployers e, se del caso, delle autorità pubbliche locali;

c) utilizzare i canali dedicati esistenti e, ove opportuno, istituirne di nuovi per la comunicazione con le PMI, comprese le start-up, i deployers, altri innovatori e, se del caso, le autorità pubbliche locali, al fine di fornire consulenza e rispondere alle domande sull'attuazione del presente regolamento, anche per quanto riguarda la partecipazione agli spazi di sperimentazione normativa per l'IA;

d) agevolare la partecipazione delle PMI e di altri portatori di interessi pertinenti al processo di sviluppo della normazione.

2. Nel fissare le tariffe per la valutazione della conformità a norma dell'articolo 43 si tiene conto degli interessi e delle esigenze specifici delle PMI fornitrici, comprese le start-up, riducendo tali tariffe proporzionalmente alle loro dimensioni, alle dimensioni del loro mercato e ad altri indicatori pertinenti.

3. L'ufficio per l'IA intraprende le azioni seguenti:

a) fornire modelli standardizzati per i settori contemplati dal presente regolamento, come specificato dal comitato nella sua richiesta;

b) sviluppare e mantenere una piattaforma unica di informazione che fornisce informazioni di facile uso in relazione al presente regolamento per tutti gli operatori in tutta l'Unione;

c) organizzare adeguate campagne di comunicazione per sensibilizzare in merito agli obblighi derivanti dal presente regolamento;

d) valutare e promuovere la convergenza delle migliori pratiche nelle procedure di appalto pubblico in relazione ai sistemi di IA.

Articolo 63

Deroghe per operatori specifici

1. Le microimprese ai sensi della raccomandazione 2003/361/CE possono conformarsi a determinati elementi del sistema di gestione della qualità di cui all'articolo 17 del presente regolamento in modo semplificato, purché non abbiano imprese associate o collegate ai sensi di tale raccomandazione. A tal fine, la Commissione elabora orientamenti sugli elementi del sistema di gestione della qualità che possono essere rispettati in modo semplificato tenendo conto delle esigenze delle microimprese, senza incidere sul livello di protezione o sulla necessità di conformità ai requisiti per quanto riguarda i sistemi di IA ad alto rischio.

2. Il paragrafo 1 del presente articolo non è interpretato nel senso che esenta tali operatori dal rispetto di altri requisiti e obblighi di cui al presente regolamento, compresi quelli stabiliti agli articoli 9, 10, 11, 12, 13, 14, 15, 72 e 73.

CAPO VII

GOVERNANCE

SEZIONE 1

Governance a livello dell'Unione

Articolo 64

Ufficio per l'IA

1. La Commissione sviluppa le competenze e le capacità dell'Unione nel settore dell'IA attraverso l'ufficio per l'IA.

2. Gli Stati membri agevolano i compiti affidati all'ufficio per l'IA, come indicato nel presente regolamento.

Articolo 65

Istituzione e struttura del consiglio per l'IA europeo per l'intelligenza artificiale

1. È istituito un consiglio per l'IA europeo per l'intelligenza artificiale («consiglio per l'IA»).

2. Il consiglio per l'IA è composto di un rappresentante per Stato membro. Il Garante europeo della protezione dei dati partecipa come osservatore. Anche l'ufficio per l'IA partecipa alle riunioni del consiglio per l'IA senza partecipare alle votazioni. Altre autorità, organismi o esperti nazionali e dell'Unione possono essere invitati alle riunioni dal consiglio per l'IA caso per caso, qualora le questioni discusse siano di loro pertinenza.

3. Ciascun rappresentante è designato dal rispettivo Stato membro per un periodo di tre anni, rinnovabile una volta.

4. Gli Stati membri provvedono affinché i loro rappresentanti nel consiglio per l'IA:

a) dispongano delle competenze e dei poteri pertinenti nel proprio Stato membro in modo da contribuire attivamente allo svolgimento dei compiti del consiglio per l'IA di cui all'articolo 66;

b) siano designati come punto di contatto unico nei confronti del consiglio per l'IA e, se del caso tenendo conto delle esigenze degli Stati membri, come punto di contatto unico per i portatori di interessi;

c) abbiano il potere di agevolare la coerenza e il coordinamento tra le autorità nazionali competenti nel rispettivo Stato membro per quanto riguarda l'attuazione del presente regolamento, anche attraverso la raccolta di dati e informazioni pertinenti ai fini dello svolgimento dei loro compiti in seno al consiglio per l'IA.

5. I rappresentanti designati degli Stati membri adottano il regolamento interno del consiglio per l'IA a maggioranza di due terzi. Il regolamento interno stabilisce, in particolare, le procedure per il processo di selezione, la durata del mandato e le specifiche riguardanti i compiti del presidente, le modalità dettagliate relative al voto e l'organizzazione delle attività del consiglio per l'IA e dei suoi sottogruppi.

6. Il consiglio per l'IA istituisce due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e notificare le autorità su questioni relative rispettivamente alla vigilanza del mercato e agli organismi notificati.

Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per il presente regolamento ai sensi dell'articolo 30 del regolamento (UE) 2019/1020.

Il consiglio per l'IA può istituire altri sottogruppi permanenti o temporanei, se del caso, ai fini dell'esame di questioni specifiche. Se del caso, i rappresentanti del forum consultivo di cui all'articolo 67 possono essere invitati a tali sottogruppi o a riunioni specifiche di tali sottogruppi in qualità di osservatori.

7. Il consiglio per l'IA è organizzato e gestito in modo che sia salvaguardata l'obiettività e l'imparzialità delle sue attività.

8. Il consiglio per l'IA è presieduto da uno dei rappresentanti degli Stati membri. L'ufficio per l'IA provvede alle funzioni di segretariato per il consiglio per l'IA, convoca le riunioni su richiesta della presidenza e prepara l'ordine del giorno in conformità dei compiti del consiglio per l'IA a norma del presente regolamento e del relativo regolamento interno.

Articolo 66

Compiti del consiglio per l'IA

Il consiglio per l'IA fornisce consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del presente regolamento. A tal fine il consiglio per l'IA può in particolare:

a) contribuire al coordinamento tra le autorità nazionali competenti responsabili dell'applicazione del presente regolamento e, in cooperazione con le autorità di vigilanza del mercato interessate e previo accordo di queste ultime, sostenere le attività congiunte delle autorità di vigilanza del mercato di cui all'articolo 74, paragrafo 11;

b) raccogliere e condividere tra gli Stati membri conoscenze e migliori pratiche tecniche e normative;

c) fornire consulenza sull'attuazione del presente regolamento, in particolare per quanto riguarda l'applicazione delle norme sui modelli di IA per finalità generali;

d) contribuire all'armonizzazione delle pratiche amministrative negli Stati membri, anche in relazione alla deroga alle procedure di valutazione della conformità di cui all'articolo 46, al funzionamento degli spazi di sperimentazione normativa per l'IA e alle prove in condizioni reali di cui agli articoli 57, 59 e 60;

e) su richiesta della Commissione o di propria iniziativa, formulare raccomandazioni e pareri scritti su qualsiasi questione pertinente relativa all'attuazione del presente regolamento e alla sua applicazione coerente ed efficace, tra l'altro:

   i) sull'elaborazione e l'applicazione di codici di condotta e codici di buone pratiche a norma del presente regolamento, nonché degli orientamenti della Commissione;

   ii) sulla valutazione e il riesame del presente regolamento a norma dell'articolo 112, anche per quanto riguarda la comunicazione di incidenti gravi di cui all'articolo 73, e il funzionamento della banca dati dell'UE di cui all'articolo 71, la preparazione degli atti delegati o di esecuzione e gli eventuali allineamenti del presente regolamento alla normativa di armonizzazione elencata nell'allegato I;

   iii) sulle specifiche tecniche o sulle norme esistenti relative ai requisiti di cui al capo III, sezione 2;

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

v) sulle tendenze, quali la competitività globale europea nell'IA, l'adozione dell'IA nell'Unione e lo sviluppo di competenze digitali;

vi) sulle tendenze relative all'evoluzione della tipologia delle catene del valore dell'IA, in particolare per quanto riguarda le conseguenti implicazioni in termini di responsabilità;

vii) sull'eventuale necessità di modificare l'allegato III conformemente all'articolo 7 e sull'eventuale necessità di una possibile revisione dell'articolo 5 a norma dell'articolo 112, tenendo conto delle pertinenti prove disponibili e degli ultimi sviluppi tecnologici;

f) sostenere la Commissione nella promozione dell'alfabetizzazione in materia di IA, della sensibilizzazione del pubblico e della comprensione dei benefici, dei rischi, delle garanzie e dei diritti e degli obblighi in relazione all'uso dei sistemi di IA;

g) facilitare lo sviluppo di criteri comuni e una comprensione condivisa tra gli operatori del mercato e le autorità competenti dei concetti pertinenti di cui al presente regolamento, anche contribuendo allo sviluppo di parametri di riferimento;

h) cooperare, se del caso, con altre istituzioni e altri organi e organismi dell'Unione nonché con i pertinenti gruppi di esperti e reti dell'Unione, in particolare nei settori della sicurezza dei prodotti, della cibersicurezza, della concorrenza, dei servizi digitali e dei media, dei servizi finanziari, della protezione dei consumatori, dei dati e dei diritti fondamentali;

i) contribuire all'efficace cooperazione con le autorità competenti dei paesi terzi e con le organizzazioni internazionali;

j) assistere le autorità nazionali competenti e la Commissione nello sviluppo delle competenze organizzative e tecniche necessarie per l'attuazione del presente regolamento, anche contribuendo alla valutazione delle esigenze di formazione del personale degli Stati membri coinvolto nell'attuazione del presente regolamento;

k) assistere l'ufficio per l'IA nel sostenere le autorità nazionali competenti nell'istituzione e nello sviluppo di spazi di sperimentazione normativa per l'IA e facilitare la cooperazione e la condivisione di informazioni tra gli spazi di sperimentazione normativa per l'IA;

l) contribuire all'elaborazione di documenti di orientamento e fornire consulenza al riguardo;

m) fornire consulenza alla Commissione sulle questioni internazionali in materia di IA;

n) fornire pareri alla Commissione sulle segnalazioni qualificate relative ai modelli di IA per finalità generali;

o) ricevere pareri dagli Stati membri sulle segnalazioni qualificate relative ai modelli di IA per finalità generali e sulle esperienze e pratiche nazionali in materia di monitoraggio e applicazione dei sistemi di IA, in particolare dei sistemi che integrano i modelli di IA per finalità generali.

Articolo 67

Forum consultivo

1. È istituito un forum consultivo per fornire consulenza e competenze tecniche al consiglio per l'IA e alla Commissione, nonché per contribuire ai loro compiti a norma del presente regolamento.

2. La composizione del forum consultivo rappresenta una selezione equilibrata di portatori di interessi, tra cui l'industria, le start-up, le PMI, la società civile e il mondo accademico. La composizione del forum consultivo è equilibrata per quanto riguarda gli interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, per quanto riguarda le PMI e le altre imprese.

3. La Commissione nomina i membri del forum consultivo, conformemente ai criteri stabiliti al paragrafo 2, tra i portatori di interessi con competenze riconosciute nel settore dell'IA.

4. Il mandato dei membri del forum consultivo ha una durata di due anni, prorogabile fino a un massimo di quattro anni.

5. L'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo per le norme di telecomunicazione (ETSI) sono membri permanenti del forum consultivo.

6. Il forum consultivo redige il proprio regolamento interno. Esso elegge due copresidenti tra i suoi membri, conformemente ai criteri stabiliti al paragrafo 2. Il mandato dei copresidenti ha una durata di due anni, rinnovabile una volta.

7. Il forum consultivo tiene riunioni almeno due volte all'anno. Il forum consultivo può invitare esperti e altri portatori di interessi alle sue riunioni.

8. Il forum consultivo può elaborare pareri, raccomandazioni e contributi scritti su richiesta del consiglio per l'IA o della Commissione.

9. Il forum consultivo può istituire sottogruppi permanenti o temporanei, se necessario, per esaminare questioni specifiche connesse agli obiettivi del presente regolamento.

10. Il forum consultivo prepara una relazione annuale sulle sue attività. Tale relazione è resa pubblica.

Articolo 68

Gruppo di esperti scientifici indipendenti

1. La Commissione adotta, mediante un atto di esecuzione, disposizioni sull'istituzione di un gruppo di esperti scientifici indipendenti («gruppo di esperti scientifici») inteso a sostenere le attività di esecuzione a norma del presente regolamento. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

2. Il gruppo di esperti scientifici è composto da esperti selezionati dalla Commissione sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'IA necessarie per lo svolgimento dei compiti di cui al paragrafo 3 ed è in grado di dimostrare di soddisfare tutte le condizioni seguenti:

a) possesso di particolari conoscenze e capacità nonché competenze scientifiche o tecniche nel settore dell'IA;

b) indipendenza da qualsiasi fornitore di sistemi di IA o di modelli di IA per finalità generali;

c) capacità di svolgere attività in modo diligente, accurato e obiettivo.

La Commissione, in consultazione con il consiglio per l'IA, determina il numero di esperti del gruppo in funzione delle esigenze richieste e garantisce un'equa rappresentanza di genere e geografica.

3. Il gruppo di esperti scientifici fornisce consulenza e sostegno all'ufficio per l'IA, in particolare per quanto riguarda i compiti seguenti:

a) sostenere l'attuazione e l'esecuzione del presente regolamento per quanto riguarda i modelli e i sistemi di IA per finalità generali, in particolare:

   i) segnalare all'ufficio per l'IA i possibili rischi sistemici a livello dell'Unione dei modelli di IA per finalità generali, conformemente all'articolo 90;

   ii) contribuire allo sviluppo di strumenti e metodologie per valutare le capacità dei modelli e sistemi di IA per finalità generali, anche attraverso parametri di riferimento;

   iii) fornire consulenza sulla classificazione dei modelli di IA per finalità generali con rischio sistemico;

   iv) fornire consulenza sulla classificazione di vari modelli e sistemi di IA per finalità generali;

v) contribuire allo sviluppo di strumenti e modelli;

b) sostenere il lavoro delle autorità di vigilanza del mercato, su richiesta di queste ultime;

c) sostenere le attività transfrontaliere di vigilanza del mercato di cui all'articolo 74, paragrafo 11, fatti salvi i poteri delle autorità di vigilanza del mercato;

d) sostenere l'ufficio per l'IA nello svolgimento delle sue funzioni nell'ambito della procedura di salvaguardia dell'Unione di cui all'articolo 81.

4. Gli esperti scientifici del gruppo svolgono i loro compiti con imparzialità e obiettività e garantiscono la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività. Non sollecitano né accettano istruzioni da nessuno nell'esercizio dei loro compiti di cui al paragrafo 3. Ogni esperto compila una dichiarazione di interessi, che rende accessibile al pubblico. L'ufficio per l'IA istituisce sistemi e procedure per gestire attivamente e prevenire potenziali conflitti di interesse.

5. L'atto di esecuzione di cui al paragrafo 1 comprende disposizioni sulle condizioni, le procedure e le modalità dettagliate in base alle quali il gruppo di esperti scientifici e i suoi membri effettuano segnalazioni e chiedono l'assistenza dell'ufficio per l'IA per lo svolgimento dei compiti del gruppo di esperti scientifici.

Articolo 69

Accesso al gruppo di esperti da parte degli Stati membri

1. Gli Stati membri possono ricorrere agli esperti scientifici del gruppo affinché sostengano le loro attività di esecuzione a norma del presente regolamento.

2. Gli Stati membri possono essere tenuti a pagare tariffe per la consulenza e il sostegno forniti dagli esperti. La struttura e il livello delle tariffe, nonché l'entità e la struttura delle spese ripetibili sono indicati nell'atto di esecuzione di cui all'articolo 68, paragrafo 1, tenendo conto degli obiettivi di adeguata attuazione del presente regolamento, efficacia in termini di costi e necessità di garantire un accesso effettivo agli esperti per tutti gli Stati membri.

3. La Commissione facilita l'accesso tempestivo agli esperti da parte degli Stati membri, ove necessario, e garantisce che la combinazione di attività di sostegno svolte dalle strutture di sostegno dell'Unione per la prova dell'IA a norma dell'articolo 84 e dagli esperti a norma del presente articolo sia organizzata in modo efficiente e fornisca il miglior valore aggiunto possibile.

SEZIONE 2

Autorità nazionali competenti

Articolo 70

Designazione delle autorità nazionali competenti e dei punti di contatto unici

1. Ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità si astengono da qualsiasi atto incompatibile con le loro funzioni. A condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro.

2. Gli Stati membri comunicano alla Commissione l'identità delle autorità di notifica e delle autorità di vigilanza del mercato e i compiti di tali autorità, nonché ogni successiva modifica degli stessi. Gli Stati membri mettono a disposizione del pubblico le informazioni sulle modalità con cui le autorità competenti e i punti di contatto unici possono essere contattati, tramite mezzi di comunicazione elettronica, entro il 2 agosto 2025. Gli Stati membri designano un'autorità di vigilanza del mercato che funga da punto di contatto unico per il presente regolamento e notificano alla Commissione l'identità del punto di contatto unico. La Commissione elabora un elenco dei punti di contatto unici disponibili al pubblico.

3. Gli Stati membri garantiscono che le loro autorità nazionali competenti dispongano di risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti 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 IA, della protezione dei dati personali, della cibersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti. Gli Stati membri valutano e, se necessario, aggiornano annualmente i requisiti in termini di competenze e risorse di cui al presente paragrafo.

4. Le autorità nazionali competenti adottano misure adeguate per garantire un livello adeguato di cibersicurezza.

5. Nello svolgimento dei propri compiti, le autorità nazionali competenti agiscono in conformità degli obblighi di riservatezza di cui all'articolo 78.

6. Entro il 2 agosto 2025, e successivamente una volta ogni due anni, gli Stati membri riferiscono 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 consiglio per l'IA affinché le discuta e formuli eventuali raccomandazioni.

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

8. Le autorità nazionali competenti possono fornire orientamenti e consulenza sull'attuazione del presente regolamento, in particolare alle PMI, comprese le start-up, tenendo conto degli orientamenti e della consulenza del consiglio per l'IA e della Commissione, a seconda dei casi. Ogniqualvolta le autorità nazionali competenti intendono fornire orientamenti e consulenza in relazione a un sistema di IA in settori disciplinati da altre disposizioni di diritto dell'Unione, sono consultate le autorità nazionali competenti a norma di tali disposizioni di diritto dell'Unione, come opportuno.

9. Qualora le istituzioni, gli organi e gli organismi dell'Unione rientrino nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità competente per la loro vigilanza.

CAPO VIII

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

Articolo 71

Banca dati dell'UE per i sistemi di IA ad alto rischio elencati nell'allegato III

1. La Commissione, in collaborazione con gli Stati membri, istituisce e mantiene una banca dati dell'UE contenente le informazioni di cui ai paragrafi 2 e 3 del presente articolo relative ai sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2, registrati conformemente agli articoli 49 e 60 e ai sistemi di IA che non sono considerati ad alto rischio a norma dell'articolo 6, paragrafo 3, e che sono registrati in conformità dell'articolo 6, paragrafo 4 e dell'articolo 69. Nel definire le specifiche funzionali di tale banca dati, la Commissione consulta gli esperti competenti e, nell'aggiornare le specifiche funzionali di tale banca dati, consulta il consiglio per l'IA.

2. I dati elencati nell'allegato VIII, sezioni A e B, sono inseriti nella banca dati dell'UE dal fornitore o, se del caso, dal rappresentante autorizzato.

3. I dati elencati nell'allegato VIII, sezione C, sono inseriti nella banca dati dell'UE dal deployer che è un'autorità, un'agenzia o un organismo pubblico, conformemente all'articolo 49, paragrafi 3 e 4, o che agisce per conto di essi.

4. Ad eccezione della sezione di cui all'articolo 49, paragrafo 4, e all'articolo 60, paragrafo 4, lettera c), le informazioni contenute nella banca dati dell'UE registrate a norma dell'articolo 49 sono accessibili e disponibili al pubblico in modo facilmente fruibile. Le informazioni dovrebbero essere di facile consultazione e leggibili meccanicamente. Le informazioni registrate a norma dell'articolo 60 sono accessibili solo alle autorità di vigilanza del mercato e alla Commissione, a meno che il fornitore o il potenziale fornitore non abbia dato il suo consenso anche a rendere tali informazioni accessibili al pubblico.

5. La banca dati dell'UE contiene dati personali solo nella misura necessaria per la raccolta e il trattamento delle informazioni in conformità del 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 o il deployer, se del caso.

6. La Commissione è il titolare del trattamento della banca dati dell'UE. Essa mette a disposizione dei fornitori, dei potenziali fornitori e dei deployer un adeguato sostegno tecnico e amministrativo. La banca dati dell'UE è conforme ai requisiti di accessibilità applicabili.

CAPO IX

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

SEZIONE 1

Monitoraggio successivo all'immissione sul mercato

Articolo 72

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 IA 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 che possono essere forniti dai deployer o che possono essere 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 capo III, sezione 2. Se del caso, il monitoraggio successivo all'immissione sul mercato include un'analisi dell'interazione con altri sistemi di IA. Tale obbligo non riguarda i dati operativi sensibili dei deployer che sono autorità di contrasto.

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 entro il 2 febbraio 2026. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

4. Per i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, qualora tale normativa preveda già un sistema e un piano di monitoraggio successivo all'immissione sul mercato, al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari elementi di cui ai paragrafi 1, 2 e 3 utilizzando il modello di cui al paragrafo 3 nei sistemi e nei piani già esistenti in virtù di tale normativa, a condizione che consegua un livello di protezione equivalente.

Il primo comma del presente paragrafo si applica anche ai sistemi di IA ad alto rischio di cui all'allegato III, punto 5, immessi sul mercato o messi in servizio da istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari.

SEZIONE 2

Condivisione di informazioni su incidenti gravi

Articolo 73

Comunicazione di incidenti gravi

1. I fornitori di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi incidente grave alle autorità di vigilanza del mercato degli Stati membri in cui tali incidenti si sono verificati.

2. La segnalazione di cui al paragrafo 1 è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente grave o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che il fornitore o, se del caso, il deployer, è venuto a conoscenza dell'incidente grave.

Il periodo per la segnalazione di cui al primo comma tiene conto della gravità dell'incidente grave.

3. In deroga al paragrafo 2 del presente articolo, in caso di un'infrazione diffusa o di un incidente grave quale definito all'articolo 3, punto 49, lettera b), la segnalazione di cui al paragrafo 1 del presente articolo è trasmessa immediatamente e non oltre due giorni dopo che il fornitore o, se del caso, il deployer è venuto a conoscenza di tale incidente.

4. In deroga al paragrafo 2, in caso di decesso di una persona, la segnalazione è trasmessa immediatamente dopo che il fornitore o il deployer ha stabilito, o non appena sospetta, un nesso causale tra il sistema di IA ad alto rischio e l'incidente grave, ma non oltre 10 giorni dalla data in cui il fornitore o, se del caso, il deployer è venuto a conoscenza dell'incidente grave.

5. Se necessario per garantire una comunicazione tempestiva, il fornitore o, se del caso, il deployer, può presentare una relazione iniziale incompleta, seguita da una relazione completa.

6. A seguito della comunicazione di un incidente grave a norma del paragrafo 1, il fornitore svolge senza indugio le indagini necessarie in relazione all'incidente grave e al sistema di IA interessato. Ciò comprende una valutazione del rischio dell'incidente nonché misure correttive.

Il fornitore coopera con le autorità competenti e, se del caso, con l'organismo notificato interessato durante le indagini di cui al primo comma e non svolge alcuna indagine che comporti una modifica del sistema di IA interessato in un modo che possa incidere su un'eventuale successiva valutazione delle cause dell'incidente, prima di informare le autorità competenti di tale azione.

7. Al ricevimento di una notifica relativa a un incidente grave di cui all'articolo 3, punto 49, lettera c), l'autorità di vigilanza del mercato interessata informa le autorità o gli organismi pubblici nazionali di cui all'articolo 77, paragrafo 1. La Commissione elabora orientamenti specifici per facilitare il rispetto degli obblighi di cui al paragrafo 1 del presente articolo. Tali orientamenti sono emanati entro il 2 agosto 2025 e sono valutati periodicamente.

8. L'autorità di vigilanza del mercato adotta le misure appropriate di cui all'articolo 19 del regolamento (UE) 2019/1020 entro sette giorni dalla data di ricevimento della notifica di cui al paragrafo 1 del presente articolo e segue le procedure di notifica previste da tale regolamento.

9. Per i sistemi di IA ad alto rischio di cui all'allegato III che sono immessi sul mercato o messi in servizio da fornitori soggetti a strumenti legislativi dell'Unione che stabiliscono obblighi in materia di segnalazione equivalenti a quelli previsti dal presente regolamento, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 49, lettera c).

10. Per i sistemi di IA ad alto rischio che sono componenti di sicurezza di dispositivi, o sono essi stessi dispositivi, disciplinati dai regolamenti (UE) 2017/745 e (UE) 2017/746, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 49, lettera c), del presente regolamento, del presente regolamento ed è trasmessa all'autorità nazionale competente scelta a tal fine dagli Stati membri in cui si è verificato l'incidente.

11. Le autorità nazionali competenti notificano immediatamente alla Commissione qualsiasi incidente grave, indipendentemente dal fatto che abbiano o meno preso provvedimenti al riguardo, conformemente all'articolo 20 del regolamento (UE) 2019/1020.

SEZIONE 3

Applicazione

Articolo 74

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. 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 all'articolo 2, paragrafo 1, 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. Nell'ambito dei loro obblighi in materia di segnalazione a norma dell'articolo 34, paragrafo 4, del regolamento (UE) 2019/1020, le autorità di vigilanza del mercato comunicano annualmente 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. Essi riferiscono inoltre annualmente alla Commissione in merito al ricorso a pratiche vietate verificatosi nel corso di tale anno e alle misure adottate.

3. Per i sistemi di IA ad alto rischio collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, 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.

In deroga al primo comma e in determinate circostanze, gli Stati membri possono designare un'altra autorità pertinente che agisca in qualità di autorità di vigilanza del mercato, a condizione che garantiscano il coordinamento con le pertinenti autorità settoriali di vigilanza del mercato responsabili dell'esecuzione della normativa di armonizzazione dell'Unione elencata nell'allegato I.

4. Le procedure di cui agli articoli da 79 a 83 del presente regolamento non si applicano ai sistemi di IA collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, qualora tali atti giuridici prevedano già procedure che garantiscono un livello equivalente di protezione e aventi lo stesso obiettivo. In tali casi si applicano invece le pertinenti procedure settoriali.

5. Fatti salvi i poteri delle autorità di vigilanza del mercato di cui all'articolo 14 del regolamento (UE) 2019/1020, al fine di garantire l'efficace applicazione del presente regolamento, le autorità di vigilanza del mercato possono esercitare i poteri di cui all'articolo 14, paragrafo 4, lettere d) e j), di tale regolamento a distanza, se del caso.

6. Per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti ai sensi di tale diritto, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di IA siano direttamente collegati alla fornitura di tali servizi finanziari.

7. In deroga al paragrafo 6, in determinate circostanze e a condizione che sia garantito il coordinamento, lo Stato membro può individuare un'altra autorità competente come autorità di vigilanza del mercato ai fini del presente regolamento.

Le autorità nazionali di vigilanza del mercato che controllano gli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento (UE) n, 1024/2013, dovrebbero comunicare senza indugio alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento.

8. Per i sistemi di IA ad alto rischio elencati nell'allegato III del presente regolamento, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III del presente regolamento, punti 6, 7 e 8, 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 del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680. Le attività di vigilanza del mercato non pregiudicano in alcun modo l'indipendenza delle autorità giudiziarie né interferiscono in altro modo con le loro attività nell'esercizio delle loro funzioni giurisdizionali.

9. Nei casi in cui le istituzioni, gli organi 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, tranne nei confronti della Corte di giustizia dell'Unione europea nell'esercizio delle sue funzioni giurisdizionali.

10. 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 I o di altre disposizioni del diritto dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III.

11. Le autorità di vigilanza del mercato e la Commissione possono proporre attività congiunte, comprese indagini congiunte, che dovrebbero essere condotte dalle autorità di vigilanza del mercato o dalle autorità di vigilanza del mercato di concerto con la Commissione, al fine di promuovere la conformità, individuare casi di non conformità, sensibilizzare e fornire orientamenti in relazione al presente regolamento riguardo a specifiche categorie di sistemi di IA ad alto rischio che si rileva presentino un rischio grave in due o più Stati membri conformemente all'articolo 9 del regolamento (UE) 2019/1020. L'ufficio per l'IA fornisce sostegno di coordinamento per le indagini congiunte.

12. Fatti salvi i poteri di cui al regolamento (UE) 2019/1020 e se del caso e nei limiti di quanto necessario per lo svolgimento dei loro compiti, i fornitori concedono alle autorità di vigilanza del mercato pieno accesso alla documentazione nonché ai set di dati di addestramento, convalida e prova utilizzati per lo sviluppo dei sistemi di IA ad alto rischio, anche, ove opportuno e fatte salve le garanzie di sicurezza, attraverso interfacce di programmazione delle applicazioni (API) o altri mezzi e strumenti tecnici pertinenti che consentano l'accesso remoto.

13. Alle autorità di vigilanza del mercato è concesso l'accesso al codice sorgente del sistema di IA ad alto rischio su richiesta motivata e solo qualora siano soddisfatte entrambe le condizioni seguenti:

a) l'accesso al codice sorgente è necessario per valutare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo III, sezione 2; e

b) le procedure di prova o di audit e le verifiche basate sui dati e sulla documentazione presentati dal fornitore sono state esaurite o si sono dimostrate insufficienti.

14. Qualsiasi informazione o documentazione ottenuta dalle autorità di vigilanza del mercato è trattata in conformità degli obblighi di riservatezza di cui all'articolo 78.

Articolo 75

Assistenza reciproca, vigilanza del mercato e controllo dei sistemi di IA per finalità generali

1. Qualora un sistema di IA si basi su un modello di IA per finalità generali e il modello e il sistema siano sviluppati dallo stesso fornitore, l'ufficio per l'IA ha il potere di monitorare e supervisionare la conformità di tale sistema di IA agli obblighi di cui al presente regolamento. Per svolgere i suoi compiti di monitoraggio e supervisione, l'ufficio per l'IA dispone di tutti i poteri di un'autorità di vigilanza del mercato prevista dalla presente sezione e dal regolamento (UE) 2019/1020.

2. Qualora abbiano motivi sufficienti per ritenere che i sistemi di IA per finalità generali che possono essere utilizzati direttamente dai deployer per almeno una finalità classificata come ad alto rischio a norma del presente regolamento non siano conformi ai requisiti di cui al presente regolamento, le pertinenti autorità di vigilanza del mercato cooperano con l'ufficio per l'IA per effettuare valutazioni della conformità e informano di conseguenza il consiglio per l'IA e le altre autorità di vigilanza del mercato.

3. Qualora non sia in grado di concludere la propria indagine sul sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali nonostante abbia compiuto tutti gli sforzi opportuni per ottenere tali informazioni, un'autorità di vigilanza del mercato può presentare una richiesta motivata all'ufficio per l'IA, che garantisce l'accesso a tali informazioni. In tal caso, l'ufficio per l'IA fornisce all'autorità richiedente senza indugio, e in ogni caso entro 30 giorni, tutte le informazioni che esso ritiene pertinenti al fine di stabilire se un sistema di IA ad alto rischio non è conforme. Le autorità di vigilanza del mercato salvaguardano la riservatezza delle informazioni ottenute conformemente all'articolo 78 del presente regolamento. La procedura di cui al capo VI del regolamento (UE) 2019/1020 si applica mutatis mutandis.

Articolo 76

Controllo delle prove in condizioni reali da parte delle autorità di vigilanza del mercato

1. Le autorità di vigilanza del mercato hanno le competenze e i poteri per garantire che le prove in condizioni reali siano conformi al presente regolamento.

2. Qualora siano effettuate prove in condizioni reali per i sistemi di IA sottoposti a controllo all'interno di uno spazio di sperimentazione normativa per l'IA a norma dell'articolo 58, le autorità di vigilanza del mercato verificano la conformità dell'articolo 60 nell'ambito del loro ruolo di controllo per lo spazio di sperimentazione normativa per l'IA. Tali autorità possono, se del caso, consentire che le prove in condizioni reali siano effettuate dal fornitore o potenziale fornitore in deroga alle condizioni di cui all'articolo 60, paragrafo 4, lettere f) e g).

3. Qualora sia stata informata dal potenziale fornitore, dal fornitore o da un terzo di un incidente grave o abbia altri motivi per ritenere che le condizioni di cui agli articoli 60 e 61 non siano soddisfatte, un'autorità di vigilanza del mercato può adottare una delle seguenti decisioni sul suo territorio, a seconda dei casi:

a) sospendere o cessare le prove in condizioni reali;

b) imporre al fornitore o potenziale fornitore e al deployer o al potenziale deployer di modificare qualsiasi aspetto delle prove in condizioni reali.

4. Ove un'autorità di vigilanza del mercato abbia adottato una decisione di cui al paragrafo 3 o sollevato un'obiezione ai sensi dell'articolo 60, paragrafo 4, lettera b), la decisione o l'obiezione ne indica i motivi ed espone le modalità con cui il fornitore o potenziale fornitore può contestare la decisione o l'obiezione.

5. Se del caso, ove un'autorità di vigilanza del mercato abbia adottato una decisione di cui al paragrafo 3, ne comunica i motivi alle autorità di vigilanza del mercato degli altri Stati membri in cui il sistema di IA è stato sottoposto a prova conformemente al piano di prova.

Articolo 77

Poteri delle autorità che tutelano i diritti fondamentali

1. Le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, compreso il diritto alla non discriminazione, 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, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati 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.

2. Entro il 2 novembre 2024 ciascuno Stato membro individua le autorità o gli organismi pubblici di cui al paragrafo 1 e ne pubblica l'elenco. Gli Stati membri notificano l'elenco alla Commissione e agli altri Stati membri e lo tengono aggiornato.

3. Qualora la documentazione di cui al paragrafo 1 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 1 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.

4. Qualsiasi informazione o documentazione ottenuta a norma del presente articolo dalle autorità o dagli organismi pubblici nazionali di cui al paragrafo 1 del presente articolo è trattata in conformità degli obblighi di riservatezza stabiliti all'articolo 78.

Articolo 78

Riservatezza

1. In conformità del diritto dell'Unione o nazionale, la Commissione, le autorità di vigilanza del mercato e gli organismi notificati, nonché le altre persone fisiche o giuridiche che partecipano all'applicazione del presente regolamento, garantiscono 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 nei casi di cui all'articolo 5 della direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio ([57]);

b) l'efficace attuazione del presente regolamento, in particolare ai fini delle ispezioni, delle indagini e degli audit;

c) gli interessi pubblici e di sicurezza nazionale;

d) lo svolgimento del procedimento penale o amministrativo;

e) le informazioni classificate a norma del diritto dell'Unione o nazionale.

2. Le autorità che partecipano all'applicazione del presente regolamento a norma del paragrafo 1 richiedono solo i dati strettamente necessari per la valutazione del rischio posto dai sistemi di IA e per l'esercizio dei loro poteri conformemente al presente regolamento e al regolamento (UE) 2019/1020. Esse pongono in essere misure di cibersicurezza adeguate ed efficaci per proteggere la sicurezza e la riservatezza delle informazioni e dei dati ottenuti e cancellano i dati raccolti non appena non sono più necessari per lo scopo per il quale sono stati ottenuti, conformemente al diritto dell'Unione o nazionale applicabile.

3. Fatti salvi i paragrafi 1 e 2, nel momento in cui i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 o 7, sono utilizzati dalle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo, le informazioni scambiate in via riservata tra le autorità nazionali competenti, o tra le autorità nazionali competenti e la Commissione, non sono divulgate senza previa consultazione dell'autorità nazionale competente e del deployer che hanno prodotto tali informazioni, qualora tale divulgazione rischi di compromettere gli interessi pubblici e di sicurezza nazionale. Tale scambio di informazioni non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo.

Qualora le autorità competenti in materia di contrasto, di immigrazione o di asilo siano fornitori di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 o 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 74, paragrafi 8 e 9, 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.

4. I paragrafi 1, 2 e 3 non pregiudicano i diritti o gli obblighi della Commissione, degli Stati membri e delle rispettive autorità pertinenti nonché quelli degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, anche nel contesto della cooperazione transfrontaliera, né pregiudicano gli obblighi delle parti interessate di fornire informazioni a norma del diritto penale degli Stati membri.

5. La Commissione e gli Stati membri possono scambiare, ove necessario e conformemente alle pertinenti disposizioni degli accordi internazionali e commerciali, 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 79

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

1. Un sistema di IA che presenta un rischio è inteso come un «prodotto che presenta un rischio» quale definito all'articolo 3, punto 19, del regolamento (UE) 2019/1020 nella misura in cui presenta rischi per la salute o la sicurezza o per i diritti fondamentali delle persone.

2. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia un motivo sufficiente per ritenere che un sistema di IA presenti un rischio di cui al paragrafo 1 del presente articolo, 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. Particolare attenzione è prestata ai sistemi di IA che presentano un rischio per i gruppi vulnerabili. Qualora siano individuati rischi per i diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti di cui all'articolo 77, paragrafo 1, e coopera pienamente con essi. I pertinenti operatori cooperano, per quanto necessario, con l'autorità di vigilanza del mercato e con le altre autorità o gli altri organismi pubblici nazionali di cui all'articolo 77, paragrafo 1.

([57]) Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (GU L 157 del 15.6.2016, pag. 1).

Se, nel corso di tale valutazione, l'autorità di vigilanza del mercato o, se del caso, l'autorità di vigilanza del mercato in cooperazione con l'autorità pubblica nazionale di cui all'articolo 77, paragrafo 1, rilevano che il sistema di IA non è conforme ai requisiti e agli obblighi di cui al presente regolamento, esse chiedono senza indebito ritardo al pertinente operatore di adottare tutte le misure correttive adeguate al fine di rendere il sistema di IA conforme, ritirarlo dal mercato o richiamarlo entro il termine che l'autorità di vigilanza del mercato può prescrivere o, in ogni caso, entro 15 giorni lavorativi a seconda di quale termine sia il più breve, oppure entro il termine previsto dalla pertinente normativa di armonizzazione dell'Unione.

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 del presente paragrafo.

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 senza indebito ritardo 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 dell'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 o la messa in servizio del sistema di IA sul mercato nazionale, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo. Tale autorità notifica senza indebito ritardo tali misure alla Commissione e agli altri Stati membri.

6. La notifica di cui al paragrafo 5 include tutti i particolari disponibili, soprattutto le informazioni necessarie all'identificazione del sistema di IA non conforme, la sua origine e la catena di approvvigionamento, 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) non conformità al divieto delle pratiche di IA di cui all'articolo 5;

b) mancato rispetto da parte di un sistema di IA ad alto rischio dei requisiti di cui al capo III, sezione 2;

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

d) non conformità all'articolo 50.

7. Le autorità di vigilanza del mercato diverse dall'autorità di vigilanza del mercato dello Stato membro che ha avviato la procedura comunicano senza indebito 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 della notifica di cui al paragrafo 5 del presente articolo, un'autorità di vigilanza del mercato di uno Stato membro o la Commissione non sollevano obiezioni contro la misura provvisoria adottata da un'autorità di vigilanza del mercato di un altro Stato membro, tale misura è ritenuta giustificata. Ciò non pregiudica i diritti procedurali dell'operatore interessato in conformità dell'articolo 18 del regolamento (UE) 2019/1020. Il periodo di tre mesi di cui al presente paragrafo è ridotto a 30 giorni in caso di non conformità al divieto delle pratiche di IA di cui all'articolo 5 del presente regolamento.

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

Articolo 80

Procedura per i sistemi di IA classificati dal fornitore come non ad alto rischio in applicazione dell'allegato III

1. Se ha motivi sufficienti per ritenere che un sistema di IA classificato dal fornitore come non ad alto rischio a norma dell'articolo 6, paragrafo 3, sia in realtà ad alto rischio, l'autorità di vigilanza del mercato effettua una valutazione del sistema di IA interessato in relazione alla sua classificazione come sistema di IA ad alto rischio sulla base delle condizioni di cui all'articolo 6, paragrafo 3, e degli orientamenti della Commissione.

2. Se, nel corso di tale valutazione, ritiene che il sistema di IA interessato sia ad alto rischio, l'autorità di vigilanza del mercato chiede senza indebito ritardo al fornitore pertinente di adottare tutte le misure necessarie per rendere il sistema di IA conforme ai requisiti e agli obblighi di cui al presente regolamento, nonché di adottare le opportune misure correttive entro un termine che l'autorità di vigilanza del mercato può prescrivere.

3. Se ritiene che l'uso del sistema di IA interessato non sia limitato al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri senza indebito ritardo dei risultati della valutazione e delle misure che ha chiesto al fornitore di adottare.

4. Il fornitore garantisce che siano adottate tutte le misure necessarie per rendere il sistema di IA conforme ai requisiti e agli obblighi di cui al presente regolamento. Qualora il fornitore di un sistema di IA interessato non renda il sistema di IA conforme a tali requisiti e obblighi entro il termine di cui al paragrafo 2 del presente articolo, il fornitore è soggetto a sanzioni pecuniarie conformemente all'articolo 99.

5. Il fornitore 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 dell'Unione.

6. Se il fornitore del sistema di IA in questione non adotta misure correttive adeguate entro il periodo di cui al paragrafo 2 del presente articolo, si applica l'articolo 79, paragrafi da 5 a 9.

7. Qualora, nel corso della valutazione di cui al paragrafo 1 del presente articolo, l'autorità di vigilanza del mercato stabilisca che il sistema di IA è stato classificato erroneamente dal fornitore come non ad alto rischio al fine di eludere l'applicazione dei requisiti di cui al capo III, sezione 2, il fornitore è soggetto a sanzioni pecuniarie conformemente all'articolo 99.

8. Nell'esercizio del loro potere di monitorare l'applicazione del presente articolo e in conformità dell'articolo 11 del regolamento (UE) 2019/1020, le autorità di vigilanza del mercato possono eseguire i controlli del caso, tenendo conto in particolare delle informazioni conservate nella banca dati dell'UE di cui all'articolo 71 del presente regolamento.

Articolo 81

Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di cui all'articolo 79, paragrafo 5, o entro 30 giorni in caso di non conformità al divieto delle pratiche di IA di cui all'articolo 5, l'autorità di vigilanza del mercato di uno Stato membro solleva obiezioni contro una misura adottata da un'altra autorità di vigilanza del mercato, o se la Commissione ritiene che la misura sia contraria al diritto dell'Unione, la Commissione consulta senza indebito ritardo l'autorità di vigilanza del mercato dello Stato membro interessato e l'operatore o gli operatori e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione, entro sei mesi, o entro 60 giorni in caso di non conformità al divieto delle pratiche di IA di cui all'articolo 5, a decorrere dalla notifica di cui all'articolo 79, paragrafo 5, decide se la misura nazionale sia giustificata e notifica la sua decisione all'autorità di vigilanza del mercato dello Stato membro interessato. La Commissione informa anche tutte le altre autorità di vigilanza del mercato della sua decisione.

2. Se la Commissione ritiene che la misura adottata dallo Stato membro interessato sia giustificata, tutti gli Stati membri provvedono ad adottare misure restrittive appropriate in relazione al sistema di IA interessato, ad esempio richiedendo il ritiro del sistema di IA dal loro mercato senza indebito ritardo, e ne informano la Commissione. Se la Commissione ritiene che la misura nazionale sia ingiustificata, lo Stato membro interessato provvede a ritirarla e ne informa la Commissione.

3. Se la misura nazionale è ritenuta giustificata e la non conformità del sistema di IA è 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 prevista all'articolo 11 del regolamento (UE) n, 1025/2012.

Articolo 82

Sistemi di IA conformi che presentano un rischio

1. Se, dopo aver effettuato una valutazione a norma dell'articolo 79 e aver consultato la pertinente autorità pubblica nazionale di cui all'articolo 77, paragrafo 1, l'autorità di vigilanza del mercato di uno Stato membro ritiene che un sistema di IA ad alto rischio, pur conforme al presente regolamento, rappresenti comunque un rischio per la salute o la sicurezza delle persone, per i 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 in questione, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio senza indebito ritardo entro un termine che essa può prescrivere.

2. Il fornitore o un altro operatore pertinente garantisce l'adozione di misure correttive nei confronti di tutti i sistemi di IA interessati che ha messo a disposizione sul mercato dell'Unione entro il termine prescritto dall'autorità di vigilanza del mercato dello Stato membro di cui al paragrafo 1.

3. Gli Stati membri informano immediatamente la Commissione e gli altri Stati membri della conclusione cui sono giunti conformemente al paragrafo 1. 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 indebito ritardo consultazioni con gli Stati membri interessati e gli operatori pertinenti e valuta le misure nazionali adottate. In base ai risultati di tale valutazione, la Commissione decide se la misura sia giustificata e propone, ove necessario, altre misure appropriate.

5. La Commissione comunica immediatamente la propria decisione agli Stati membri interessati e agli operatori pertinenti e ne informa anche gli altri Stati membri.

Articolo 83

Non conformità formale

1. L'autorità di vigilanza del mercato di uno Stato membro chiede al fornitore pertinente, entro un termine che essa può prescrivere, di porre fine alla contestata non conformità qualora giunga a una delle conclusioni riportate di seguito:

a) la marcatura CE è stata apposta in violazione dell'articolo 48;

b) la marcatura CE non è stata apposta;

c) la dichiarazione di conformità UE di cui all'articolo 47 non è stata redatta;

d) la dichiarazione di conformità UE di cui all'articolo 47 non è stata redatta correttamente;

e) la registrazione nella banca dati dell'UE di cui all'articolo 71 non è stata effettuata;

f) se del caso, non è stato nominato nessun rappresentante autorizzato;

g) la documentazione tecnica non è disponibile.

2. Se la non conformità di cui al paragrafo 1 permane, l'autorità di vigilanza del mercato dello Stato membro interessato adotta misure appropriate e proporzionate per limitare o proibire la messa a disposizione sul mercato del sistema di IA ad alto rischio o per garantire che sia richiamato o ritirato dal mercato senza ritardo.

Articolo 84

Strutture di sostegno dell'Unione per la prova dell'IA

1. La Commissione designa una o più strutture di sostegno dell'Unione per la prova dell'IA per lo svolgimento dei compiti di cui all'articolo 21, paragrafo 6, del regolamento (UE) 2019/1020/nel settore dell'IA.

2. Fatti salvi i compiti di cui al paragrafo 1, le strutture di sostegno dell'Unione per la prova dell'IA forniscono anche pareri tecnici o scientifici indipendenti su richiesta del consiglio per l'IA, della Commissione o delle autorità di vigilanza del mercato.

SEZIONE 4

Mezzi di ricorso

Articolo 85

Diritto di presentare un reclamo a un'autorità di vigilanza del mercato

Fatti salvi altri ricorsi amministrativi o giurisdizionali, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del presente regolamento può presentare un reclamo alla pertinente autorità di vigilanza del mercato.

Conformemente al regolamento (UE) 2019/1020, tali reclami sono presi in considerazione ai fini dello svolgimento delle attività di vigilanza del mercato e sono trattati in linea con le procedure specifiche stabilite a tal fine dalle autorità di vigilanza del mercato.

Articolo 86

Diritto alla spiegazione dei singoli processi decisionali

1. Qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi elencati al punto 2 dello stesso, e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali ha il diritto di ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata.

2. Il paragrafo 1 non si applica all'uso di sistemi di IA per i quali sono previste eccezioni o limitazioni all'obbligo stabilito in tale paragrafo in virtù del diritto dell'Unione o del diritto nazionale, in linea con il diritto dell'Unione.

3. Il presente articolo si applica solo nella misura in cui il diritto di cui al paragrafo 1 non sia altrimenti previsto dal diritto dell'Unione.

Articolo 87

Segnalazione delle violazioni e protezione delle persone segnalanti

La direttiva (UE) 2019/1937 si applica alla segnalazione di violazioni del presente regolamento e alla protezione delle persone che segnalano tali violazioni.

SEZIONE 5

Supervisione, indagini, esecuzione e monitoraggio in relazione ai fornitori di modelli di IA per finalità generali

Articolo 88

Esecuzione degli obblighi dei fornitori di modelli di IA per finalità generali

1. La Commissione ha competenze esclusive per la vigilanza e l'esecuzione del capo V, tenendo conto delle garanzie procedurali a norma all'articolo 94. La Commissione affida l'attuazione di tali compiti all'ufficio per l'IA, fatte salve le competenze di organizzazione della Commissione e la ripartizione delle competenze tra gli Stati membri e l'Unione sulla base dei trattati.

2. Fatto salvo l'articolo 75, paragrafo 3, le autorità di vigilanza del mercato possono chiedere alla Commissione di esercitare le competenze di cui alla presente sezione, ove ciò sia necessario e proporzionato per assisterle nell'adempimento dei loro compiti a norma del presente regolamento.

Articolo 89

Azioni di monitoraggio

1. Ai fini dello svolgimento dei compiti ad esso assegnati a norma della presente sezione, l'ufficio per l'IA può intraprendere le azioni necessarie per monitorare l'efficace attuazione e il rispetto del presente regolamento da parte dei fornitori di modelli di IA per finalità generali, compresa la loro adesione ai codici di buone pratiche approvati.

2. I fornitori a valle hanno il diritto di presentare un reclamo per presunta violazione del presente regolamento. Il reclamo è debitamente motivato e indica almeno:

a) il punto di contatto del fornitore del modello di IA per finalità generali in questione;

b) una descrizione dei fatti di cui trattasi, delle pertinenti disposizioni del presente regolamento e del motivo per cui il fornitore a valle ritiene che il fornitore del modello di IA per finalità generali in questione abbia violato il presente regolamento;

c) qualsiasi altra informazione che il fornitore a valle che ha inviato la richiesta ritenga pertinente, comprese, se del caso, le informazioni raccolte di propria iniziativa.

Articolo 90

Segnalazioni di rischi sistemici da parte del gruppo di esperti scientifici

1. Il gruppo di esperti scientifici può effettuare una segnalazione qualificata all'ufficio per l'IA qualora abbia motivo di sospettare che:

a) un modello di IA per finalità generali presenti un rischio concreto identificabile a livello dell'Unione; o

b) un modello di IA per finalità generali soddisfi le condizioni di cui all'articolo 51.

2. In seguito a tale segnalazione qualificata, la Commissione, tramite l'ufficio per l'IA e dopo avere informato il consiglio per l'IA, può esercitare le competenze di cui alla presente sezione ai fini della valutazione della questione. L'ufficio per l'IA informa il consiglio per l'IA di qualsiasi misura conformemente agli articoli da 91 a 94.

3. La segnalazione qualificata è debitamente motivata e indica almeno:

a) il punto di contatto del fornitore del modello di IA per finalità generali con rischio sistemico in questione;

b) una descrizione dei fatti di cui trattasi e dei motivi della segnalazione effettuata dal gruppo di esperti scientifici;

c) qualsiasi altra informazione che il gruppo di esperti scientifici ritenga pertinente, comprese, se del caso, le informazioni raccolte di propria iniziativa.

Articolo 91

Potere di richiedere documentazione e informazioni

1. La Commissione può chiedere al fornitore del modello di IA per finalità generali in questione di fornire la documentazione redatta dal fornitore in conformità degli articoli 53 e 55 o qualsiasi altra informazione supplementare necessaria al fine di valutare la conformità del fornitore al presente regolamento.

2. Prima di inviare la richiesta di informazioni, l'ufficio per l'IA può avviare un dialogo strutturato con il fornitore del modello di IA per finalità generali.

3. Su richiesta debitamente motivata del gruppo di esperti scientifici, la Commissione può presentare una richiesta di informazioni a un fornitore di un modello di IA per finalità generali, qualora l'accesso alle informazioni sia necessario e proporzionato per l'adempimento dei compiti del gruppo di esperti scientifici a norma dell'articolo 68, paragrafo 2.

4. La richiesta di informazioni indica la base giuridica e lo scopo della richiesta, precisa quali informazioni sono richieste, fissa un termine entro il quale le informazioni devono essere fornite e indica le sanzioni pecuniarie previste all'articolo 101 in caso di comunicazione di informazioni inesatte, incomplete o fuorvianti.

5. Il fornitore del modello di IA per finalità generali in questione o il suo rappresentante fornisce le informazioni richieste. Nel caso di persone giuridiche, società o imprese, o qualora il fornitore non abbia personalità giuridica, le persone autorizzate a rappresentarle per legge o in virtù del loro statuto forniscono le informazioni richieste per conto del fornitore del modello di IA per finalità generali in questione. Gli avvocati debitamente incaricati possono fornire le informazioni per conto dei loro clienti. I clienti restano tuttavia pienamente responsabili se le informazioni fornite sono incomplete, inesatte o fuorvianti.

Articolo 92

Potere di effettuare valutazioni

1. L'ufficio per l'IA, previa consultazione del consiglio per l'IA, può effettuare valutazioni del modello di IA per finalità generali in questione:

a) per valutare la conformità del fornitore agli obblighi previsti dal presente regolamento, qualora le informazioni raccolte a norma dell'articolo 91 siano insufficienti; o

b) per indagare sui rischi sistemici a livello dell'Unione dei modelli di IA per finalità generali con rischio sistemico, in particolare a seguito di una segnalazione qualificata del gruppo di esperti scientifici conformemente all'articolo 90, paragrafo 1, lettera a).

2. La Commissione può decidere di nominare esperti indipendenti incaricati di effettuare valutazioni per suo conto, anche provenienti dal gruppo di esperti scientifici istituito a norma dell'articolo 68. Gli esperti indipendenti nominati per tale compito soddisfano i criteri di cui all'articolo 68, paragrafo 2.

3. Ai fini del paragrafo 1, la Commissione può chiedere l'accesso al modello di IA per finalità generali in questione attraverso API o altri mezzi e strumenti tecnici adeguati, compreso il codice sorgente.

4. La richiesta di accesso indica la base giuridica, lo scopo e i motivi della richiesta e fissa il termine entro il quale deve essere fornito l'accesso e le sanzioni pecuniarie previste all'articolo 101 in caso di mancata fornitura dell'accesso.

5. I fornitori del modello di IA per finalità generali in questione o il loro rappresentante forniscono le informazioni richieste. Nel caso di persone giuridiche, società o imprese, o qualora i fornitori non abbiano personalità giuridica, le persone autorizzate a rappresentarli per legge o in virtù del loro statuto, forniscono l'accesso richiesto per conto del fornitore del modello di IA per finalità generali in questione.

6. La Commissione adotta atti di esecuzione che stabiliscono le modalità dettagliate e le condizioni per le valutazioni, comprese le modalità dettagliate per la partecipazione di esperti indipendenti, nonché la procedura per la loro selezione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

7. Prima di richiedere l'accesso al modello di IA per finalità generali in questione, l'ufficio per l'IA può avviare un dialogo strutturato con il fornitore del modello di IA per finalità generali al fine di raccogliere maggiori informazioni sulle prove interne del modello, sulle garanzie interne per prevenire rischi sistemici e su altre procedure e misure interne che il fornitore ha adottato per attenuare tali rischi.

Articolo 93

Potere di richiedere misure

1. Se necessario e opportuno, la Commissione può chiedere ai fornitori di:

a) adottare misure adeguate per adempiere gli obblighi di cui agli articoli 53 e 54;

b) attuare misure di attenuazione se la valutazione effettuata conformemente all'articolo 92 ha suscitato un timore serio e comprovato di un rischio sistemico a livello dell'Unione;

c) limitare la messa a disposizione sul mercato, ritirare o richiamare il modello.

2. Prima di richiedere una misura, l'ufficio per l'IA può avviare un dialogo strutturato con il fornitore del modello di IA per finalità generali.

3. Se, durante il dialogo strutturato di cui al paragrafo 2, il fornitore del modello di IA per finalità generali con rischio sistemico si assume impegni relativi all'attuazione di misure di attenuazione per far fronte a un rischio sistemico a livello dell'Unione, la Commissione può, mediante decisione, rendere tali impegni vincolanti e dichiarare che non vi sono ulteriori motivi di intervento.

Articolo 94

Diritti procedurali degli operatori economici del modello di IA per finalità generali

L'articolo 18 del regolamento (UE) 2019/1020 si applica mutatis mutandis ai fornitori del modello di IA per finalità generali, fatti salvi i diritti procedurali più specifici previsti dal presente regolamento.

CAPO X

CODICI DI CONDOTTA E ORIENTAMENTI

Articolo 95

Codici di condotta per l'applicazione volontaria di requisiti specifici

1. L'ufficio per l'IA e gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta, compresi i relativi meccanismi di governance, intesi a promuovere l'applicazione volontaria ai sistemi di IA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti di cui al capo III, sezione 2, tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore che consentono l'applicazione di tali requisiti.

2. L'ufficio per l'IA e gli Stati membri agevolano l'elaborazione di codici di condotta relativi all'applicazione volontaria, anche da parte dei deployer, di requisiti specifici a tutti i sistemi di IA, sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi, compresi elementi quali, a titolo puramente esemplificativo:

a) gli elementi applicabili previsti negli orientamenti etici dell'Unione per un'IA affidabile;

b) la valutazione e la riduzione al minimo dell'impatto dei sistemi di IA sulla sostenibilità ambientale, anche per quanto riguarda la programmazione efficiente sotto il profilo energetico e le tecniche per la progettazione, l'addestramento e l'uso efficienti dell'IA;

c) la promozione dell'alfabetizzazione in materia di IA, in particolare quella delle persone che si occupano dello sviluppo, del funzionamento e dell'uso dell'IA;

d) la facilitazione di una progettazione inclusiva e diversificata dei sistemi di IA, anche attraverso la creazione di gruppi di sviluppo inclusivi e diversificati e la promozione della partecipazione dei portatori di interessi a tale processo;

e) la valutazione e la prevenzione dell'impatto negativo dei sistemi di IA sulle persone vulnerabili o sui gruppi di persone vulnerabili, anche per quanto riguarda l'accessibilità per le persone con disabilità, nonché sulla parità di genere.

3. I codici di condotta possono essere elaborati da singoli fornitori o deployer di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione di qualsiasi portatore di interessi e delle sue organizzazioni rappresentative, comprese le organizzazioni della società civile e il mondo accademico. 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 dei codici di condotta, l'ufficio per l'IA e gli Stati membri tengono conto degli interessi e delle esigenze specifici delle PMI, comprese le start-up.

Articolo 96

Orientamenti della Commissione sull'attuazione del regolamento

1. La Commissione elabora orientamenti sull'attuazione pratica del presente regolamento, in particolare per quanto riguarda:

a) l'applicazione dei requisiti e degli obblighi di cui agli articoli da 8 a 15 e all'articolo 25;

b) le pratiche vietate di cui all'articolo 5;

c) l'attuazione pratica delle disposizioni relative alla modifica sostanziale;

d) l'attuazione pratica degli obblighi di trasparenza di cui all'articolo 50;

e) informazioni dettagliate sulla relazione del presente regolamento con la normativa di armonizzazione dell'Unione elencata nell'allegato I, nonché con altre disposizioni pertinenti di diritto dell'Unione, anche per quanto riguarda la coerenza nella loro applicazione;

f) l'applicazione della definizione di sistema di IA di cui all'articolo 3, punto 1).

Quando pubblica tali orientamenti, la Commissione presta particolare attenzione alle esigenze delle PMI, comprese le start-up, delle autorità pubbliche locali e dei settori maggiormente interessati dal presente regolamento.

Gli orientamenti di cui al primo comma del presente paragrafo tengono debitamente conto dello stato dell'arte generalmente riconosciuto in materia di IA, nonché delle pertinenti norme armonizzate e specifiche comuni di cui agli articoli 40 e 41, o delle norme armonizzate o specifiche tecniche stabilite a norma della normativa di armonizzazione dell'Unione.

2. Su richiesta degli Stati membri o dell'ufficio per l'IA, o di propria iniziativa, la Commissione aggiorna gli orientamenti adottati quando lo ritiene necessario.

CAPO XI

DELEGA DI POTERE E PROCEDURA DI COMITATO

Articolo 97

Esercizio della delega

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

2. Il potere di adottare atti delegati di cui all'articolo 6, paragrafi 6 e 7, all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, all'articolo 47, paragrafo 5, all'articolo 51, paragrafo 3, all'articolo 52, paragrafo 4, e all'articolo 53, paragrafi 5 e 6, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 1º agosto 2024. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 6, paragrafi 6 e 7, all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, all'articolo 47, paragrafo 5, all'articolo 51, paragrafo 3, all'articolo 52, paragrafo 4, e all'articolo 53, paragrafi 5 e 6, 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. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

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

6. Qualsiasi atto delegato adottato a norma dell'articolo 6, paragrafi 6 o 7, dell'articolo 7, paragrafi 1 o 3, dell'articolo 11, paragrafo 3, dell'articolo 43, paragrafi 5 o 6, dell'articolo 47, paragrafo 5, dell'articolo 51, paragrafo 3, dell'articolo 52, paragrafo 4, o dell'articolo 53, paragrafi 5 o 6, 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 98

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.

CAPO XII

SANZIONI

Articolo 99

Sanzioni

1. In conformità dei termini e delle condizioni di cui al presente regolamento, gli Stati membri stabiliscono le norme relative alle sanzioni e alle altre misure di esecuzione, che possono includere anche avvertimenti e misure non pecuniarie, applicabili in caso di violazione del presente regolamento da parte degli operatori, e adottano tutte le misure necessarie per garantirne un'attuazione corretta ed efficace, tenendo conto degli orientamenti emanati dalla Commissione a norma dell'articolo 96. Le sanzioni previste sono effettive, proporzionate e dissuasive. Esse tengono conto degli interessi delle PMI, comprese le start-up, e della loro sostenibilità economica.

2. Gli Stati membri notificano alla Commissione, senza indugio e al più tardi entro la data di entrata in applicazione, le norme relative alle sanzioni e le altre misure di esecuzione di cui al paragrafo 1, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

3. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 35 000 000 EUR o, se l'autore del reato è un'impresa, fino al 7 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4. La non conformità a qualsiasi delle seguenti disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 EUR o, se l'autore del reato è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi dei fornitori a norma dell'articolo 16;

b) gli obblighi dei rappresentati autorizzati a norma dell'articolo 22;

c) gli obblighi degli importatori a norma dell'articolo 23;

d) gli obblighi dei distributori a norma dell'articolo 24;

e) gli obblighi dei deployer a norma dell'articolo 26;

f) i requisiti e gli obblighi degli organismi notificati a norma dell'articolo 31, dell'articolo 33, paragrafi 1, 3 e 4, o dell'articolo 34;

g) gli obblighi di trasparenza per i fornitori e i deployers a norma dell'articolo 50.

5. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni amministrative pecuniarie fino a 7 500 000 EUR o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

6. Nel caso delle PMI, comprese le start-up, ciascuna sanzione pecuniaria di cui al presente articolo è pari al massimo alle percentuali o all'importo di cui ai paragrafi 3, 4 e 5, se inferiore.

7. 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, se del caso, si tiene in considerazione quanto segue:

a) la natura, la gravità e la durata della violazione e delle sue conseguenze, tenendo in considerazione la finalità del sistema di IA, nonché, ove opportuno, il numero di persone interessate e il livello del danno da esse subito;

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

c) se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento;

d) le dimensioni, il fatturato annuo e la quota di mercato dell'operatore che ha commesso la violazione;

e) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione;

f) il grado di cooperazione con le autorità nazionali competenti al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) il grado di responsabilità dell'operatore tenendo conto delle misure tecniche e organizzative attuate;

h) il modo in cui le autorità nazionali competenti sono venute a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'operatore;

i) il carattere doloso o colposo della violazione;

j) l'eventuale azione intrapresa dall'operatore per attenuare il danno subito dalle persone interessate.

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

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

10. L'esercizio dei poteri attribuiti dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e nazionale, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

11. Gli Stati membri riferiscono annualmente alla Commissione in merito alle sanzioni amministrative pecuniarie inflitte nel corso dell'anno, in conformità del presente articolo, e a eventuali controversie o procedimenti giudiziari correlati.

Articolo 100

Sanzioni amministrative pecuniarie inflitte a istituzioni, organi e organismi dell'Unione

1. Il Garante europeo della protezione dei dati può infliggere sanzioni amministrative pecuniarie alle istituzioni, agli organi 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, tenendo in considerazione la finalità del sistema di IA interessato, nonché se del caso, il numero di persone interessate e il livello del danno da esse subito;

b) il grado di responsabilità dell'istituzione, dell'organo o dell'organismo dell'Unione, tenendo conto delle misure tecniche e organizzative da essi attuate;

c) qualsiasi azione intrapresa dall'istituzione, dall'organo o dall'organismo dell'Unione per attenuare il danno subito dalle persone interessate;

d) il grado di 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'organo o dell'organismo dell'Unione interessato in relazione allo stesso tema;

e) eventuali precedenti violazioni analoghe commesse dall'istituzione, dall'organo o dall'organismo dell'Unione;

f) il modo in cui il Garante europeo della protezione dei dati è venuto a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'istituzione, dall'organo o dall'organismo dell'Unione;

g) il bilancio annuale dell'istituzione, dell'organo o dell'organismo dell'Unione.

2. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 1 500 000 EUR.

3. La non conformità del sistema di IA ai requisiti o agli obblighi a norma del presente regolamento, diversi da quelli previsti all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 750 000 EUR.

4. Prima di adottare qualsiasi decisione a norma del presente articolo, il Garante europeo della protezione dei dati dà all'istituzione, all'organo 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 contribuiscono al bilancio generale dell'Unione. Le sanzioni pecuniarie non pregiudicano l'effettivo funzionamento dell'istituzione, dell'organo o dell'organismo dell'Unione sanzionato.

7. Il Garante europeo della protezione dei dati notifica annualmente alla Commissione le sanzioni amministrative pecuniarie da esso inflitte a norma del presente articolo e qualsiasi controversia o procedimento giudiziario che ha avviato.

Articolo 101

Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali

1. La Commissione può infliggere ai fornitori di modelli di IA per finalità generali sanzioni pecuniarie non superiori al 3 % del fatturato mondiale annuo totale dell'esercizio precedente o a 15 000 000 EUR, se superiore, ove essa rilevi che il fornitore, intenzionalmente o per negligenza:

a) ha violato le pertinenti disposizioni del presente regolamento;

b) non ha ottemperato a una richiesta di documento o di informazioni a norma dell'articolo 91 o ha fornito informazioni inesatte, incomplete o fuorvianti;

c) non ha ottemperato a una misura richiesta a norma dell'articolo 93;

d) non ha messo a disposizione della Commissione l'accesso al modello di IA per finalità generali o al modello di IA per finalità generali con rischio sistemico al fine di effettuare una valutazione a norma dell'articolo 92.

Nel determinare l'importo della sanzione pecuniaria o della penalità di mora, si tengono in considerazione la natura, la gravità e la durata della violazione, tenendo debitamente conto dei principi di proporzionalità e di adeguatezza. La Commissione tiene conto anche degli impegni assunti in conformità dell'articolo 93, paragrafo 3, o assunti nei pertinenti codici di condotta in conformità dell'articolo 56.

2. Prima di adottare la decisione a norma del paragrafo 1, la Commissione comunica le sue constatazioni preliminari al fornitore del modello di IA per finalità generali o del modello di IA e gli dà l'opportunità di essere ascoltato.

3. Le sanzioni pecuniarie inflitte in conformità del presente articolo sono effettive, proporzionate e dissuasive.

4. Le informazioni in merito alle sanzioni pecuniarie inflitte a norma del presente articolo sono altresì comunicate al consiglio per l'IA, se del caso.

5. La Corte di giustizia dell'Unione europea ha competenza giurisdizionale anche di merito per esaminare le decisioni mediante le quali la Commissione ha fissato una sanzione pecuniaria a norma del presente articolo. Essa può estinguere, ridurre o aumentare la sanzione pecuniaria inflitta.

6. La Commissione adotta atti di esecuzione contenenti modalità dettagliate per i procedimenti e garanzie procedurali in vista dell'eventuale adozione di decisioni a norma del paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

CAPO XIII

DISPOSIZIONI FINALI

Articolo 102

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) 2024/1689 o del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 o del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 103

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) 2024/1689 del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 104

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) 2024/1689 del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 105

Modifica della direttiva 2014/90/UE

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

«5. Per i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/1689 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 capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)».

Articolo 106

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) 2024/1689 del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 107

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) 2024/1689 del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 108

Modifiche 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) 2024/1689 del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento(UE) 2024/… del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).»;

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) 2024/1689, si tiene conto dei requisiti di cui al capo III, sezione 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) 2024/1689, si tiene conto dei requisiti di cui al capo III, sezione 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) 2024/1689, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.»;

5) all'articolo 57 è aggiunto il comma 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) 2024/1689, si tiene conto dei requisiti di cui al capo III, sezione 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) 2024/1689, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.».

Articolo 109

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) 2024/1689 del Parlamento europeo e del Consiglio (*), si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

(*) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 110

Modifica della direttiva (UE) 2020/1828

All'allegato I della direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio ([58]) è aggiunto il punto seguente:

«68) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio. del 13 giugno 2024. che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Articolo 111

Sistemi di IA già immessi sul mercato o messi in servizio e modelli di IA per finalità generali già immessi sul mercato

1. Fatta salva l'applicazione dell'articolo 5 di cui all'articolo 113, paragrafo 3, lettera a), i sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'allegato X che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2027 sono resi conformi al presente regolamento entro il 31 dicembre 2030.

Si tiene conto dei requisiti di cui al presente regolamento nella valutazione di ciascun sistema IT su larga scala istituito dagli atti giuridici elencati nell'allegato X da effettuare come previsto in tali atti giuridici e ove tali atti giuridici siano sostituiti o modificati.

2. Fatta salva l'applicazione dell'articolo 5 di cui all'articolo 113, paragrafo 3, lettera a), il presente regolamento si applica agli operatori dei sistemi di IA ad alto rischio, diversi dai sistemi di cui al paragrafo 1 del presente articolo, che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2026, solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione. In ogni caso, i fornitori e deployers di sistemi di IA ad alto rischio destinati a essere utilizzati dalle autorità pubbliche adottano le misure necessarie per conformarsi ai requisiti e agli obblighi del presente regolamento entro il 2 agosto 2030.

3. I fornitori di modelli di IA per finalità generali che sono stati immessi sul mercato prima del 2 agosto 2025 adottano le misure necessarie per conformarsi agli obblighi di cui al presente regolamento entro 2 agosto 2027.

([58]) Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (GU L 409 del 4.12.2020, pag. 1).

Articolo 112

Valutazione e riesame

1. La Commissione valuta la necessità di modificare l'elenco stabilito nell'allegato III e l'elenco di pratiche di IA vietate di cui all'articolo 5 una volta all'anno dopo l'entrata in vigore del presente regolamento e fino al termine del periodo della delega di potere di cui all'articolo 97. La Commissione trasmette i risultati della valutazione al Parlamento europeo e al Consiglio.

2. Entro il 2 agosto 2028 e successivamente ogni quattro anni, la Commissione valuta e riferisce al Parlamento europeo e al Consiglio in merito a quanto segue:

a) la necessità di modifiche che amplino le rubriche settoriali esistenti o ne aggiungano di nuove all'allegato III;

b) modifiche dell'elenco dei sistemi di IA che richiedono ulteriori misure di trasparenza di cui all'articolo 50;

c) modifiche volte a migliorare l'efficacia del sistema di supervisione e di governance.

3. Entro il 2 agosto 2029 e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento. La relazione include una valutazione in merito alla struttura di esecuzione e all'eventuale necessità di un'agenzia dell'Unione che ponga rimedio alle carenze individuate. Sulla base dei risultati, la relazione è corredata, se del caso, di una proposta di modifica del presente regolamento. Le relazioni sono rese pubbliche.

4. Le relazioni di cui al paragrafo 2 dedicano particolare attenzione agli aspetti seguenti:

a) lo stato delle risorse finanziarie, tecniche 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 99, paragrafo 1, applicate dagli Stati membri in caso di violazione del presente regolamento;

c) le norme armonizzate adottate e le specifiche comuni elaborate a sostegno del presente regolamento;

d) il numero di imprese che entrano sul mercato dopo l'entrata in vigore del presente regolamento e quante di esse sono PMI.

5. Entro il 2 agosto 2028, la Commissione valuta il funzionamento dell'ufficio per l'IA, se all'ufficio per l'IA siano stati conferiti poteri e competenze adeguati per svolgere i suoi compiti e se sia pertinente e necessario per la corretta attuazione ed esecuzione del presente regolamento potenziare l'ufficio per l'IA e le sue competenze di esecuzione e aumentarne le risorse. La Commissione trasmette una relazione sulla valutazione di tale ufficio per l'IA al Parlamento europeo e al Consiglio.

6. Entro il 2 agosto 2028 e successivamente ogni quattro anni, la Commissione presenta una relazione sull'esame dei progressi compiuti riguardo allo sviluppo di prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico di modelli di IA per finalità generali e valuta la necessità di ulteriori misure o azioni, comprese misure o azioni vincolanti. La relazione è presentata al Parlamento europeo e al Consiglio ed è resa pubblica.

7. Entro il 2 agosto 2028 e successivamente ogni tre anni la Commissione valuta l'impatto e l'efficacia dei codici di condotta volontari per la promozione dell'applicazione dei requisiti di cui al capo III, sezione 2, per i sistemi di IA diversi dai sistemi di IA ad alto rischio ed eventualmente di altri requisiti supplementari per i sistemi di IA diversi dai sistemi di IA ad alto rischio, anche per quanto riguarda la sostenibilità ambientale.

8. Ai fini dei paragrafi da 1 a 7, il consiglio per l'IA, gli Stati membri e le autorità nazionali competenti forniscono alla Commissione informazioni su sua richiesta e senza indebito ritardo.

9. Nello svolgere le valutazioni e i riesami di cui ai paragrafi da 1 a 7, la Commissione tiene conto delle posizioni e delle conclusioni del consiglio per l'IA, del Parlamento europeo e del Consiglio, nonché di altri organismi o fonti pertinenti.

10. Se necessario, la Commissione presenta opportune proposte di modifica del presente regolamento tenendo conto, in particolare, degli sviluppi delle tecnologie e dell'effetto dei sistemi di IA sulla salute, sulla sicurezza e sui diritti fondamentali, nonché alla luce dei progressi della società dell'informazione.

11. Per orientare le valutazioni e i riesami di cui ai paragrafi da 1 a 7, l'Ufficio per l'IA si impegna a sviluppare una metodologia obiettiva e partecipativa per la valutazione dei livelli di rischio basata sui criteri definiti negli articoli pertinenti e l'inclusione di nuovi sistemi:

a) nell'elenco stabilito nell'allegato III, compreso l'ampliamento delle rubriche settoriali esistenti o l'aggiunta di nuove rubriche settoriali in tale allegato;

b) nell'elenco delle pratiche vietate stabilite all'articolo 5; e

c) nell'elenco dei sistemi di IA che richiedono ulteriori misure di trasparenza a norma dell'articolo 50.

12. Eventuali modifiche al presente regolamento a norma del paragrafo 10, o i pertinenti atti delegati o di esecuzione, che riguardano la normativa settoriale di armonizzazione dell'Unione elencata nell'allegato I, sezione B, tengono conto delle specificità normative di ciascun settore e dei vigenti meccanismi di governance, valutazione della conformità ed esecuzione e delle autorità da essi stabilite.

13. Entro il 2 agosto 2031, la Commissione effettua una valutazione dell'esecuzione del presente regolamento e riferisce in merito al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo, tenendo conto dei primi anni di applicazione del presente regolamento. Sulla base dei risultati, la relazione è accompagnata, se del caso, da una proposta di modifica del presente regolamento in relazione alla struttura di esecuzione e alla necessità di un'agenzia dell'Unione che ponga rimedio alle carenze individuate.

Articolo 113

Entrata in vigore e applicazione

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

Si applica a decorrere dal 2 agosto 2026.

Tuttavia:

a) I capi I e II si applicano a decorrere dal 2 febbraio 2025;

b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101;

c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027.

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

Fatto a Bruxelles, il 13 giugno 2024

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
R. METSOLA	M. MICHEL

ALLEGATO I

Elenco della normativa di armonizzazione dell'Unione

Sezione A. Elenco della normativa di armonizzazione dell'Unione in base al nuovo quadro legislativo

1. Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24) [abrogata dal regolamento sui prodotti macchina];

2. direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli (GU L 170 del 30.6.2009, pag. 1);

3. direttiva 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarcazioni da diporto e alle moto d'acqua e che abroga la direttiva 94/25/CE (GU L 354 del 28.12.2013, pag. 90);

4. direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori (GU L 96 del 29.3.2014, pag. 251);

5. direttiva 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva (GU L 96 del 29.3.2014, pag. 309);

6. direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62);

7. direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione (GU L 189 del 27.6.2014, pag. 164);

8. regolamento (UE) 2016/424 del Parlamento europeo e del Consiglio, del 9 marzo 2016, relativo agli impianti a fune e che abroga la direttiva 2000/9/CE (GU L 81 del 31.3.2016, pag. 1);

9. regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio (GU L 81 del 31.3.2016, pag. 51);

10. regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la direttiva 2009/142/CE (GU L 81 del 31.3.2016, pag. 99);

11. 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);

12. 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).

Sezione B – Elenco di altre normative di armonizzazione dell'Unione

13. 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);

14. 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);

15. 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);

16. 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);

17. 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);

18. 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);

19. 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);

20. 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), nella misura in cui si tratta della progettazione, della produzione e dell'immissione sul mercato degli aeromobili di cui all'articolo 2, paragrafo 1, lettere a) e b), relativamente agli aeromobili senza equipaggio e ai loro motori, eliche, parti e dispositivi di controllo remoto.

ALLEGATO II

Elenco dei reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii)

Reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii):

— terrorismo,

— tratta di esseri umani,

— sfruttamento sessuale di minori e pornografia minorile,

— traffico illecito di stupefacenti o sostanze psicotrope,

— traffico illecito di armi, munizioni ed esplosivi,

— omicidio volontario, lesioni gravi,

— traffico illecito di organi e tessuti umani,

— traffico illecito di materie nucleari e radioattive,

— sequestro, detenzione illegale e presa di ostaggi,

— reati che rientrano nella competenza giurisdizionale della Corte penale internazionale,

— illecita cattura di aeromobile o nave,

— violenza sessuale,

— reato ambientale,

— rapina organizzata o a mano armata,

— sabotaggio,

— partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

I sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, sono i sistemi di IA elencati in uno dei settori indicati di seguito.

1. Biometria, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

   a) i sistemi di identificazione biometrica remota.

      Non vi rientrano i sistemi di IA destinati a essere utilizzati per la verifica biometrica la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere;

   b) i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti basati sulla deduzione di tali attributi o caratteristiche;

   c) i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni.

2. Infrastrutture critiche: i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità.

3. Istruzione e formazione professionale:

   a) i sistemi di IA destinati a essere utilizzati per determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli;

   b) i sistemi di IA destinati a essere utilizzati per valutare i risultati dell'apprendimento, anche nei casi in cui tali risultati sono utilizzati per orientare il processo di apprendimento di persone fisiche in istituti di istruzione o formazione professionale a tutti i livelli;

   c) i sistemi di IA destinati a essere utilizzati per valutare il livello di istruzione adeguato che una persona riceverà o a cui potrà accedere, nel contesto o all'interno di istituti di istruzione o formazione professionale a tutti i livelli;

   d) i sistemi di IA destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli.

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

   a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati;

   b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

5. Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi:

   a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;

   b) i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie;

   c) i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie;

d) i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza;

6. Attività di contrasto, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto o per loro conto, per determinare il rischio per una persona fisica di diventare vittima di reati;

b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, come poligrafi e strumenti analoghi;

c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;

d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per determinare il rischio di commissione del reato o di recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;

e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per effettuare la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati.

7. Migrazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, o per loro conto, o da istituzioni, organi e organismi dell'Unione, come poligrafi o strumenti analoghi;

b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per valutare un rischio (compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro;

c) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto o di permesso di soggiorno e per i relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status, compresa le valutazioni correlate dell'affidabilità degli elementi probatori;

d) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, o da istituzioni, organi e organismi dell'Unione, nel contesto della migrazione, dell'asilo o della gestione del controllo delle frontiere, al fine di individuare, riconoscere o identificare persone fisiche, a eccezione della verifica dei documenti di viaggio.

8. Amministrazione della giustizia e processi democratici:

a) i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie;

b) i sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum. Sono esclusi i sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.

ALLEGATO IV

Documentazione tecnica di cui all'articolo 11, paragrafo 1

La documentazione tecnica di cui all'articolo 11, paragrafo 1, deve includere almeno le seguenti informazioni, a seconda dell'applicabilità al pertinente sistema di IA.

1. Una descrizione generale del sistema di IA comprendente:

   a) la finalità prevista, il nome del fornitore e la versione del sistema che indichi il suo rapporto con le versioni precedenti;

   b) il modo in cui il sistema di IA interagisce o può essere utilizzato per interagire con hardware o software, compresi altri sistemi di IA, che non fanno parte del sistema di IA stesso, ove applicabile;

   c) le versioni dei pertinenti software o firmware e qualsiasi requisito relativo all'aggiornamento della versione;

   d) la descrizione di tutte le forme in cui il sistema di IA è immesso sul mercato o messo in servizio, quali pacchetti software incorporati nell'hardware, download o API;

   e) la descrizione dell'hardware su cui è destinato a operare il sistema di IA;

   f) se il sistema di IA è un componente di prodotti, le fotografie o le illustrazioni che mostrino le caratteristiche esterne, la marcatura e il layout interno di tali prodotti;

   g) una descrizione di base dell'interfaccia utente fornita al deployer;

   h) le istruzioni per l'uso destinate al deployer e una descrizione di base dell'interfaccia utente fornita al deployer, se applicabile.

2. Una descrizione dettagliata degli elementi del sistema di IA e del processo relativo al suo sviluppo, compresi:

   a) i metodi applicati e le azioni eseguite per lo sviluppo del sistema di IA, compresi, ove opportuno, il ricorso a sistemi o strumenti preaddestrati forniti da terzi e il modo in cui sono stati utilizzati, integrati o modificati dal fornitore;

   b) le specifiche di progettazione del sistema, vale a dire la logica generale del sistema di IA e degli algoritmi; le principali scelte di progettazione, comprese le motivazioni e le ipotesi formulate, anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato; le principali scelte di classificazione; gli aspetti che il sistema è progettato per ottimizzare e la pertinenza dei diversi parametri; la descrizione dell'output atteso e della qualità dell'output del sistema; le decisioni in merito a eventuali compromessi posti in essere con riguardo alle soluzioni tecniche adottate per soddisfare i requisiti di cui al capo III, sezione 2;

   c) la descrizione dell'architettura del sistema che spiega in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo; le risorse computazionali utilizzate per sviluppare, addestrare, sottoporre a prova e convalidare il sistema di IA;

   d) ove pertinente, i requisiti in materia di dati mediante schede tecniche che descrivono le metodologie e le tecniche di addestramento e i set di dati di addestramento utilizzati, comprese una descrizione generale di tali set di dati e le informazioni sulla loro origine, sul loro ambito di applicazione e sulle loro principali caratteristiche; le modalità di ottenimento e di selezione dei dati; le procedure di etichettatura, ad esempio per l'apprendimento supervisionato, e le metodologie di pulizia dei dati, ad esempio il rilevamento di valori anomali (outlier);

   e) la valutazione delle misure di sorveglianza umana necessarie in conformità dell'articolo 14, compresa una valutazione delle misure tecniche necessarie per facilitare l'interpretazione degli output dei sistemi di IA da parte dei deployer, in conformità dell'articolo 13, paragrafo 3, lettera d);

   f) ove applicabile, una descrizione dettagliata delle modifiche predeterminate del sistema di IA e delle sue prestazioni, unitamente a tutte le informazioni pertinenti relative alle soluzioni tecniche adottate per garantire la conformità costante del sistema di IA ai requisiti pertinenti di cui al capo III, sezione 2;

   g) le procedure di convalida e di prova utilizzate, comprese le informazioni sui dati di convalida e di prova utilizzati e sulle loro principali caratteristiche; le metriche utilizzate per misurare l'accuratezza, la robustezza e la conformità ad altri requisiti pertinenti di cui al capo III, sezione 2, nonché gli impatti potenzialmente discriminatori; i log delle prove e tutte le relazioni di prova corredate di data e firma delle persone responsabili, anche per quanto riguarda le modifiche predeterminate di cui alla lettera f);

h) le misure di cibersicurezza poste in essere.

3. Informazioni dettagliate sul monitoraggio, sul funzionamento e sul controllo del sistema di IA, in particolare per quanto riguarda: le sue capacità e limitazioni in termini di prestazioni, compresi i gradi di accuratezza relativi a determinate persone o determinati gruppi di persone sui quali il sistema è destinato a essere utilizzato e il livello di accuratezza complessivo atteso in relazione alla finalità prevista del sistema; i prevedibili risultati indesiderati e fonti di rischio per la salute, la sicurezza e i diritti fondamentali, nonché di rischio di discriminazione in considerazione della finalità prevista del sistema di IA; le misure di sorveglianza umana necessarie in conformità dell'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte dei deployer; le specifiche relative ai dati di input, se del caso.

4. Una descrizione dell'adeguatezza delle metriche di prestazione per il sistema di IA specifico.

5. Una descrizione dettagliata del sistema di gestione dei rischi in conformità dell'articolo 9.

6. Una descrizione delle modifiche pertinenti apportate dal fornitore al sistema durante il suo ciclo di vita.

7. Un elenco delle norme armonizzate applicate integralmente o in parte i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*; nei casi in cui tali norme armonizzate non sono state applicate, una descrizione dettagliata delle soluzioni adottate per soddisfare i requisiti di cui al capo III, sezione 2, compreso un elenco delle altre norme e specifiche tecniche pertinenti applicate.

8. Una copia della dichiarazione di conformità UE di cui all'articolo 47.

9. Una descrizione dettagliata del sistema predisposto per valutare le prestazioni del sistema di IA nella fase successiva all'immissione sul mercato in conformità dell'articolo 72, compreso il piano di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72, paragrafo 3.

ALLEGATO V

Dichiarazione di conformità UE

La dichiarazione di conformità UE di cui all'articolo 47 deve contenere tutte le informazioni seguenti:

1. il nome e il tipo del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;
2. il nome e l'indirizzo del fornitore o, ove applicabile, del suo rappresentante autorizzato;
3. un'attestazione secondo cui la dichiarazione di conformità UE di cui all'articolo 47 è rilasciata sotto la responsabilità esclusiva del fornitore;
4. un'attestazione secondo cui il sistema di IA è conforme al presente regolamento e, ove applicabile, a qualsiasi altra disposizione pertinente del diritto dell'Unione che preveda il rilascio di una dichiarazione di conformità UE di cui all'articolo 47;
5. se un sistema di IA comporta il trattamento di dati personali, una dichiarazione attestante che tale sistema di IA è conforme ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680;
6. i riferimenti alle pertinenti norme armonizzate utilizzate o a qualsiasi altra specifica comune in relazione alla quale è dichiarata la conformità;
7. ove applicabile, il nome e il numero di identificazione dell'organismo notificato, una descrizione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato;
8. il luogo e la data di rilascio della dichiarazione, il nome e la funzione della persona che firma la dichiarazione nonché un'indicazione della persona a nome o per conto della quale ha firmato, e la firma.

ALLEGATO VI

Procedura di valutazione della conformità basata sul controllo interno

1. La procedura di valutazione della conformità basata sul controllo interno è la procedura di valutazione della conformità basata sui punti 2, 3 e 4.
2. Il fornitore verifica la conformità del sistema di gestione della qualità istituito ai requisiti di cui all'articolo 17.
3. Il fornitore esamina le informazioni contenute nella documentazione tecnica al fine di valutare la conformità del sistema di IA ai pertinenti requisiti essenziali di cui al capo III, sezione 2.
4. Il fornitore verifica inoltre che il processo di progettazione e sviluppo del sistema di IA e il monitoraggio successivo alla sua immissione sul mercato di cui all'articolo 72 siano coerenti con la documentazione tecnica.

ALLEGATO VII

Conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica

1. Introduzione

La conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica scaturisce dalla procedura di valutazione della conformità di cui ai punti da 2 a 5.

2. Aspetti generali

Il sistema di gestione della qualità approvato per la progettazione, lo sviluppo e la prova dei sistemi di IA a norma dell'articolo 17 deve essere esaminato conformemente al punto 3 e deve essere soggetto alla vigilanza di cui al punto 5. La documentazione tecnica del sistema di IA deve essere esaminata conformemente al punto 4.

3. Sistema di gestione della qualità

3.1. La domanda presentata dal fornitore deve comprendere:

a) il nome e l'indirizzo del fornitore e, nel caso in cui la domanda sia presentata da un rappresentante autorizzato, anche il nome e l'indirizzo di quest'ultimo;

b) l'elenco dei sistemi di IA cui si applica lo stesso sistema di gestione della qualità;

c) la documentazione tecnica di ciascuno dei sistemi di IA cui si applica lo stesso sistema di gestione della qualità;

d) la documentazione relativa al sistema di gestione della qualità che deve contemplare tutti gli aspetti elencati all'articolo 17;

e) una descrizione delle procedure vigenti per garantire che il sistema di gestione della qualità rimanga adeguato ed efficace;

f) una dichiarazione scritta attestante che la stessa domanda non è stata presentata a nessun altro organismo notificato.

3.2. Il sistema di gestione della qualità deve essere valutato dall'organismo notificato, che deve stabilire se soddisfa i requisiti di cui all'articolo 17.

La decisione deve essere notificata al fornitore o al suo rappresentante autorizzato.

Tale notifica deve indicare le conclusioni della valutazione del sistema di gestione della qualità e la decisione di valutazione motivata.

3.3. Il sistema di gestione della qualità approvato deve continuare a essere attuato e mantenuto dal fornitore in modo da rimanere adeguato ed efficiente.

3.4. Il fornitore deve portare all'attenzione dell'organismo notificato qualsiasi modifica prevista del sistema di gestione della qualità approvato o dell'elenco dei sistemi di IA cui si applica tale sistema.

Le modifiche proposte devono essere esaminate dall'organismo notificato, che deve decidere se il sistema di gestione della qualità modificato continua a soddisfare i requisiti di cui al punto 3.2 o se è necessaria una nuova valutazione.

L'organismo notificato deve notificare al fornitore la propria decisione. Tale notifica deve indicare le conclusioni dell'esame e la decisione di valutazione motivata.

4. Controllo della documentazione tecnica.

4.1. Oltre alla domanda di cui al punto 3, il fornitore deve presentare una domanda a un organismo notificato di propria scelta per la valutazione della documentazione tecnica relativa al sistema di IA che il fornitore intende immettere sul mercato o mettere in servizio e cui si applica il sistema di gestione della qualità di cui al punto 3.

4.2. La domanda deve comprendere:

a) il nome e l'indirizzo del fornitore;

b) una dichiarazione scritta attestante che la stessa domanda non è stata presentata a nessun altro organismo notificato;

c) la documentazione tecnica di cui all'allegato IV.

4.3. La documentazione tecnica deve essere esaminata dall'organismo notificato. Se del caso e nei limiti di quanto necessario per lo svolgimento dei suoi compiti, all'organismo notificato deve essere concesso pieno accesso ai set di dati di addestramento, convalida e prova utilizzati, anche, ove opportuno e fatte salve le garanzie di sicurezza, attraverso API o altri mezzi e strumenti tecnici pertinenti che consentano l'accesso remoto.

4.4. Nell'esaminare la documentazione tecnica, l'organismo notificato può chiedere al fornitore di presentare elementi probatori supplementari o di eseguire ulteriori prove per consentire una corretta valutazione della conformità del sistema di IA ai requisiti di cui al capo III, sezione 2. Qualora non sia soddisfatto delle prove effettuate dal fornitore, l'organismo notificato stesso deve effettuare prove adeguate, a seconda dei casi.

4.5. Ove necessario per valutare la conformità del sistema di IA ad alto rischio ai requisiti di cui al capo III, sezione 2, dopo che tutti gli altri mezzi ragionevoli per verificare la conformità sono stati esauriti e si sono rivelati insufficienti, e su richiesta motivata, anche all'organismo notificato deve essere concesso l'accesso ai modelli di addestramento e addestrati del sistema di IA, compresi i relativi parametri. Tale accesso è soggetto al vigente diritto dell'Unione in materia di protezione della proprietà intellettuale e dei segreti commerciali.

4.6. La decisione dell'organismo notificato deve essere notificata al fornitore o al suo rappresentante autorizzato. Tale notifica deve indicare le conclusioni della valutazione della documentazione tecnica e la decisione di valutazione motivata.

Se il sistema di IA è conforme ai requisiti di cui al capo III, sezione 2, l'organismo notificato deve rilasciare un certificato di valutazione della documentazione tecnica dell'Unione. Tale certificato deve indicare il nome e l'indirizzo del fornitore, le conclusioni dell'esame, le eventuali condizioni di validità e i dati necessari per identificare il sistema di IA.

Il certificato e i suoi allegati devono contenere tutte le informazioni pertinenti per consentire la valutazione della conformità del sistema di IA e il controllo del sistema di IA durante l'uso, ove applicabile.

Se il sistema di IA non è conforme ai requisiti di cui al capo III, sezione 2, l'organismo notificato deve rifiutare il rilascio di un certificato di valutazione della documentazione tecnica dell'Unione e deve informare in merito il richiedente, motivando dettagliatamente il suo rifiuto.

Se il sistema di IA non soddisfa il requisito relativo ai dati utilizzati per l'addestramento, sarà necessario addestrare nuovamente il sistema di IA prima di presentare domanda per una nuova valutazione della conformità. In tal caso, la decisione di valutazione motivata dell'organismo notificato che rifiuta il rilascio del certificato di valutazione della documentazione tecnica dell'Unione contiene considerazioni specifiche sui dati di qualità utilizzati per addestrare il sistema di IA, in particolare sui motivi della non conformità.

4.7. Qualsiasi modifica del sistema di IA che potrebbe incidere sulla conformità ai requisiti o sulla finalità prevista dello stesso deve essere valutata dall'organismo notificato che ha rilasciato il certificato di valutazione della documentazione tecnica dell'Unione. Il fornitore deve informare tale organismo notificato quando intende introdurre una delle modifiche di cui sopra o quando viene altrimenti a conoscenza del verificarsi di tali modifiche. Le modifiche previste devono essere valutate dall'organismo notificato, che deve decidere se esse rendono necessaria una nuova valutazione della conformità a norma dell'articolo 43, paragrafo 4, o se possono essere gestite tramite un supplemento del certificato di valutazione della documentazione tecnica dell'Unione. In quest'ultimo caso, l'organismo notificato deve valutare le modifiche, notificare al fornitore la propria decisione e, in caso di approvazione delle modifiche, rilasciare a quest'ultimo un supplemento del certificato di valutazione della documentazione tecnica dell'Unione.

5. Vigilanza del sistema di gestione della qualità approvato.

5.1. La finalità della vigilanza a cura dell'organismo notificato di cui al punto 3 è garantire che il fornitore sia conforme ai termini e alle condizioni del sistema di gestione della qualità approvato.

5.2. Ai fini della valutazione, il fornitore deve consentire all'organismo notificato di accedere ai locali in cui hanno luogo la progettazione, lo sviluppo e le prove dei sistemi di IA. Il fornitore deve inoltre condividere con l'organismo notificato tutte le informazioni necessarie.

5.3. L'organismo notificato deve eseguire audit periodici per assicurarsi che il fornitore mantenga e applichi il sistema di gestione della qualità e deve trasmettere al fornitore una relazione di audit. Nel contesto di tali audit, l'organismo notificato può effettuare prove supplementari dei sistemi di IA per i quali è stato rilasciato un certificato di valutazione della documentazione tecnica dell'Unione.

ALLEGATO VIII

Informazioni da presentare all'atto della registrazione di sistemi di IA ad alto rischio in conformità dell'articolo 49

Sezione A - Informazioni che i fornitori di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 1

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA ad alto rischio che devono essere registrati a norma dell'articolo 49, paragrafo 1:

1. il nome, l'indirizzo e i dati di contatto del fornitore;
2. se le informazioni sono trasmesse da un'altra persona per conto del fornitore: il nome, l'indirizzo e i dati di contatto di tale persona;
3. il nome, l'indirizzo e i dati di contatto del rappresentante autorizzato, ove applicabile;
4. la denominazione commerciale del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;
5. la descrizione della finalità prevista del sistema di IA e dei componenti e delle funzioni supportati da tale sistema di IA;
6. una descrizione di base concisa delle informazioni utilizzate dal sistema (dati, input) e della sua logica operativa;
7. lo status del sistema di IA (sul mercato, o in servizio; non più immesso sul mercato/in servizio, richiamato);
8. il tipo, il numero e la data di scadenza del certificato rilasciato dall'organismo notificato e il nome o il numero di identificazione di tale organismo notificato, ove applicabile;
9. una copia scannerizzata del certificato di cui al punto 8, ove applicabile;
10. eventuali Stati membri dell'Unione in cui il sistema di IA è stato immesso sul mercato, messo in servizio o reso disponibile;
11. una copia della dichiarazione di conformità UE di cui all'articolo 47;
12. le istruzioni per l'uso in formato elettronico; questa informazione non deve essere fornita per i sistemi di IA ad alto rischio nei settori delle attività di contrasto o della migrazione, dell'asilo e della gestione del controllo delle frontiere di cui all'allegato III, punti 1, 6 e 7;
13. un indirizzo internet per ulteriori informazioni (facoltativo).

Sezione B - Informazioni che i fornitori di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 2

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA che devono essere registrati a norma dell'articolo 49, paragrafo 2:

1. il nome, l'indirizzo e i dati di contatto del fornitore;
2. se le informazioni sono trasmesse da un'altra persona per conto del fornitore: il nome, l'indirizzo e i dati di contatto di tale persona;
3. il nome, l'indirizzo e i dati di contatto del rappresentante autorizzato, ove applicabile;
4. la denominazione commerciale del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;
5. la descrizione della finalità prevista del sistema di IA;
6. la o le condizioni di cui all'articolo 6, paragrafo 3, sulla base delle quali il sistema di IA non è ritenuto ad alto rischio;
7. una breve sintesi dei motivi per i quali il sistema di IA non è ritenuto ad alto rischio in applicazione della procedura di cui all'articolo 6, paragrafo 3;
8. lo status del sistema di IA (sul mercato, o in servizio; non più immesso sul mercato/in servizio, richiamato);
9. eventuali Stati membri dell'Unione in cui il sistema di IA è stato immesso sul mercato, messo in servizio o reso disponibile.

Sezione C - Informazioni che i deployer di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 3

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA ad alto rischio che devono essere registrati a norma dell'articolo 49:

1. il nome, l'indirizzo e i dati di contatto del deployer;
2. il nome, l'indirizzo e i dati di contatto della persona che fornisce informazioni a nome del deployer;
3. l'indirizzo internet dell'inserimento del sistema di IA nella banca dati dell'UE da parte del suo fornitore;
4. una sintesi dei risultati della valutazione d'impatto sui diritti fondamentali effettuata a norma dell'articolo 27;
5. una sintesi della valutazione d'impatto sulla protezione dei dati effettuata ai sensi dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, come specificato all'articolo 26, paragrafo 8, del presente regolamento, ove applicabile.

ALLEGATO IX

Informazioni da presentare all'atto della registrazione dei sistemi di IA ad alto rischio elencati nell'allegato III in relazione alle prove in condizioni reali in conformità dell'articolo 60

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione alle prove in condizioni reali che devono essere registrate a norma dell'articolo 60:

1. un numero di identificazione unico a livello dell'Unione della prova in condizioni reali;
2. il nome e i dati di contatto del fornitore o potenziale fornitore e dei deployer coinvolti nella prova in condizioni reali;
3. una breve descrizione del sistema di IA, la sua finalità prevista e altre informazioni necessarie per l'identificazione del sistema;
4. una sintesi delle principali caratteristiche del piano di prova in condizioni reali;
5. informazioni sulla sospensione o sulla cessazione della prova in condizioni reali.

ALLEGATO X

Atti legislativi dell'Unione sui sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia

1. Sistema di informazione Schengen

a) Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 312 del 7.12.2018, pag. 1).

b) regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n, 1987/2006 (GU L 312 del 7.12.2018, pag. 14).

c) regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n, 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

2. Sistema di informazione visti

a) Regolamento (UE) 2021/1133 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che modifica i regolamenti (UE) n, 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 e (UE) 2019/818 per quanto riguarda la definizione delle condizioni di accesso agli altri sistemi di informazione dell'UE ai fini del sistema di informazione visti (GU L 248 del 13.7.2021, pag. 1);

b) regolamento (UE) 2021/1134 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che modifica i regolamenti (CE) n, 767/2008, (CE) n, 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (UE) 2019/1896 del Parlamento europeo e del Consiglio e che abroga le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, ai fini della riforma del sistema di informazione visti (GU L 248 del 13.7.2021, pag. 11)

3. Eurodac

Regolamento (UE) 2024/1358 o del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1315 e (UE) 2024/1350 del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n, 603/2013 del Parlamento europeo e del Consiglio (GU L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Sistema di ingressi/uscite

Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n, 767/2008 e (UE) n, 1077/2011 (GU L 327 del 9.12.2017, pag. 20).

5. Sistema europeo di informazione e autorizzazione ai viaggi

a) Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n, 1077/2011, (UE) n, 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (GU L 236 del 19.9.2018, pag. 1);

b) regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (GU L 236 del 19.9.2018, pag. 72).

6. Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi

Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).

7. Interoperabilità

a) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n, 767/2008, (UE) n, 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27);

b) regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85).

ALLEGATO XI

Documentazione tecnica di cui all'articolo 53, paragrafo 1, lettera a) — documentazione tecnica per i fornitori di modelli di IA per finalità generali

Sezione 1

Informazioni che devono fornire tutti i fornitori di modelli di IA per finalità generali

La documentazione tecnica di cui all'articolo 53, paragrafo 1, lettera a), deve includere almeno le seguenti informazioni, in funzione della dimensione e del profilo di rischio del modello:

1. Una descrizione generale del modello di IA per finalità generali comprendente:

   a) i compiti che il modello è destinato a eseguire e il tipo e la natura dei sistemi di IA in cui può essere integrato;

   b) le politiche di utilizzo accettabili applicabili;

   c) la data di pubblicazione e i metodi di distribuzione;

   d) l'architettura e il numero di parametri;

   e) la modalità (ad esempio testo, immagine) e il formato degli input e degli output;

   f) la licenza.

2. Una descrizione dettagliata degli elementi del modello di cui al punto 1 e informazioni pertinenti sul processo di sviluppo, compresi gli elementi seguenti:

   a) i mezzi tecnici (ad esempio istruzioni per l'uso, infrastruttura, strumenti) necessari per integrare il modello di IA per finalità generali nei sistemi di IA;

   b) le specifiche di progettazione del modello e del processo di addestramento, comprese le metodologie e le tecniche di addestramento, le principali scelte progettuali, comprese le motivazioni e le ipotesi formulate; gli aspetti che il modello è progettato per ottimizzare e la pertinenza dei diversi parametri, se del caso;

   c) informazioni sui dati utilizzati per l'addestramento, la prova e la convalida, se del caso, compresi il tipo e la provenienza dei dati e le metodologie di organizzazione (ad esempio pulizia, filtraggio, ecc.), il numero di punti di dati, la loro portata e le principali caratteristiche; il modo in cui i dati sono stati ottenuti e selezionati e tutte le altre misure per rilevare l'inadeguatezza delle fonti di dati e i metodi per rilevare distorsioni identificabili, se del caso;

   d) le risorse computazionali utilizzate per addestrare il modello (ad esempio il numero di operazioni in virgola mobile), il tempo di addestramento e altri dettagli pertinenti relativi all'addestramento;

   e) il consumo energetico noto o stimato del modello.

   Per quanto riguarda la lettera e), se il consumo energetico del modello non è noto, il consumo energetico può basarsi su informazioni relative alle risorse computazionali utilizzate.

Sezione 2

Informazioni aggiuntive che devono fornire i fornitori di modelli di IA per finalità generali con rischio sistemico

1. Una descrizione dettagliata delle strategie di valutazione, compresi i risultati della valutazione, sulla base dei protocolli e degli strumenti di valutazione pubblici disponibili o di altri metodi di valutazione. Le strategie di valutazione comprendono criteri di valutazione, metriche e metodi per l'individuazione delle limitazioni.

2. Se del caso, una descrizione dettagliata delle misure messe in atto al fine di effettuare il test contraddittorio (adversarial testing) interno e/o esterno (ad esempio, red teaming), adeguamenti dei modelli, compresi l'allineamento e la messa a punto.

3. Se del caso, una descrizione dettagliata dell'architettura del sistema che spiega in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo.

ALLEGATO XII

Informazioni sulla trasparenza di cui all'articolo 53, paragrafo 1, lettera b) - documentazione tecnica per i fornitori di modelli di IA per finalità generali ai fornitori a valle che integrano il modello nel loro sistema di IA

Le informazioni di cui all'articolo 53, paragrafo 1, lettera b), contengono almeno quanto segue:

1. Una descrizione generale del modello di IA per finalità generali comprendente:
   a) i compiti che il modello è destinato a eseguire e il tipo e la natura dei sistemi di IA in cui può essere integrato;
   b) le politiche di utilizzo accettabili applicabili;
   c) la data di pubblicazione e i metodi di distribuzione;
   d) il modo in cui il modello interagisce o può essere utilizzato per interagire con hardware o software che non fanno parte del modello stesso, ove applicabile;
   e) le versioni del software pertinente relative all'uso del modello di IA per finalità generali, se del caso;
   f) l'architettura e il numero di parametri;
   g) la modalità (ad esempio testo, immagine) e il formato degli input e degli output;
   h) la licenza per il modello.
2. Una descrizione degli elementi del modello e del processo relativo al suo sviluppo, compresi:
   a) i mezzi tecnici (ad esempio istruzioni per l'uso, infrastruttura, strumenti) necessari per integrare il modello di IA per finalità generali nei sistemi di IA;
   b) la modalità (ad esempio testo, immagine, ecc.) e il formato degli input e degli output e la loro dimensione massima (ad esempio, lunghezza della finestra contestuale, ecc.);
   c) informazioni sui dati utilizzati per l'addestramento, la prova e la convalida, se del caso, compresi il tipo e la provenienza dei dati e le metodologie di organizzazione.

ALLEGATO XIII

Criteri per la designazione dei modelli di IA per finalità generali con rischio sistemico di cui all'articolo 51

Al fine di determinare se un modello di IA per finalità generali ha capacità o un impatto equivalente a quelli di cui all'articolo 51, paragrafo 1, lettera a), la Commissione tiene conto dei criteri seguenti:

a) il numero di parametri del modello;

b) la qualità o la dimensione del set di dati, ad esempio misurata mediante token;

c) la quantità di calcolo utilizzata per addestrare il modello misurata in operazioni in virgola mobile o indicata da una combinazione di altre variabili quali il costo stimato dell'addestramento, il tempo stimato necessario per l'addestramento o il consumo energetico stimato per l'addestramento;

d) le modalità di input e output del modello, come da testo a testo (modelli linguistici di grandi dimensioni), da testo a immagine, multimodalità e soglie di punta per determinare le capacità ad alto impatto per ciascuna modalità, nonché il tipo specifico di input e output (ad esempio sequenze biologiche);

e) i parametri di riferimento e le valutazioni delle capacità del modello, anche tenendo conto del numero di compiti che non richiedono un addestramento aggiuntivo, la capacità di apprendere nuovi compiti distinti, il livello di autonomia e scalabilità e gli strumenti a cui ha accesso;

f) se il modello ha un alto impatto sul mercato interno in considerazione della sua portata, che viene presunta quando il modello stesso è stato messo a disposizione di almeno 10 000 utenti commerciali registrati stabiliti nell'Unione;

g) il numero di utenti finali registrati.

Regione Puglia - Legge regionale n. 4 del 14 aprile 2025

Misure di promozione in materia di innovazione aperta e intelligenza artificiale e disposizioni varie

Capo I

Disposizioni in materia di innovazione aperta e intelligenza artificiale

Art. 1 Finalità

In vigore dal 18 aprile 2025

1. La Regione, al fine di sostenere e accelerare lo sviluppo e l'innovazione tecnologica del sistema produttivo regionale, valorizzando le risorse e le competenze presenti sul territorio, nonché attraendo talenti tecnologici e creativi, disciplina le misure per favorire lo scambio di flussi di conoscenza tra gli attori dei processi produttivi e della ricerca con l'obiettivo di agevolare e stimolare, anche attraverso il coinvolgimento delle agenzie strategiche regionali e delle società in house, l'incontro tra la domanda di innovazione e l'offerta innovativa.

2. Gli interventi e gli obiettivi della presente legge, concretamente declinati sul territorio regionale in coerenza con le iniziative nazionali e unionali in materia di innovazione aperta, nonché con la strategia di specializzazione intelligente regionale (S3) e con le altre strategie regionali pertinenti, mirano a promuovere altresì collaborazioni e partenariati, a favorire la diffusione delle eccellenze industriali e scientifiche, a dare impulso alla creazione di comunità attive in materia.

3. La Regione promuove inoltre, in collaborazione con tutti i portatori di interessi, con le agenzie strategiche regionali e le società in house, la costituzione di comunità digitali e di hub territoriali di innovazione aperta di cui all'articolo 5.

4. La Regione sostiene la diffusione dell'intelligenza artificiale quale strumento per lo sviluppo del sistema economico e sociale regionale.

5. Le finalità di cui al precedente comma e gli interventi di cui agli articoli seguenti sono perseguiti in coerenza con il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/ UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), l'ulteriore disciplina, anche nazionale, di settore e i documenti strategici regionali in materia di innovazione, trasformazione digitale e partecipazione.

Art. 2 Definizioni

In vigore dal 18 aprile 2025

1. Ai fini della presente legge si intende per:

a) “innovazione aperta o open innovation”, un modello di innovazione di carattere strategico e collaborativo, basato sullo scambio di flussi di conoscenza dall'esterno all'interno dell'organizzazione e viceversa, finalizzato a sostenere lo sviluppo e l'innovazione tecnologica del sistema produttivo regionale secondo principi di neutralità tecnologica e orientato a:

1. promuovere la collaborazione tra le imprese e l'ambiente esterno, in particolar modo start-up, università, organismi di ricerca, incubatori certificati d'impresa, altri enti e istituzioni pubbliche e private;

2. determinare sinergie tali da accelerare e migliorare i processi di innovazione;

3. stimolare la logica di rete, favorendo l'innovazione di processi, servizi, prodotti, modelli e metodi contribuendo a risolvere le sfide economiche, sociali ed ambientali, presenti e future, anche attraverso l'utilizzo di intelligenza artificiale e delle altre tecnologie abilitanti (Key Enabling Technologies - KETs);

4. accelerare l'innovazione e ottenere vantaggi competitivi attraverso una maggiore apertura e collaborazione con l'ecosistema esterno;

b) "ecosistema dell'innovazione", l'insieme degli attori dell'innovazione, pubblici e privati, presenti su un territorio, che interagiscono e collaborano secondo dinamiche di reciproca contaminazione al fine di produrre o ridistribuire valore attraverso formazione di alto livello, costante innovazione e ricerca applicata;

c) "piattaforma digitale dell'innovazione", uno strumento on-line finalizzato ad agevolare e stimolare le relazioni tra tutti gli attori dell'innovazione (imprese, università e centri di ricerca, incubatori certificati, istituti tecnici superiori - ITS, associazioni di categoria, camere di commercio, digital innovation hub, pubbliche amministrazioni, terzo settore, cittadini e ogni altro portatore di interesse), che intendano avere un ruolo attivo nelle politiche di ricerca e sviluppo;

d) "hub territoriali dell'open Innovation", centri per l'innovazione destinati ad accogliere attività ad alta tecnologia, anche sotto forma di "experience center" con l'obiettivo di promuovere la conoscenza e il trasferimento tecnologico al sistema produttivo, attraverso la creazione di laboratori di fabbricazione digitale, di percorsi di incubazione e accelerazione e di altri servizi a supporto dello sviluppo di idee e progetti imprenditoriali.

Art. 3 Agenda strategica triennale

In vigore dal 18 aprile 2025

1. La Giunta regionale, in armonia con gli strumenti di programmazione vigenti e con le pianificazioni di settore, anche in tema di attrazione e valorizzazione dei talenti, approva l'agenda strategica triennale in materia di innovazione aperta, che individua gli ambiti e le priorità dell'intervento regionale per favorirne la diffusione sul territorio pugliese.

2. Nel corso del triennio, l'agenda strategica può essere modificata con deliberazione di Giunta regionale.

3. Entro il 31 marzo di ogni anno, l'assessore competente in materia di sviluppo economico relaziona alla Giunta regionale circa lo stato di attuazione dell'agenda strategica.

Art. 4 Piattaforma digitale dell'innovazione

In vigore dal 18 aprile 2025

1. La Regione, coerentemente con il piano di riorganizzazione digitale dell'amministrazione, istituisce la piattaforma digitale dell'innovazione per favorire la diffusione dell'innovazione aperta e promuovere lo sviluppo di progetti e collaborazioni, nel rispetto dei principi di pubblicità, trasparenza, parità di accesso e di trattamento, pari opportunità e non discriminazione. La piattaforma

assicura adeguati standard di sicurezza informatica e di protezione dei dati personali, dei diritti di autore, della proprietà intellettuale e del segreto industriale.

2. Nel rispetto dei principi previsti nel comma 1 la Regione, attraverso la piattaforma, persegue i seguenti obiettivi:

a) valorizzare le risorse e le competenze presenti sul territorio, promuovendo collaborazioni e partenariati;

b) censire le pregresse esperienze regionali in tema di innovazione aperta;

c) garantire una mappatura trasversale e georeferenziata degli attori dell'innovazione, particolarmente delle start-up, mettendo a disposizione degli utenti uno strumento di interrogazione tramite motore di ricerca;

d) favorire l'incontro tra domanda e offerta di innovazione;

e) diffondere la conoscenza delle eccellenze industriali e scientifiche;

f) attrarre talenti tecnologici e creativi;

g) individuare le sfide innovative e tecnologiche a cui il sistema industriale può rispondere in ottica di ecosistema;

h) contribuire allo sviluppo di industrie emergenti valorizzando le competenze e le tecnologie chiave abilitanti;

i) promuovere l'aggregazione degli attori dei processi di innovazione in un ecosistema digitale collaborativo, in cui si definiscono e realizzano progettualità in linea con gli obiettivi strategici per la crescita della Regione, sia in termini di miglioramento della competitività delle imprese che di qualità della vita dei cittadini.

3. La piattaforma digitale dell'innovazione si sviluppa su tre pilastri:

a) luogo di incontro tra domanda di innovazione espressa o rilevata da imprese, pubblica amministrazione e altre istituzioni o organizzazioni e soluzioni provenienti da innovatori, micro, piccole e medie imprese, start-up e spin-off;

b) vetrina di proposte e iniziative di innovazione, nuovi prodotti e servizi innovativi provenienti dall'ecosistema;

c) ambiente per lavoro cooperativo, supporto a progetti di ricerca ed innovazione e alla gestione di gruppi di lavoro.

4. Al fine di garantire il dialogo tra la domanda di innovazione e le competenze, la piattaforma prevista nel comma 1 implementa altresì processi di incontro automatico, basato anche su tecniche di intelligenza artificiale, finalizzati ad analizzare gli interessi, le esperienze e le innovazioni dell'utente e a suggerire sfide e innovazioni pubblicate da altri attori.

5. La piattaforma fornisce agli utenti informazioni adeguate per consentire decisioni consapevoli riguardo all'uso dei servizi che utilizzano l'intelligenza artificiale e garantisce ai massimi livelli i principi di equità, trasparenza e non discriminazione.

Art. 5 Hub territoriali dell'open innovation

In vigore dal 18 aprile 2025

1. La Regione, per le finalità previste nell'articolo 1, favorisce la costituzione di hub territoriali dell'innovazione aperta all'interno di spazi pubblici esistenti, idonei ad accogliere iniziative nei settori della ricerca e sviluppo.

2. Per la realizzazione delle attività da svolgere negli hub territoriali, la Regione può avvalersi del supporto dell'agenzia strategica per la tecnologia, il trasferimento tecnologico e l'innovazione (ARTI), che pianifica e attua interventi tesi a valorizzare i risultati della ricerca, ad agevolare il trasferimento tecnologico, nonché ad accelerare la trasformazione digitale dei processi produttivi in un'ottica di sostenibilità economica e ambientale e di impatto sociale sul territorio e secondo principi di neutralità tecnologica.

Art. 6 Ulteriori interventi in favore dell'open innovation

In vigore dal 18 aprile 2025

1. Per incentivare lo sviluppo dell'innovazione aperta la Regione, nel rispetto dei principi di cui all'articolo 4, comma 1, può prevedere:

a) l'organizzazione di eventi volti ad attivare processi di incontro tra offerta e domanda di competenze e conoscenze, stimolando la rimozione delle barriere alla libera circolazione delle idee e favorendo la nascita e lo sviluppo di reti tra gli attori dei processi di innovazione, nonché la promozione di eventi informativi sulle opportunità europee di sostegno all'innovazione e sull'identificazione di possibili partner internazionali;

b) la promozione, in correlazione con gli strumenti agevolativi regionali, di specifici interventi formativi e di sensibilizzazione a favore delle realtà produttive pugliesi, mediante azioni volte a promuovere la domanda di innovazione, anche di tipo aggregato per filiera, settore, comparto, e a favorire la capacità delle imprese, in particolar modo delle micro, piccole e medie imprese (MPMI), di redigere e implementare piani e iniziative di innovazione aziendale;

c) la pubblicazione di avvisi aperti, rivolti a start-up, MPMI, associazioni, professionisti o anche singoli individui, al fine di promuovere lo sviluppo di progetti e soluzioni innovative in specifici settori di mercato;

d) la promozione di forme di premialità per incentivare iniziative di open innovation;

e) il rafforzamento, anche mediante il supporto dell'ARTI, delle attività di ricerca industriale da parte delle università e degli altri organismi di ricerca, nonché della loro collaborazione con le imprese e della valorizzazione imprenditoriale dei risultati;

f) il sostegno e il coinvolgimento dei giovani, quali portatori di competenze, valori, energie e talenti, nello sviluppo della dimensione imprenditoriale dell'innovazione, anche attraverso specifici accordi con le istituzioni scolastiche e universitarie, per favorire l'aumento di opportunità occupazionali di alta formazione e qualificazione presso le imprese o presso gli organismi di ricerca e per stimolare la partecipazione degli aspiranti innovatori ad attività come tirocini innovativi, workshop, hackathon e laboratori dell'innovazione;

g) il coinvolgimento degli enti del terzo settore e della società civile, quali soggetti portatori di una peculiare domanda di innovazione collegata alle sfide sociali.

2. Nel caso in cui gli interventi disposti in applicazione della presente legge si configurino come aiuti di Stato, la Regione assicura il rispetto degli articoli 107, 108 e 109 del Trattato sul funzionamento dell'Unione europea (TFUE).

Art. 7 Disposizioni attuative

In vigore dal 18 aprile 2025

1. Entro 120 giorni dall'entrata in vigore della presente legge, nel rispetto dei principi richiamati nella stessa, con deliberazione di Giunta regionale sono definite le modalità attuative degli interventi a favore dell'open innovation.

Art. 8 Promozione dell'intelligenza artificiale nella pubblica amministrazione

In vigore dal 18 aprile 2025

1. La Regione supporta lo sviluppo di reti costituite tra i responsabili per la transizione digitale delle pubbliche amministrazioni del territorio, per promuovere l'utilizzo dell'intelligenza artificiale al fine di migliorare la qualità e la gamma dell'offerta di servizi, nel pieno rispetto dei diritti fondamentali delle persone e di accessibilità ai servizi pubblici digitali.

2. Per le finalità di cui al presente articolo, la Regione può promuovere:

a) studi e ricerche specifiche sul tema;

b) attività formative dedicate all'acquisizione di competenze per il proprio personale e per il personale delle pubbliche amministrazioni del territorio, anche in collaborazione con le università pugliesi attraverso l'attività del centro di cui al successivo articolo 9;

c) sviluppo di attività condivise con le agenzie strategiche regionali e le proprie società in house;

d) costituzione di comunità di pratica.

Art. 9 Centro di competenza regionale per l'intelligenza artificiale nella pubblica amministrazione

In vigore dal 18 aprile 2025

1. Il Centro di competenza regionale per l'intelligenza artificiale nella pubblica amministrazione (Centro), istituito con la deliberazione della Giunta regionale 30 ottobre 2023, n. 1488, è la sede nella quale la Regione definisce la strategia e gli interventi in tema di intelligenza artificiale nella pubblica amministrazione regionale.

2. Il Centro ha le seguenti finalità:

a) indagare, analizzare, comprendere, monitorare e valutare le implicazioni e la sostenibilità di applicazioni, sistemi, strumenti e soluzioni di intelligenza artificiale nella pubblica amministrazione regionale;

b) promuovere la redazione di linee di indirizzo, attività di ricerca, formazione e studio specifiche, anche tramite costituzione di tavoli di lavoro;

c) sperimentare l'utilizzo di applicazioni, sistemi, strumenti e soluzioni di intelligenza artificiale in ambito regionale, all'interno di processi e sistemi.

3. Il Centro può sottoscrivere protocolli di collaborazione in ambito pubblico e in ambito pubblico-privato, senza ulteriori oneri a carico del bilancio regionale, allo scopo di monitorare l'offerta di sistemi di intelligenza artificiale sul territorio regionale.

Art. 10 Promozione dello sviluppo di applicazioni di intelligenza artificiale delle MPMI e diffusione della conoscenza

In vigore dal 18 aprile 2025

1. Per supportare, a livello regionale, le opportunità dell'intelligenza artificiale, in particolare nelle MPMI, la Regione può prevedere:

a) iniziative di riqualificazione e miglioramento delle competenze in tutti i contesti produttivi sull'utilizzo dell'intelligenza artificiale per l'innovazione di processo, di prodotto e organizzativa;

b) il sostegno a progetti di ricerca collaborativa per la realizzazione di applicazioni specifiche e contestualizzate in domini rilevanti per le filiere dell'innovazione regionale;

c) la promozione, anche attraverso la piattaforma informatica di cui all'articolo 4, dell'interconnessione delle filiere manifatturiere e dei servizi con l'ecosistema dell'innovazione digitale pugliese, costituito dalle università, dagli istituti tecnici superiori, dai poli per l'innovazione digitale, dai centri di competenza, dai distretti tecnologici e produttivi operanti nel settore delle tecnologie dell'informazione e delle telecomunicazioni;

d) il sostegno e il potenziamento dell'ecosistema delle start-up;

e) il sostegno all'apertura del patrimonio dati pubblici delle amministrazioni locali, nonché all'utilizzo dei dati trasmessi dai satelliti nell'ambito dei programmi spaziali europei e nazionali.

2. Per promuove la diffusione della cultura e delle competenze digitali e l'uso consapevole degli strumenti e delle applicazioni basate sull'intelligenza artificiale, anche attraverso l'interconnessione delle iniziative presenti sul territorio, la Regione può sviluppare iniziative di divulgazione e di facilitazione, finalizzate a realizzare:

a) campagne di comunicazione dedicate ai rischi e alle opportunità dell'intelligenza artificiale, anche attraverso i propri portali istituzionali e i propri social media;

b) eventi sul territorio, in collaborazione con associazioni di persone o professionali;

c) dibattiti pubblici e percorsi partecipativi che coinvolgono i diversi portatori di interesse, anche con il supporto delle proprie piattaforme telematiche;

d) programmi e corsi di formazione in materia di intelligenza artificiale e di uso conforme alla normativa della stessa.

Art. 11 Clausola valutativa

In vigore dal 18 aprile 2025

1. Il Consiglio regionale esercita il controllo sull'attuazione della presente legge e ne valuta i risultati ottenuti. A tal fine, trascorsi tre anni dall'entrata in vigore della legge, la Giunta regionale presenta entro il mese di marzo al Consiglio regionale una relazione annuale sullo stato di attuazione e sulla efficacia della stessa.

Art. 12 Norma finanziaria

In vigore dal 18 aprile 2025

1. Per le finalità di cui alla presente legge, nel bilancio regionale autonomo, è assegnata una dotazione finanziaria per l'esercizio 2025, in termini di competenza e cassa, nell'ambito della missione 14, programma 1, titolo 1, di euro 20 mila e nell'ambito della missione 1, programma 8, titolo 1, di euro 20 mila. Per ciascuno degli esercizi 2026 e 2027, è assegnata una dotazione finanziaria, in

termini di competenza, nell'ambito della missione 14, programma 1, titolo 1, di euro 15 mila e nell'ambito della missione 1, programma 8, titolo 1, di euro 15 mila.

2. Per la quantificazione e la copertura dell'onere finanziario per gli anni successivi si rinvia alle competenti leggi di bilancio.

3. All'attuazione degli interventi di cui alla presente legge possono concorrere inoltre le risorse concernenti i programmi cofinanziati con i fondi strutturali e di investimento europei (SIE) per gli anni 2021-2027, relative al programma operativo FESR e FSE+, nonché con i fondi di coesione nazionali del ciclo di programmazione 2021-2027 destinati alla Puglia".

Capo II

Disposizioni diverse

Art. 13 Modifiche alla l.r. 42/2024

In vigore dal 18 aprile 2025

1. Alla legge regionale 31 dicembre 2024, n. 42 (Disposizioni per la formazione del bilancio di previsione 2025 e bilancio pluriennale 2025-2027 della Regione Puglia (legge di stabilità regionale 2025)), sono apportate le seguenti modifiche:

a) all'articolo 23, comma 1, le parole: "negli asili nido" sono sostituite dalle seguenti: "nei nidi";

b) all'articolo 54, dopo le parole: "è assegnata", sono aggiunte le seguenti: ", al Comune di Margherita di Savoia,";

c) l'articolo 168 è sostituito dal seguente:

"1. Per consentire il funzionamento e l'accreditamento annuale presso l'Università degli Studi di Bari Aldo Moro del corso di laurea magistrale in "Scienze e Tecniche dello Sport" appartenente alla classe LM-68, con la possibilità di potenziare nel territorio pugliese competenze metodologiche e ricerche specifiche nell'ambito delle attività motorie e sportive, ai fini della realizzazione e del coordinamento delle Palestre Etiche ai sensi della legge regionale 18 maggio 2017, n. 14 (Norme in materia di riconoscimento, svolgimento, promozione e tutela dell'attività fisica adattata (AFA) - Modifica e integrazione alla legge regionale 4 dicembre 2006, n. 33 (Norme per lo sviluppo dello sport per tutte e per tutti)), è assegnata una dotazione finanziaria complessiva di euro 2.505.678,00 a partire dall'esercizio finanziario 2025 e per una validità temporale di quindici anni. Nel bilancio regionale autonomo, nell'ambito della missione 4, programma 4, titolo 1, è assegnata una dotazione finanziaria, per l'esercizio finanziario 2025 in termini di competenza e cassa, di euro 167.045,20.

2. Il contributo straordinario di cui al comma 1 è finalizzato al finanziamento di 1 posto di professore di prima fascia nel gruppo scientifico disciplinare 06/MEDF-01 - Scienze dell'esercizio fisico e dello sport, Settore scientifico disciplinare MEDF-01/B - Metodi e didattiche delle attività sportive, interno ai sensi dell'articolo 24, comma 6, della legge 30 dicembre 2010, n. 240 (Norme in materia di organizzazione delle università, di personale accademico e reclutamento, nonché delega al Governo per incentivare la qualità e l'efficienza del sistema universitario), e di 1 posto di professore di prima fascia nel gruppo scientifico disciplinare 06/MEDF-01 - Scienze dell'esercizio fisico e dello sport - Settore scientifico disciplinare MEDF-01/A - Metodi e didattiche delle attività motorie interno o esterno ai sensi dell'articolo 18, comma 1, della l. 240/2010, presso il Dipartimento di Biomedicina Traslazionale e Neuroscienze; il loro utilizzo sarà oggetto di rendicontazione e di apposita relazione che comprovi l'efficacia della misura.

3. Il contributo straordinario di cui al comma 1 è altresì finalizzato al finanziamento di contratti di ricerca ex articolo 22 della l.240/2010 di anni due nei settori scientifici ssd MEDF-01/A Metodi e didattiche delle attività motorie e MEDF-01/B Metodi e didattiche delle attività sportive. I contratti di ricerca sono finalizzati alla conduzione delle attività previste dalla l.r. 14/2017 relative alla sperimentazione ed erogazione di AFA nel contesto del territorio tarantino in collaborazione tra Università Aldo Moro Bari, Corso di Studio in Scienze e Tecniche dello Sport, Azienda sanitaria locale Taranto e Ospedali Moscati a Statte.

4. Per le finalità di cui ai commi 1 e 2, è sottoscritta apposita convenzione tra la Regione Puglia e l'Università degli Studi di Bari, ai sensi dell'articolo 18, comma 3, della l. 240/2010.";

d) il comma 1 dell'articolo 204 è sostituito dal seguente:

"1. Per sostenere il buon funzionamento delle scuole secondarie di primo grado e prevenire situazioni di scopertura nel territorio, è disposto un contributo straordinario in favore delle scuole secondarie di primo grado paritarie con sede nel territorio regionale.";

e) al comma 2 dell'articolo 211, dopo la parola: "assegnazione", sono aggiunte le seguenti: "alla Fondazione San Pio da Pietrelcina".

Art. 14 Modifiche alla l.r. 2/2023

In vigore dal 18 aprile 2025

1. Alla legge regionale 21 marzo 2023, n. 2 (Disciplina del modello di educazione in natura agrinido e agriasilo. Modifiche alla legge regionale 10 luglio 2006, n. 19 "Disciplina del sistema integrato dei servizi sociali per la dignità e il benessere delle donne e degli uomini in Puglia"), come modificata dall'articolo 149 della l.r. 42/2024, sono apportate le seguenti modifiche:

a) l'articolo 3 è sostituito dal seguente:

"1. Il modello di educazione in natura è rivolto sia alla fascia di età del nido che alla fascia di età della scuola dell'infanzia.

2. Il modello di educazione in natura destinato ai bambini e alle bambine di età compresa tra tre e trentasei mesi, qualificato come nido che svolge un progetto educativo prevalentemente in natura, è autorizzato e gestito nel rispetto della legge 8 novembre 2000, n. 328 (Legge quadro per la realizzazione del sistema integrato di interventi e servizi sociali), della legge regionale 10 luglio 2006, n. 19 (Disciplina del sistema integrato dei servizi sociali per la dignità e il benessere delle donne e degli uomini in Puglia) e del regolamento regionale 18 gennaio 2007, n. 4 (Legge regionale 10 luglio 2006, n. 19 - "Disciplina del sistema integrato dei servizi sociali per la dignità e il benessere delle donne e degli uomini di Puglia") e rientra nell'ambito dei servizi autorizzati all'esercizio delle attività educative destinate ai minori. La Giunta regionale definisce con regolamento i requisiti tecnico-strutturali, funzionali, organizzativi e professionali dei servizi di nido che svolge un progetto educativo prevalentemente in natura.

3. Il modello di educazione in natura destinato ai bambini e alle bambine di età compresa tra i tre e i sei anni, qualificato come scuola dell'infanzia che svolge un progetto educativo prevalentemente in natura, è disciplinato dal complesso normativo dedicato alla scuola dell'infanzia anche ai fini del riconoscimento della parità scolastica.

4. Il modello di educazione in natura per i nidi e le scuole dell'infanzia che svolgono un progetto educativo prevalentemente in natura opera, inoltre, in conformità e nel rispetto della normativa statale

concernente il sistema integrato di educazione e istruzione dalla nascita sino ai sei anni di cui al d.lgs. 65/2017 e, in particolare, delle indicazioni nazionali per il curricolo della scuola dell'infanzia e del primo ciclo di istruzione.

5. Le attività di educazione in natura sono inserite in un contesto ambientale agricolo-rurale, aperto e ricco di verde. Nel caso in cui le attività di nido e scuola dell'infanzia che svolge un progetto educativo prevalentemente in natura ricadano all'interno di un'area naturale protetta le disposizioni di cui alla presente legge devono tenere conto delle competenze attribuite agli enti di gestione delle aree naturali protette dalla normativa statale e regionale vigente in materia.";

b) il comma 2 dell'articolo 5 è sostituito dal seguente:

"2. Il progetto educativo basato sul modello dell'educazione in natura definisce le linee di indirizzo e le modalità operative da adottare da parte degli educatori dei nidi che svolgono un progetto educativo prevalentemente in natura e delle scuole dell'infanzia che svolgono un progetto educativo prevalentemente in natura. Il progetto educativo è fondato sull'idea del bambino quale protagonista del proprio processo di sviluppo, delle proprie esperienze e conoscenze, tenendo in debito conto l'offerta formativa specifica della fascia di età".

Art. 15 Entrata in vigore

In vigore dal 18 aprile 2025

1. La presente legge è dichiarata urgente ed entra in vigore il giorno stesso della sua pubblicazione sul Bollettino ufficiale della Regione.

La presente legge è dichiarata urgente e sarà pubblicata sul Bollettino ufficiale della Regione ai sensi e per gli effetti dell'articolo 53, comma 1, della legge regionale 12 maggio 2004, n° 7 "Statuto della Regione Puglia" ed entrerà in vigore il giorno stesso della sua pubblicazione.

E' fatto obbligo a chiunque spetti di osservarla e farla osservare come legge della Regione Puglia.

Data a Bari, addì 14 aprile 2025

Regione Toscana - Legge regionale n. 57 del 9 dicembre 2024

Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla L.R. 54/2009.

IL CONSIGLIO REGIONALE

ha approvato

IL PRESIDENTE DELLA GIUNTA

Promulga

la seguente legge

PREAMBOLO

Il Consiglio regionale

Visto l'articolo 117, comma secondo, lettera r), comma terzo e comma quarto, della Costituzione;

Visti l'articolo 4, comma 1, lettera z), e l'articolo 62 dello Statuto;

Visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, che abroga il regolamento (UE) 2013/526 (regolamento sulla cybersicurezza);

Visto il regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240;

Visto il regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022, relativo alla governance europea dei dati, che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati);

Vista la direttiva 2022/2555/UE del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), che definisce la strategia cyber dell'Unione europea, predisponendo adeguate risposte coordinate e innovative da parte di tutti gli stati membri per garantire la continuità dei servizi digitali in caso di incidenti di sicurezza;

Vista la decisione 2022/2481/UE del Parlamento europeo e del Consiglio del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030, finalizzata a conseguire una serie di obiettivi digitali vincolanti, nei settori delle competenze digitali, delle infrastrutture digitali, della digitalizzazione delle imprese, della digitalizzazione dei servizi pubblici;

Vista la direttiva 2022/2557/UE del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio;

Visto il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (AI Act) che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144

e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), e in particolare la definizione di cui all'articolo 3 (sistema di intelligenza artificiale);

Vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 19 aprile 2016, n. 179 (Piano d'azione dell'UE per l'e-Government 2016-2020. Accelerare la trasformazione digitale della pubblica amministrazione);

Vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato europeo delle regioni del 21 aprile 2021, n. 205 (Promuovere un approccio europeo all'intelligenza artificiale);

Visto il decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400);

Vista la legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi);

Visto il decreto legislativo 7 marzo 2005 n. 82 (Codice dell'amministrazione digitale);

Visto il decreto-legge 24 giugno 2014 n. 90 (Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziarie), convertito con modificazioni dalla legge 11 agosto 2014, n. 114;

Vista la legge 7 agosto 2015 n. 124 (Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche);

Vista la legge 27 dicembre 2019, n. 160 (Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022), in particolare l'articolo 1, comma 402;

Visto il decreto-legge 16 luglio 2020, n. 76 (Misure urgenti per la semplificazione e l'innovazione digitale), convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120 e, in particolare, l'articolo 26;

Visto il decreto legislativo 31 marzo 2023, n. 36 (Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici);

Vista la legge 28 giugno 2024, n. 90 (Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici);

Vista la legge regionale 5 ottobre 2009 n. 54 (Istituzione del sistema informativo e del sistema statistico regionale. Misure per il coordinamento delle infrastrutture e dei servizi per lo sviluppo della società dell'informazione e della conoscenza);

Vista la legge regionale 10 novembre 2014, n. 65 (Norme per il governo del territorio);

Vista la legge regionale 18 febbraio 2015, n. 19 (Disposizioni in materia di dati aperti e il loro riutilizzo);

Visto il parere favorevole con raccomandazioni del Consiglio delle autonomie locali espresso nella seduta del 13 settembre 2024;

Considerato quanto segue:

Per quanto concerne il capo I:

1. La comunicazione della Commissione europea del 19 aprile 2016, n. 179, ha fissato i principi di base cui ispirare l'azione per l'e-government e, in particolare, il libero accesso ai dati ed ai servizi delle amministrazioni pubbliche, propedeutici ad un effettivo coinvolgimento delle parti interessate nel processo decisionale, nonché la interoperabilità delle varie banche dati delle pubbliche amministrazioni da intendersi come la capacità delle singole componenti del sistema pubblica amministrazione di interagire e dialogare in forma automatica, scambiando informazioni e condividendo risorse, affinché vengano erogati "servizi pubblici end-to-end senza frontiere il più possibile personalizzati ed intuitivi a tutti i cittadini e a tutte le imprese dell'Unione europea (UE)";

2. L'uso delle tecnologie dell'informazione e della comunicazione (TIC) costituisce una leva essenziale per la semplificazione e la riorganizzazione dei procedimenti amministrativi, promuovendo un maggiore coordinamento delle competenze;

3. Lo Stato opera per la digitalizzazione dei processi amministrativi e l'uso delle tecnologie digitali nei rapporti tra cittadini e pubblica amministrazione mediante il D.Lgs. 85/2005 e semplifica le comunicazioni fra pubbliche amministrazioni e i cittadini con il servizio di notifiche digitali di cui all'articolo 26 del d.l. 76/2020 convertito dalla L. 120/2020;

4. La diffusione delle TIC è funzionale alla realizzazione del modello di "open government", in base al quale l'esercizio del potere pubblico si ispira a totale apertura e trasparenza, favorendo la massima partecipazione dei cittadini e garantendo al tempo stesso maggiori margini di controllo sul risultato finale, sull'operato della pubblica amministrazione e la collaborazione interistituzionale quale volano di efficienza dell'azione complessiva dell'amministrazione;

5. La presente legge è in linea con l'articolo 14 del D.Lgs. 82/2005 sui rapporti tra Stato, Regioni e autonomie locali, promuovendo intese e accordi, adottando, attraverso la Conferenza unificata, gli indirizzi utili per realizzare gli obiettivi dell'Agenda digitale europea e nazionale, realizzando un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso;

6. La legge regionale 26 gennaio 2004, n. 1 (Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale. Disciplina della "Rete telematica regionale toscana"), la individuato principi e criteri guida per lo sviluppo coordinato dei sistemi informativi pubblici, per la valorizzazione e condivisione del patrimonio informativo pubblico e per la promozione dell'interoperabilità tra tutte le pubbliche amministrazioni a livello territoriale, al fine di favorire l'interazione e la cooperazione, e previsto l'istituzione di una rete telematica regionale Toscana (RTRT) quale forma stabile di coordinamento delle autonomie locali e di cooperazione con gli altri soggetti pubblici e privati;

7. La L.R. 54/2009 ha valorizzato il patrimonio informativo pubblico quale strumento di trasparenza, diffusione della conoscenza e risorsa per lo sviluppo economico e sociale del territorio e disciplinato la diffusione di dati pubblici, di tipo sociale, economico, geografico, climatico, turistico, ambientale e il riutilizzo degli stessi nel rispetto della normativa, con particolare attenzione alla protezione dei dati personali, al diritto d'autore e alle ulteriori norme che pongono limitazioni o esclusioni all'apertura e al riutilizzo dei dati;

8. La L.R. 40/2009 ha realizzato una significativa semplificazione amministrativa e trasparenza nei rapporti tra imprese e pubbliche amministrazioni, individuando nello sportello unico delle attività produttive (SUAP) l'interlocutore privilegiato per le imprese prevedendo un sito istituzionale

regionale idoneo a fornire informazioni semplici e trasparenti in ordine alle possibilità di insediamento di attività produttive sul territorio e ai relativi procedimenti amministrativi;

9. È necessario unificare in un unico atto normativo la L.R. 1/2004 e le parti ad essa collegate della L.R. 54/2009, al fine di razionalizzarle e renderle organiche garantendo un adeguamento al contesto normativo, alle mutate esigenze dei cittadini e delle imprese e alla conseguente necessità di innovazione a sostegno della competitività e della trasformazione digitale per una pubblica amministrazione più accessibile ed efficiente, anche attraverso lo sviluppo di infrastrutture tecnologiche che assicurino l'interoperabilità dei sistemi informativi e, più in generale, tramite la riorganizzazione dei servizi della pubblica amministrazione e la loro digitalizzazione;

10. È necessario rimuovere e prevenire gli ostacoli che impediscono la piena parità di accesso alle informazioni e alle tecnologie dell'informazione e della comunicazione (TIC), riducendo il divario digitale all'accesso effettivo ai servizi ed alle tecnologie dell'informazione, per coloro che, per ragioni di disabilità, disagio economico e sociale, diversità culturale, localizzazione territoriale, ne risultano esclusi;

11. È necessario definire le modalità di azione della Regione per promuovere un costante potenziamento della sicurezza dei dati e dei sistemi informativi delle pubbliche amministrazioni toscane nonché, per il presidio degli ambiti strategici, in attuazione della normativa europea e nazionale;

12. È necessario che la Regione, nel quadro della normativa europea di attuazione e di riferimento, persegua i seguenti obiettivi:

a) effettivo esercizio dei diritti alla cittadinanza digitale, al fine di favorire la fruizione, anche in termini di inclusione, dei servizi resi ai cittadini e alle imprese dalla pubblica amministrazione, nonché la partecipazione responsabile alle attività sociali e civiche della collettività;

b) realizzazione personale e professionale dei cittadini tramite la formazione e l'aggiornamento sulle tecnologie digitali;

c) promozione delle forme di cittadinanza attiva e partecipativa in attuazione delle disposizioni della normativa regionale in materia;

d) progressiva eliminazione del divario digitale rimuovendo gli eventuali ostacoli alla fruizione dei servizi digitali in condizioni di pari opportunità e senza discriminazioni su tutto il territorio regionale;

e) attuazione dell'amministrazione digitale in Toscana e della interoperabilità dei diversi sistemi informativi nell'ambito del sistema informativo regionale (SIR), secondo il principio di adeguatezza dei diversi livelli istituzionali e territoriali, nel rispetto delle loro competenze;

f) sviluppo di servizi digitali rispettoso dei principi di accessibilità, elevata fruibilità e reperibilità delle informazioni, chiarezza di linguaggio e semplicità di consultazione, per garantire la partecipazione e l'accesso ai sistemi informativi da parte di tutti i soggetti interessati ed alle persone con disabilità;

g) resilienza, capacità operativa di prevenzione, dissuasione e risposta ad attacchi e incidenti informatici, cooperazione fra le autorità nazionali deputate alla cybersicurezza e gli enti pubblici e privati del territorio toscano, garantendo al contempo la protezione del cyberspazio afferente alle realtà toscane e la protezione dei dati personali in linea con la realizzazione degli obiettivi delle "strategie cloud" europea e italiana e delle "strategie cybersicurezza" europea e italiana;

h) semplicità e unitarietà dell'azione della pubblica amministrazione nei rapporti con i cittadini, le imprese e le istituzioni;

i) riuso di software tra pubbliche amministrazioni e rimozione di barriere derivanti dall'utilizzo di formati non standardizzati nella realizzazione di programmi e piattaforme, promuovendo adozione di tecnologie cloud e la fruizione in modalità "a servizi" al fine di incentivare la competitività e la trasparenza del mercato;

j) promozione della fruizione e riutilizzo dei dati e dell'accesso ai documenti informatici che costituiscono il patrimonio informativo regionale, da parte delle amministrazioni pubbliche e dai soggetti privati, alle condizioni fissate dall'ordinamento e senza oneri per gli utilizzatori, salvo per la prestazione di elaborazioni aggiuntive;

k) promozione, coerentemente agli obiettivi di sviluppo sostenibile (SDGs) dell'Agenda 2030, della sostenibilità digitale nei progetti di trasformazione digitale che possano avere un impatto significativo sull'ambiente, sull'economia, sulla salute, sulla società e sui diritti umani.

13. È opportuno consolidare l'opera, intrapresa dalla Regione a partire dalla L.R. 19/2015, di valorizzazione del patrimonio informativo pubblico quale strumento di trasparenza e diffusione della conoscenza e risorsa per lo sviluppo economico e sociale del territorio, e di disciplina della diffusione di dati pubblici di tipo sociale, economico, geografico, climatico, turistico ambientale, in conformità con la normativa europea e nazionale in materia di dati di apertura e riutilizzo dei dati, con particolare attenzione alla protezione dei dati personali, al diritto d'autore, alle particolari norme che pongono limitazioni ed esclusioni.

Per quanto concerne il capo II:

14. È opportuno individuare nel Consorzio Metis, soggetto "in house" già esistente e operante sia per la Regione Toscana, sia per il servizio sanitario regionale (SSR), in ambiti che includono l'innovazione digitale e la transizione digitale, il punto di riferimento operativo per coadiuvare la Regione Toscana, il SSR e, in prospettiva, tutto il territorio toscano nel presidio degli ambiti strategici, nonché come possibile soggetto di riferimento a disposizione della Regione e del territorio al fine di garantire un presidio strutturato e costante nella transizione digitale della Toscana, in raccordo costante con le strutture regionali che ne forniscono gli indirizzi per quanto di competenza;

15. È necessario confermare, rafforzare e rinnovare la comunità di enti afferenti alla RTRT, riprendendone gli elementi costituenti definiti con L.R. 1/2004, raccordandola maggiormente con l'agenda digitale della Regione Toscana (ADT), nonché inserendo il Consorzio Metis fra i soggetti operanti nell'ambito della direzione tecnico operativa della RTRT;

Approva la presente legge

CAPO I

Disposizioni generali

Articolo 1 Ambito di applicazione.

In vigore dal 2 gennaio 2025

1. Le disposizioni della presente legge si applicano:

a) alla Regione e agli enti dipendenti di cui all'articolo 50 dello Statuto, ivi compresi quelli di consulenza sia della Giunta regionale, sia del Consiglio regionale;

b) agli enti di diritto privato controllati dalla Regione;

c) alle aziende e agli enti del servizio sanitario regionale (SSR).

2. La presente legge, nell'ambito dei rispettivi ordinamenti e nel rispetto delle modalità organizzative di ciascuno, si applica inoltre agli enti locali della Toscana e ai loro enti e organismi dipendenti o strumentali, agli organismi privati comunque denominati, da essi controllati, nonché a ogni altro soggetto pubblico e privato che usufruisca dei servizi digitali offerti dalla Regione previa stipula di una convenzione.

Articolo 2 Oggetto.

In vigore dal 2 gennaio 2025

1. La presente legge disciplina:

a) le modalità di attuazione del processo di trasformazione digitale sul territorio regionale in un contesto organizzato di cooperazione istituzionale, al fine di garantire la semplificazione e la trasparenza dei processi amministrativi e garantire a cittadini e imprese servizi digitali efficienti ed accessibili;

b) la rete telematica regionale toscana (RTRT) quale forma stabile di coordinamento della transizione digitale della comunità delle autonomie locali e dei relativi sistemi informativi regionali e di cooperazione degli stessi con altri soggetti, pubblici e privati, nelle materie di cui alla presente legge, secondo le modalità previste al capo II;

c) il sistema informativo regionale (SIR) di cui al capo III e i servizi digitali messi a disposizione dalla Regione.

2. Per quanto non disciplinato dalla presente legge, incluse le definizioni, si applicano le disposizioni normative, primarie e secondarie regionali, nazionali e dell'Unione europea (UE).

Articolo 3 Definizioni.

In vigore dal 2 gennaio 2025

1. Agli effetti della presente legge si intende per:

a) centri di facilitazione digitale: spazi attivati in collaborazione fra la Regione, gli enti locali ed altri soggetti del Terzo settore, costituiti su tutto il territorio regionale al fine di ridurre la percentuale di popolazione a rischio di esclusione digitale "digital divide" e fornire ai cittadini supporto e formazione per l'utilizzo dei servizi digitali della pubblica amministrazione e del settore privato;

b) infrastruttura di rete regionale: insieme di collegamenti dei sistemi, degli apparati e dei servizi che garantiscono la connettività, la sicurezza, la cooperazione applicativa, anche in relazione al sistema pubblico di connettività, le comunicazioni, l'identificazione e l'accesso fra i sistemi informativi e dei soggetti aderenti e utilizzatori di tale infrastruttura;

c) agenda digitale della Toscana (ADT): documento con il quale la Regione definisce azioni atte a promuovere l'economia digitale nel proprio territorio;

d) cittadinanza digitale: insieme di diritti e doveri che ha lo scopo di semplificare il rapporto tra pubbliche amministrazioni, cittadini, imprese consentendogli di partecipare alla vita sociale attraverso mezzi e strumenti digitali;

e) sportello digitale unico: strumento per un facile accesso dei cittadini e delle imprese europee a informazioni di alta qualità e procedure online efficienti basate sul principio ″once only″;

f) governance dei dati: insieme di processi, ruoli, linee di condotta, standard e indicatori finalizzato a garantire un uso efficace ed efficiente delle informazioni, che permetta di raggiungere gli obiettivi prefissati attraverso la definizione di processi e responsabilità che assicurano la qualità e la sicurezza dei dati impiegati all'interno di un'organizzazione aziendale o di una pubblica amministrazione, e l'individuazione di soggetti chiamati a intraprendere determinate azioni, i dati coinvolti, le modalità di svolgimento e i profili di responsabilità;

g) sistema informativo regionale (SIR): l'insieme di servizi digitali e basi di dati che costituiscono il patrimonio informativo della Regione, degli enti dipendenti e delle agenzie a supporto delle funzioni di governo e amministrazione, senza pregiudizio delle competenze di ciascun soggetto nel trattamento dei propri dati;

h) lock-in tecnologico: fenomeno per il quale gli utenti sono resi dipendenti da un prodotto o servizio digitale specifico, rendendo difficile il passaggio a un'alternativa, con ricadute negative in termini di ostacolo significativo all'innovazione e alla libertà digitale;

i) infrastrutture digitali e datacenter: infrastrutture digitali e datacenter gestite da Regione Toscana che implementano tecnologie "cloud" e rispondono ai criteri di sicurezza definiti dall'Agenzia per la cybersicurezza nazionale (ACN) e costituiscono articolazione territoriale del sistema pubblico di connettività;

j) sistema di intelligenza artificiale (sistema IA): ai sensi dell'articolo 3 del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), cosiddetto "AI Act", e, in particolare, la definizione di cui all'articolo 3 (Sistema di intelligenza artificiale), il software sviluppato con una o più tecniche e approcci elencati nell'allegato I al regolamento e in grado, per un dato insieme di obiettivi definiti dall'uomo, di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono.

Articolo 4 Principi.

In vigore dal 2 gennaio 2025

1. Nel perseguimento delle finalità della presente legge la Regione e i soggetti di cui all'articolo 1, commi 1 e 2, operano conformandosi agli obiettivi indicati nel preambolo ed ai seguenti principi e criteri guida:

a) sviluppo coordinato dei sistemi informativi pubblici, valorizzazione e condivisione del patrimonio informativo pubblico, da perseguire secondo i modelli di cooperazione istituzionale definiti nella presente legge, e promozione dell'interoperabilità tra tutte le pubbliche amministrazioni a livello territoriale per favorire l'interazione e la cooperazione, e per assicurare, nel rispetto dell'articolo 117, comma secondo, lettera r), della Costituzione e salvaguardando l'autonoma potestà degli enti locali, il coordinamento informativo ed informatico dei dati tra le pubbliche amministrazioni presenti sul territorio regionale;

b) valorizzazione delle aggregazioni di soggetti pubblici costituite su base tematica o territoriale, quali le unioni di comuni o le forme di esercizio associato delle gestioni, e dei raccordi con le articolazioni territoriali dell'amministrazione statale;

c) utilizzo di standard informativi e documentali aperti negli scambi tra amministrazioni pubbliche e con riferimento ai dati da rendere pubblici;

d) qualità dei dati in termini di correttezza, aggiornamento, completezza e coerenza, nonché di integrità degli stessi nella gestione telematica, anche mediante l'adozione di tecniche di criptazione e di adeguate misure di protezione;

e) salvaguardia della sicurezza dei dati, dei sistemi, delle reti e dei servizi mediante l'adozione di misure tecniche e organizzative adeguate;

f) valorizzazione della interoperabilità di componenti prodotti da una pluralità di fornitori, di favorirne la possibilità di riuso, di ottimizzare le risorse e di garantire la piena conoscenza del processo di trattamento dei dati;

g) promozione della cittadinanza digitale favorendo la fruizione, anche in termini di inclusione, dei servizi resi ai cittadini e alle imprese dalla pubblica amministrazione;

h) promozione della cultura e delle competenze digitali e dell'uso consapevole della rete e degli strumenti digitali, anche attraverso la valorizzazione di centri di facilitazione digitale e di contatto con i cittadini;

i) promozione di misure, soluzioni tecnologiche, standard e pratiche di sviluppo che favoriscano l'inclusione sociale, garantendo l'accessibilità, con specifica attenzione alle diverse abilità e promuovendo l'usabilità dei sistemi informativi;

j) incentivazione, qualificazione e coordinamento dei servizi di rete per uno sviluppo socioeconomico equilibrato del territorio regionale.

Articolo 5 Trattamento di dati personali.

In vigore dal 2 gennaio 2025

1. La realizzazione di sistemi e servizi informativi pubblici per la trasformazione digitale e l'innovazione tecnologica e organizzativa costituisce svolgimento di funzioni istituzionali ai fini del trattamento di dati personali da parte della Regione e degli altri enti del sistema regionale delle autonomie locali.

Articolo 6 Ruolo e compiti della Regione.

In vigore dal 2 gennaio 2025

1. Per il raggiungimento degli obiettivi della presente legge la Regione:

a) promuove lo sviluppo della trasformazione digitale e della comunità della RTRT;

b) determina le condizioni per assicurare la più ampia integrazione e interoperabilità dei sistemi digitali anche verso standard e piattaforme di interoperabilità di livello europeo e nazionale;

c) assicura standard di qualità e adeguate modalità di monitoraggio per l'accessibilità e il trattamento dei dati necessari ad alimentare i servizi statistici ed informativi;

d) recepisce le indicazioni europee e nazionali circa le infrastrutture critiche da proteggere per l'erogazione e la corretta fruizione dei servizi pubblici da parte della popolazione regionale;

e) promuove forme di coinvolgimento di cittadini, imprese, professionisti che utilizzano i servizi digitali erogati nel miglioramento continuo e nella semplificazione di interfacce, servizi e processi;

f) definisce le metodologie di progettazione, organizzazione e sviluppo di sistemi informativi idonei a supportare le proprie attività istituzionali, anche attraverso la collaborazione con le altre pubbliche amministrazioni al fine di sviluppare l'integrazione dei servizi;

g) coordina lo sviluppo di infrastrutture telematiche diffuse sul territorio toscano con infrastrutture di calcolo e piattaforme tecnologiche idonee all'erogazione multicanale dei servizi in rete, alla gestione dell'identità digitale, alla cooperazione applicativa e all'interoperabilità, anche in una logica di condivisione delle infrastrutture tra gli enti toscani per garantire un costante contenimento della spesa complessiva;

h) mette a disposizione e gestisce, anche tramite il Consorzio Metis di cui all'articolo 19, infrastrutture e piattaforme di erogazione di servizi digitali e di fruizione di strati informativi, anche interconnesse a sistemi e piattaforme di livello europeo e nazionale secondo standard tecnologici definiti dalle competenti autorità europee e nazionali;

i) promuove regole di progettazione e utilizzo consapevole dei sistemi IA affidabili e sicuri soprattutto nell'esercizio delle funzioni amministrative, tenendo conto in particolar modo dei principi di trasparenza, umanità e responsabilità, in accordo con la normativa statale e dell'Unione europea, ed in collaborazione con le autorità nazionali di riferimento;

j) promuove la realizzazione degli obiettivi della transizione ecologica attraverso la più efficiente e sostenibile organizzazione ed erogazione dei servizi digitali regionali;

k) incentiva la formazione di competenze specifiche in ambito digitale;

l) si raccorda con gli enti locali della Toscana e le loro società "in house" e partecipate operanti nel settore, nel rispetto del decreto legislativo 31 marzo 2023, n. 36 (Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici), promuovendo la valorizzazione di esperienze esistenti, nuove forme di accordo con gli enti nazionali e gli operatori deputati alla diffusione della connettività sul territorio, al fine di incrementare i servizi digitali, diffondere ed ottimizzare il livello di copertura del territorio regionale con connettività fissa e mobile a banda ultra-larga sia per sedi pubbliche, sia private;

m) può adottare le misure di sicurezza ritenute idonee in rapporto con analisi del rischio, con le buone pratiche indicate dall'ACN e con il "framework" e gli standard di sicurezza, europei e nazionali, che abbiano impatto sulle infrastrutture digitali tra i quali i "data center" e i sistemi di "cloud" gestiti da Regione Toscana, sul SIR, o su sistemi di protezione della infrastruttura di rete regionale.

n) nell'acquisizione di programmi informatici adotta, in via preferenziale, software con codice a sorgente aperto, promuove il riuso e l'erogazione dei programmi in modalità "cloud", al fine di assicurare maggiore economicità alle attività della pubblica amministrazione e favorire, al tempo stesso, la concorrenza nel mercato delle soluzioni informatiche, riducendo il "lock-in" tecnologico;

o) promuove la semplificazione e standardizzazione dei procedimenti mediante il tavolo tecnico regionale dello sportello unico attività produttive (SUAP) di cui alla Delib.G.R. 7 marzo 2011, n. 129 (Modalità di organizzazione e gestione della banca dati regionale SUAP e regole tecniche per la

codificazione dei procedimenti in materia di SUAP telematico in attuazione degli articoli 37 comma 4, 42 comma 7 e 45 comma 3 della L.R. 40/2009);

p) cura la progettazione, l'organizzazione, lo sviluppo e il coordinamento della infrastruttura di rete regionale, per garantire omogeneità nei processi e standardizzazione dell'offerta di servizi integrati;

q) incentiva la promozione e la protezione dei nomi a dominio riferiti agli enti e al territorio regionale.

Articolo 7 Presidio degli ambiti strategici dell'innovazione digitale in Toscana.

In vigore dal 2 gennaio 2025

1. La Regione identifica come strategici i seguenti ambiti per il presidio della transizione digitale in Toscana, per la corretta evoluzione, il coordinamento e la gestione dei servizi digitali alla popolazione, alle imprese ed agli enti, per la protezione dei dati e dei sistemi informativi:

a) la cybersicurezza della infrastruttura di rete regionale;

b) infrastrutture digitali e datacenter gestiti da Regione Toscana, anche al fine di assicurare una adeguata migrazione degli applicativi ad architetture cloud integrate e interoperabili con le stesse;

c) le reti di telecomunicazioni per la popolazione, le imprese, gli enti pubblici;

d) la rete regionale dei responsabili per la transizione digitale delle pubbliche amministrazioni toscane aderenti alla RTRT, previsti dall'articolo 17 del decreto legislativo 7 marzo 2005 n. 82 (Codice dell'amministrazione digitale), anche in forma associata;

e) il coordinamento efficace delle iniziative regionali che promuovono la crescita delle competenze digitali nella popolazione;

f) le tecnologie basate sull'intelligenza artificiale (IA).

2. La Regione, in relazione agli ambiti strategici di cui al comma 1 coordina le politiche e le azioni per:

a) la cybersicurezza dell'infrastruttura di datacenter in gestione da parte della Regione Toscana e della infrastruttura di rete regionale;

b) la "governance", il presidio costante, il mantenimento e lo sviluppo di un centro di competenza ed operativo regionale in tema di sicurezza informatica in relazione con l'ACN, il CSIRT (Computer security incident response team) Italia, la Polizia postale e le altre organizzazioni deputate al mantenimento in sicurezza dello spazio cibernetico, nonché in raccordo con le università degli studi e gli enti di ricerca aventi sede in Toscana;

c) la governance e il presidio delle infrastrutture digitali e datacenter in coerenza con la strategia cloud europea e nazionale, perseguendo un incremento continuo dei livelli di sicurezza, resilienza e protezione di tale infrastruttura;

d) il presidio costante, l'incremento continuo e il monitoraggio del livello di copertura, di qualità del servizio e di affidabilità delle reti di telecomunicazioni in Toscana, in relazione agli organismi competenti a livello nazionale e agli operatori di telecomunicazioni del mercato, e promuovendo il continuo miglioramento nella realizzazione di infrastrutture di telecomunicazioni, al fine di garantire ai territori delle aree interne le stesse condizioni di sviluppo socio-economico dei grandi centri abitati grazie alla disponibilità di infrastrutture di telecomunicazioni, pubbliche e private, adeguate allo stato dell'arte delle tecnologie digitali;

e) il coordinamento, l'aggiornamento continuo e il supporto alla rete dei responsabili della transizione digitale degli enti aderenti alla RTRT, affinché possano diventare propulsori all'interno dei propri enti di una efficace e sicura transizione digitale dei relativi servizi e processi;

f) il coordinamento in forme strutturate e stabili di centri di facilitazione digitale sul territorio toscano, al fine di permettere a tutta la cittadinanza, con particolare attenzione alle categorie più colpite dal divario digitale, di fruire efficacemente, con continuità e con le necessarie competenze digitali, dei servizi pubblici offerti in modalità telematica dalle pubbliche amministrazioni e dagli enti che erogano servizi pubblici;

g) lo sviluppo delle tecnologie basate sull'intelligenza artificiale, perseguendo i principi definiti dalla normativa, europea e nazionale, nelle modalità e per le finalità di cui all'articolo 8.

3. Il presidio degli ambiti strategici di cui al comma 1 è rilevante per lo sviluppo coordinato della transizione digitale nel territorio toscano. La competente direzione regionale coordina il presidio di tali ambiti anche attraverso il supporto operativo del consorzio Metis di cui all'articolo 19, al fine di garantire una completa governance pubblica strutturata, stabile e duratura delle tematiche di cui al comma 1, al servizio di tutti gli enti aderenti al Consorzio Metis.

4. La Regione promuove e supporta la protezione informatica delle infrastrutture e piattaforme digitali afferenti al SIR, in attuazione di quanto previsto al comma 2.

Articolo 8 Intelligenza artificiale.

In vigore dal 2 gennaio 2025

1. La Regione, nel rispetto dell'ordinamento europeo e nazionale, tenendo conto, in particolare, dei principi di trasparenza, etica, non discriminazione, equità, responsabilità, accessibilità, inclusività, coinvolgimento delle persone e protezione dei dati personali, in accordo con la normativa di settore:

a) promuove la formazione e lo sviluppo delle competenze necessarie per gestire e applicare l'intelligenza artificiale in modo efficace nell'ambito dei servizi erogati e del supporto ai processi decisionali e operativi dell'amministrazione;

b) recepisce le indicazioni dalla normativa, europea e nazionale, circa i rischi associati all'impiego di sistemi di intelligenza artificiale nei vari ambiti e per le diverse finalità in modo da assicurare che non violino i diritti fondamentali della persona, rendere conto delle decisioni adottate e dei servizi erogati con il supporto di tecnologie di intelligenza artificiale, fornire informazioni adeguate agli utenti interessati;

c) disciplina contesti strutturati e controllati di sperimentazione al fine di testare nuovi approcci e nuove tecnologie tramite l'adozione di opportune misure di salvaguardia dei dati e di valutazione dei rischi e dei risultati connessi con l'adozione a regime delle soluzioni sperimentate;

d) tiene conto degli impatti, ambientali ed energetici, legati all'adozione di tecnologie di intelligenza artificiale, nonché del rischio di lock-in tecnologico.

2. La Giunta regionale, con propria deliberazione, definisce le possibili modalità di adozione di tecnologie e sistemi di intelligenza artificiale e il relativo impiego per i servizi amministrativi della Regione, avvalendosi dei centri di competenza di cui all'articolo 24 e delle competenze delle università degli studi e degli enti di ricerca aventi sede in Toscana, fornendo anche un supporto di indirizzo al territorio toscano.

Articolo 9 Governance dei dati.

In vigore dal 2 gennaio 2025

1. La Regione promuove azioni di sviluppo di competenze e di tecnologie di elaborazione dati al fine di migliorare le decisioni, il monitoraggio ed il governo del territorio e delle azioni della amministrazione pubblica in Toscana;

2. La governance dei dati si esplica per il tramite di indirizzi operativi e linee guida da adottarsi con deliberazione della Giunta regionale, e per mezzo di un ecosistema di basamenti informativi esposti in modalità "as a service" ossia erogati da piattaforme regionali in tecnologia cloud, nel rispetto dei principi di sicurezza informatica e tutela dei dati personali, nonché dell'uso dell'intelligenza artificiale secondo i principi di cui all'articolo 7. La governance dei dati territoriali e relativi servizi dati è disciplinata dagli articoli da 54-bis a 56 della legge regionale 10 novembre 2014, n. 65 (Norme per il governo del territorio) e relativo regolamento attuativo del sistema informativo regionale integrato per il governo del territorio.

3. Le basi di dati regionali e gli applicativi che le utilizzano, individuati nel modo previsto dall'articolo 24-quater, comma 2, del decreto legge 24 giugno 2014 n. 90 (Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziarie), includono altresm le banche dati territoriali di cui all'articolo 59 del D.Lgs. 82/2005 e alla L.R. 65/2014.

4. La Regione promuove intese istituzionali con le amministrazioni statali e gli enti pubblici nazionali per l'integrazione nel SIR e nei sistemi informativi degli enti aderenti a RTRT dei flussi informativi a scala nazionale e per l'utilizzo dei dati su scala regionale.

5. La Regione interviene con progetti mirati all'accrescimento e alla valorizzazione del patrimonio informativo pubblico, all'eliminazione di duplicazioni e ridondanze, nonché allo sviluppo di servizi e sistemi informativi integrati. A tal fine promuove intese istituzionali con gli enti locali e con altri enti pubblici, incluse le aziende sanitarie, anche sulla base di accordi che prevedano ruoli specifici, modalità di gestione dei sistemi e dei flussi informativi, modalità di fruizione delle informazioni.

Articolo 10 Gestioni associate e unioni degli enti locali.

In vigore dal 2 gennaio 2025

1. La Regione promuove le gestioni associate degli enti locali, sia attivate dalle unioni di comuni, sia tramite convenzione fra enti o in altre forme previste dalle norme, finalizzate a:

a) gestione comune delle funzioni di programmazione e coordinamento della transizione digitale;

b) gestione comune delle componenti strategiche per la trasformazione digitale e delle componenti tecnologiche fra quelle definite nel piano triennale per l'informatica nella pubblica amministrazione, emesso dall'Agenzia per l'Italia digitale (AgID) come stabilito dell'articolo 14-bis, comma 2, lettera b), del D.Lgs. 82/2005, individuate con deliberazione della Giunta regionale.

Articolo 11 Raccordi istituzionali.

In vigore dal 2 gennaio 2025

1. Nel perseguimento degli obiettivi definiti nel preambolo, la Regione Toscana coordina i propri interventi con quelli dell'Unione europea, dello Stato, delle altre regioni e degli enti locali, mediante la partecipazione al sistema delle conferenze o nelle rispettive sedi istituzionali, anche al fine di implementare azioni e interventi necessari per lo sviluppo e dell'ADT.

2. Per promuovere la più ampia collaborazione e cooperazione degli enti pubblici e delle imprese del territorio toscano la Regione definisce le modalità di collaborazione e integrazione con gli enti locali, anche attraverso la realizzazione in ambito regionale di progetti nazionali e sovranazionali.

3. Per realizzare le sinergie di cui al comma 2, la Regione:

a) può supportare lo sviluppo e l'interconnessione di infrastrutture e reti strumentali, organizzative e operative e lo sviluppo integrato di servizi attivi sulla rete della pubblica amministrazione, anche attraverso la collaborazione con tutte le amministrazioni periferiche dello Stato, i soggetti pubblici e privati e le organizzazioni sociali operanti sul territorio;

b) promuove il conseguimento di interessi pubblici e di obiettivi comuni;

c) promuove la collaborazione fra le pubbliche amministrazioni e le società in house e partecipate del territorio toscano negli ambiti della transizione digitale, nonché, nel perseguimento degli interessi pubblici, con associazioni, università degli studi e enti di ricerca aventi sede in Toscana, per garantire il costante miglioramento dei servizi;

d) sviluppa progetti di innovazione tecnologica sul territorio regionale, anche attraverso la collaborazione tra gli enti del territorio e in raccordo alle iniziative interregionali, nazionali ed europee e con l'obiettivo di evitare situazioni di divario tecnologico territoriale;

e) pianifica le azioni e gli interventi, anche promuovendo e coordinando l'utilizzo di fondi statali ed europei per lo sviluppo di progetti riguardanti l'amministrazione digitale e la garanzia dei diritti di cittadinanza digitale.

4. La competente direzione della Giunta regionale svolge attività di divulgazione e assistenza e formazione, anche attraverso il consorzio Metis di cui all'articolo 19, al fine di favorire la crescita di competenze in materia di protezione dei dati personali e sicurezza nell'utilizzo dei servizi digitali negli enti territoriali che ne facciano richiesta e di sostenere, anche nei rapporti con le autorità nazionali competenti in materia di cybersicurezza, privacy e digitalizzazione, forme di collaborazione interistituzionale su questioni di rilevanza regionale.

Articolo 12 Valorizzazione delle autonomie funzionali.

In vigore dal 2 gennaio 2025

1. La Regione può promuovere forme di collaborazione scientifica con le università degli studi e gli enti di ricerca aventi sede in Toscana, per garantire il costante miglioramento dei servizi, colmare i divari digitali, rendere le infrastrutture materiali e immateriali sempre più sicure.

2. La Regione può prevedere il coinvolgimento delle categorie professionali, delle associazioni economiche e sociali e di utenti attive negli ambiti di competenza, anche attraverso gruppi di studio e lavoro con funzioni di supporto tecnico e scientifico. Ai gruppi di studio e lavoro possono anche partecipare, con le modalità stabilite nei loro atti di organizzazione, rappresentanti delle università degli studi e degli enti di ricerca aventi sede in Toscana.

3. I gruppi di studio e di lavoro di cui al comma 2 sono istituiti con deliberazione della Giunta regionale. La partecipazione ai gruppi di lavoro è a titolo gratuito.

Articolo 13 Razionalizzazione dell'uso dei software per la pubblica amministrazione.

In vigore dal 2 gennaio 2025

1. La Regione, ai sensi dell'articolo 69 del D.Lgs. 82/2005, al fine di favorire la sostenibilità dei processi di innovazione tecnologica, organizzativa ed operativa delle pubbliche amministrazioni, promuove il riuso dei programmi informatici di cui le stesse abbiano la disponibilità.

2. La Regione promuove altresм l'adozione di tecnologie e soluzioni basate su "cloud computing".

Articolo 14 Agenda digitale della Toscana (ADT.

In vigore dal 2 gennaio 2025

1. La Giunta regionale approva l'ADT.

2. La Regione definisce, di norma nell'ambito del programma regionale di sviluppo (PRS) di cui all'articolo 7 della legge regionale 7 gennaio 2015, n. 1 (Disposizioni in materia di programmazione economica e finanziaria regionale e relative procedure contabili. Modifiche alla L.R. 20/2008), gli indirizzi, gli obiettivi, le linee guida, le strategie tecniche e le tipologie di intervento in tema di promozione e sviluppo dell'ADT al fine di garantire i diritti di cittadinanza digitale, coordinare le azioni per la crescita digitale della Regione e dare impulso all'amministrazione digitale.

3. Il documento di economia e finanza regionale (DEFR) di cui all'articolo 8 della L.R. 1/2015, individua gli interventi da realizzare tenuto conto degli stanziamenti del bilancio di previsione, definisce gli obiettivi specifici, le scadenze principali, le misure organizzative di supporto, gli indicatori chiave di prestazione (Key performance indicators "KPI") le altre iniziative necessarie per l'attuazione degli interventi e i benefici attesi.

4. All'ADT possono riferirsi, nei propri atti di indirizzo in tema di trasformazione digitale, i soggetti di cui all'articolo 17, comma 2.

5. Per le finalità di cui all'articolo 1 e nel rispetto dei rispettivi ambiti di autonomia, gli enti locali coordinano i propri interventi con quelli definiti nella programmazione regionale attraverso la partecipazione alle attività e ai progetti condivisi nell'ambito della RTRT, nonché attraverso eventuali strumenti negoziali di attuazione.

6. L'ADT recepisce l'indice delle attività statistiche regionali, come componente specializzata delle attività della RTRT, elaborato dalla Commissione statistica regionale.

7. L'ADT definisce gli indirizzi operativi e le linee d'azione da seguire per dare concreta attuazione a livello regionale alla strategia nazionale per la cybersicurezza secondo quanto indicato dalla disciplina nazionale ed europea.

Articolo 15 Strumenti di attuazione dell'ADT.

In vigore dal 2 gennaio 2025

1. Le strategie indicate nell'ADT sono declinate in indicazioni operative, obiettivi e risultati attesi, riconducibili all'azione amministrativa della Regione.

2. Il documento di linee di indirizzo della RTRT, di cui all'articolo 18, comma 2, lettera a), declina i contenuti dell'ADT sul territorio regionale, proponendone anche aggiornamenti.

Articolo 16 Computer security incident response team della Toscana (CSIRT Toscana.

In vigore dal 2 gennaio 2025

1. Del Computer security incident response team della Toscana (CSIRT Toscana) istituito sulla base di un accordo stipulato tra la Regione Toscana e l'ACN in qualità di autorità competente a livello nazionale in base alla direttiva 2022/2555/UE del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), fanno parte la Regione Toscana e le aziende e gli enti del SSR cosm come definito dalla legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale).

2. Il CSIRT Toscana, nei limiti di quanto definito dai propri atti costitutivi, esercita le seguenti competenze:

a) monitoraggio e analisi dei rischi e delle minacce cyber a livello regionale;

b) emissione di preallarmi, allerte, annunci e la divulgazione di rilevanti informazioni agli operatori interessati;

c) ricezione di notifiche obbligatorie e volontarie di incidenti cyber, veicolandole laddove previsto alle autorità nazionali competenti, l'analisi degli incidenti e la definizione di modalità di intervento e risposta;

d) interventi in caso di incidente;

e) analisi dinamica dei rischi e degli incidenti;

f) sensibilizzazione situazionale verso la sicurezza e resilienza cyber;

g) partecipazione alla rete degli CSIRT italiani;

h) ogni altra funzione conferita dall'ACN;

i) ogni altro compito individuato con la deliberazione di cui al comma 4, in conformità alla normativa di settore.

3. La Giunta regionale con propria deliberazione, disciplina l'organizzazione e il governo dello CSIRT Toscana, nonché le modalità di adesione allo stesso.

4. La Giunta regionale attua quanto previsto al comma 2 anche tramite il Consorzio Metis di cui all'articolo 19, e con l'eventuale apporto scientifico-tecnico delle università degli studi e degli enti di ricerca aventi sede in Toscana.

CAPO II

Rete telematica della regione toscana, governance e strumenti dell'innovazione digitale

Articolo 17 Rete telematica regionale toscana (RTRT.

In vigore dal 2 gennaio 2025

1. La RTRT è un modello organizzativo, comunità e forma stabile di coordinamento del sistema regionale delle autonomie locali ed altri soggetti, fondato sul concetto della condivisione degli obiettivi, della cooperazione e della compartecipazione di infrastrutture digitali comuni, capace di produrre e sostenere processi di innovazione digitale. La RTRT è composta dalla Regione e dai seguenti soggetti:

a) gli enti, aziende, ed agenzie regionali e altri organismi pubblici dipendenti, incluse le società in house della Regione;

b) gli enti e le aziende sanitarie pubbliche e gli enti e aziende del servizio socio-sanitario regionale.

2. Partecipano alla RTRT, mediante convenzione di adesione alla rete, i seguenti enti toscani:

a) la Città metropolitana di Firenze;

b) le province;

c) i comuni, singoli o associati, e le unioni di comuni.

3. La Giunta regionale può prevedere forme particolari di partecipazione alla RTRT per i seguenti soggetti della Toscana:

a) le università degli studi e gli enti di ricerca;

b) le amministrazioni periferiche dello Stato, previo accordo;

c) le società in house e le aziende di servizi pubblici locali;

d) le camere di commercio, industria, artigianato e agricoltura, e le altre autonomie funzionali;

e) le categorie economiche, le libere professioni e le altre associazioni;

f) le società partecipate degli enti di cui ai commi l e 2 che si occupano di tecnologie informatiche e telecomunicazioni;

g) i soggetti del servizio socio-sanitario regionale.

4. La direzione tecnico-operativa di cui all'articolo 18, predispone le convenzioni di adesione alla RTRT e gli eventuali accordi attuativi su progetti specifici ai sensi della legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi). Convenzioni ed accordi definiscono l'organizzazione e le modalità della collaborazione tra la Regione ed i soggetti di cui al comma 3 per l'attuazione degli interventi e misure previsti dalla presente legge.

5. Le attività di sviluppo, conduzione e gestione della RTRT, costituenti servizio di interessi generale ai sensi dell'articolo 1, sono improntate a principi di organicità progettuale, efficienza operativa ed economica.

Articolo 18 Organizzazione e funzioni della RTRT. Commissione statistica regionale.

In vigore dal 2 gennaio 2025

1. Sono organi della RTRT:

a) l'assemblea;

b) la direzione tecnico-operativa (DTO);

c) la segreteria.

2. L'assemblea è presieduta dal Presidente della Giunta regionale, o suo delegato, ed è composta dai rappresentanti dei soggetti aderenti alla RTRT. L'assemblea svolge i seguenti compiti:

a) approva annualmente il documento di linee di indirizzo della RTRT che individua le esigenze comuni in termini di infrastrutture e servizi relativi alle tecnologie dell'informazione e della comunicazione (TIC) dei soggetti della RTRT; il documento è recepito dalla Giunta regionale per l'aggiornamento dell'ADT di cui all'articolo 14;

b) funzioni di indirizzo generale e proposta in relazione alle attività e ai progetti della stessa;

c) può istituire presso la direzione tecnico-operativa un osservatorio degli utenti, al fine di favorire l'efficacia dei servizi digitali e promuovere la partecipazione dei cittadini;

d) disciplina la propria organizzazione con atto approvato dalla maggioranza dei componenti.

3. La direzione tecnico-operativa:

a) è presieduta dal responsabile transizione digitale (RTD) di Regione Toscana con compiti di coordinamento e di presentazione, all'assemblea della RTRT, del documento di linee di indirizzo della RTRT stessa;

b) è composta dai responsabili tecnici indicati dai soggetti che costituiscono la RTRT e dal responsabile tecnico individuato dal Consorzio Metis. Per i soggetti che rientrano nell'ambito di applicazione dell'articolo 2, comma 2, del D.Lgs. 82/2005, il rappresentante tecnico coincide con il RTD;

c) predispone il documento di linee di indirizzo della RTRT, che è presentato all'assemblea della RTRT a cura del RTD della Regione;

d) predispone lo schema di convenzione di cui all'articolo 17, comma 4;

e) può istituire gruppi di lavoro, anche temporanei, in relazione a specifiche progettualità o argomenti di comune interesse. Ai gruppi di lavoro possono candidarsi a partecipare rappresentanti o referenti indicati dagli enti aderenti alla RTRT.

4. La direzione presso cui opera il RTD della Regione assicura le funzioni di segreteria della RTRT con compiti di supporto tecnico e organizzativo, anche mediante eventuale collaborazione dei soggetti pubblici della Rete ed eventuale comando di personale.

5. La Commissione statistica regionale è composta dai responsabili degli uffici di statistica scelti dall'assemblea della RTRT, che ne disciplina le funzioni, la composizione e l'organizzazione su proposta della DTO. La Commissione statistica:

a) coordina il sistema statistico regionale e svolge le funzioni di raccordo, di orientamento e sviluppo degli interventi in materia statistica nell'ambito della Rete.

b) predispone l'indice delle attività statistiche regionali, come componente specializzata del piano di attività annuale della Rete.

6. La partecipazione e le attività di cui al presente articolo sono svolte a titolo gratuito e senza oneri.

Articolo 19 Consorzio Metis.

In vigore dal 2 gennaio 2025

1. La Regione mantiene la partecipazione al consorzio Metis cui ha aderito ai sensi dell'articolo 19 della legge regionale 20 luglio 2018, n. 37 (Interventi normativi relativi alla prima variazione al bilancio di previsione 2018 - 2020), alle seguenti condizioni:

a) totale ed esclusivo capitale pubblico;

b) svolgimento, anche in via non esclusiva, di servizi strumentali agli enti consorziati nella materia di cui alla presente legge. Per le materie relative all'innovazione digitale, oggetto della presente legge ed afferenti al settore sanitario e della salute, l'ambito di attività del consorzio Metis è regolato dalla L.R. 40/2005 per ciò che riguarda i rapporti con le aziende sanitarie e l'Ente di supporto tecnico amministrativo regionale (ESTAR).

2. La partecipazione da parte della Regione al Consorzio Metis è subordinata:

a) alla condizione che lo statuto:

1) preveda che la Regione eserciti il controllo sul consorzio Metis, analogo a quello esercitato sulle proprie strutture organizzative, sulla base della definizione preventiva, d'intesa tra la Regione, gli enti pubblici e gli altri soggetti soci, degli indirizzi da imprimere all'azione del consorzio Metis, nonché delle modalità di verifica dei risultati;

2) stabilisca le ulteriori modalità di controllo, da parte della Regione e degli altri soggetti aderenti, attribuite all'assemblea del consorzio Metis stesso;

b) alla condizione che l'oggetto del Consorzio Metis preveda:

1) gli ambiti strategici dell'innovazione digitale in Toscana di cui all'articolo 7, comma 1;

2) la sperimentazione di tecnologie innovative e relative applicazioni.

3. La Giunta regionale, effettuata la verifica delle condizioni di cui al comma 2, conferma la partecipazione al consorzio Metis di cui al presente articolo ai sensi dell'articolo 4, comma 2, della legge regionale 28 aprile 2008, n. 20 (Disciplina della partecipazione regionale a società, associazioni, fondazioni e altri organismi di diritto privato, ai sensi dell'articolo 51, comma 1 dello Statuto. Norme in materia di componenti degli organi amministrativi delle società a partecipazione regionale).

4. Il Presidente della Giunta regionale, previa deliberazione della Giunta e nel rispetto del D.Lgs. 82/2005, può conferire al consorzio Metis, o trasferire ad esso, beni o complessi o universalità di beni, sia mobili, sia immobili, di cui la Regione stessa sia proprietaria. Il decreto del Presidente della Giunta costituisce titolo per la trascrizione nei registri immobiliari.

Articolo 20 Rapporti con il consorzio Metis.

In vigore dal 2 gennaio 2025

1. La Regione e gli enti che sono consorziati al consorzio Metis regolano i rapporti con il consorzio stesso tramite apposita convenzione.

CAPO III

Sistema informativo regionale

Articolo 21 Sistema informativo regionale (SIR.

In vigore dal 2 gennaio 2025

1. Il SIR è il sistema unitario del patrimonio informativo della Regione e degli enti dipendenti, finalizzato a garantire qualità e coerenza nella gestione, analisi dei dati e delle informazioni, degli obiettivi di interesse regionale, senza pregiudizio delle competenze di ciascun soggetto nel

trattamento dei propri dati. Il SIR costituisce lo strumento di collaborazione, coordinamento e reciproca informazione con lo Stato, con le regioni e le province autonome, con gli enti pubblici nazionali, con le università degli studi e con le istituzioni di cultura e di ricerca, con le associazioni e gli altri soggetti privati che operano in ambito regionale per finalità di interesse pubblico.

2. Il SIR è disciplinato dall'insieme delle regole tecniche europee, nazionali e regionali che garantiscono l'interoperabilità, confrontabilità e circolarità dei dati e delle informazioni all'interno e verso gli altri livelli istituzionali o territoriali, attraverso l'infrastruttura di rete regionale.

3. La direzione competente della Giunta regionale coordina il SIR con l'obiettivo di garantire l'interoperabilità dei sistemi informativi e dei dati attraverso l'infrastruttura di rete regionale e la confrontabilità, l'aggiornamento e l'affidabilità dei dati e delle informazioni che lo costituiscono ed inoltre:

a) definisce gli standard di riferimento;

b) valorizza le risorse informative regionali;

c) garantisce lo sviluppo dei servizi per i cittadini e i soggetti economici in base a criteri di unificazione dei punti di accesso ai servizi, di semplificazione amministrativa e di trasparenza e controllo della spesa pubblica.

4. Per le finalità di cui al comma 1, la Regione opera affinché il SIR:

a) sia conformato per ottenere e utilizzare le informazioni determinanti per le funzioni di governo, programmazione, amministrazione e controllo della Regione e degli altri enti pubblici operanti sul territorio regionale, nonché per le funzioni inerenti all'assolvimento degli obblighi di informazione verso lo Stato e gli enti ad esso collegati ai sensi della legislazione vigente;

b) valorizzi le risorse informative già esistenti sul territorio regionale e ne garantisca l'interoperabilità con i sistemi informativi statali.

5. Tra le funzioni inerenti all'assolvimento degli obblighi di informazione di cui al comma 4, lettera a), sono comprese quelle statistiche disciplinate dalla legge regionale 5 ottobre 2009, n. 54 (Istituzione del sistema informativo e del sistema statistico regionale).

Articolo 22 Organizzazione del SIR.

In vigore dal 2 gennaio 2025

1. La Giunta regionale disciplina, con proprio atto, il funzionamento del SIR definendo:

a) il modello di governance, organizzativo, architetturale;

b) la ripartizione delle competenze fra le direzioni della Giunta regionale e gli altri soggetti che costituiscono il SIR.

2. Al fine di garantire il processo di attivazione e conduzione del SIR, la Regione può promuovere attività formative per il personale anche all'interno della RTRT nell'ambito delle risorse previste per la formazione del personale regionale.

3. La Regione e gli enti dipendenti non implementano sistemi informativi ulteriori quando è possibile l'uso o l'ampliamento delle funzioni di quelli già esistenti nell'ambito del SIR.

CAPO IV

Disposizioni attuative e strumenti di innovazione

Articolo 23 Amministrazione digitale in Toscana.

In vigore dal 2 gennaio 2025

1. La competente direzione della Giunta regionale esercita le funzioni dirette all'attuazione della presente legge e allo svolgimento di attività di assistenza e supporto ai soggetti di cui all'articolo 1, in materia di amministrazione digitale ed innovazione nelle pubbliche amministrazioni.

Articolo 24 Convenzioni e centri di competenza.

In vigore dal 2 gennaio 2025

1. La Giunta regionale può istituire, anche prevedendo forme di cofinanziamento, specifici centri di competenza regionali, in collaborazione con soggetti pubblici o privati, con finalità di ricerca scientifica, innovazione tecnologica e trasferimento di conoscenze alla pubblica amministrazione.

2. I centri di competenza di cui al comma 1 perseguono altresm obiettivi di verifica metodologica e scientifica di metodi, modelli, soluzioni e piattaforme rispetto alla normativa europea, nazionale e allo stato dell'arte della ricerca in materia.

Articolo 25 Regulatory sandboxes.

In vigore dal 2 gennaio 2025

1. Per "regulatory sandboxes" si intendono quadri controllati istituiti da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione e per un periodo di tempo limitato sotto supervisione regolamentare.

2. Negli ambiti di propria competenza, nel rispetto delle competenze statali e in raccordo con le competenti autorità nazionali, la Regione può implementare regulatory sandboxes come strumento di studio e sperimentazione di processi e tecnologie in ambiti particolarmente innovativi, tra i quali l'IA e la cybersicurezza, laddove non vietato da norme europee o nazionali.

3. La Giunta regionale, con proprio atto, approva le linee guida per disciplinare i principi e le modalità di conduzione delle sperimentazioni di cui al comma 1.

CAPO V

Istituzione del sistema statistico regionale. modifiche alla L.R. 54/2009

Articolo 26 Modifiche al titolo della L.R. 54/2009.

In vigore dal 2 gennaio 2025

1. Nel titolo della L.R. 54/2009 le parole: "del sistema informativo e" e le parole: "Misure per il coordinamento delle infrastrutture e dei servizi per lo sviluppo della società dell'informazione e della conoscenza", sono soppresse.

Articolo 27 Modifiche al preambolo della L.R. 54/2009.

In vigore dal 2 gennaio 2025

1. Il preambolo della L.R. 54/2009 è cosm modificato:

a) nei "visto":

1) le parole: "Visto l'articolo 63, comma 2, dello Statuto regionale;" sono sostituite dalle seguenti: "Visto il 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);";

2) le parole: "Vista la legge regionale 26 gennaio 2004, n. 1 (Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale. Disciplina della "Rete telematica regionale toscana")" sono sostituite dalle seguenti: "Visto il decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400)";

3) dopo le parole: "Visto il decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400)", sono aggiunte le seguenti: "Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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)";

4) dopo le parole: "Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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)", sono aggiunte le seguenti: "Vista la legge regionale 9 dicembre 2024, n. 57 (Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla L.R. 54/2009);".

b) nei "considerato":

1) sono abrogati i numeri da 1 a 12;

2) al numero 13 le parole: "coordinandosi con sistema informativo regionale" sono sostituite dalle seguenti: "coordinato con il sistema informativo regionale di cui alla L.R. 57/2024";

3) dopo il numero 13 è inserito il seguente:

"13-bis: "la legge specifica e dettaglia le funzioni dell'ufficio di statistica della Regione, nel rispetto ed in attuazione del D.Lgs. 322/1989.".

Articolo 28 Ordinamento del sistema statistico regionale Modifiche all'articolo 28 della L.R. 54/2009.

In vigore dal 2 gennaio 2025

1. All'articolo 28, comma 2, della L.R. 54/2009 le parole: "al capo II della L.R. 1/2004" sono sostituite dalle seguenti: "alla legge regionale 9 dicembre 2024, n. 57 (Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla L.R. 54/2009).".

Articolo 29 Organizzazione dell'attività statistica della Regione Sostituzione dell'articolo 31 della L.R. 54/2009.

In vigore dal 2 gennaio 2025

1. L'articolo 31 della L.R. 54/2009 è sostituito dal seguente:
"Art. 31
Organizzazione dell'attività statistica della Regione
1. Le funzioni dell'ufficio di statistica della Regione, di cui all'articolo 5 del D.Lgs. 322/1989, sono esercitate dalla struttura individuata ai sensi della legge regionale 8 gennaio 2009, n. 1 (Testo unico in materia di organizzazione e ordinamento del personale).
2. L'Ufficio di statistica è titolare delle attività statistiche ufficiali della Regione e, oltre alle funzioni di cui all'articolo 6, comma 1, del D.Lgs. 322/1989:
a) garantisce la qualità dei processi statistici e ne valida i risultati;
b) garantisce gli adempimenti previsti dal programma statistico nazionale (PSN);
c) predispone ed aggiorna il programma statistico regionale (PSR);
d) assicura il rispetto delle norme e delle procedure del sistema statistico nazionale (SISTAN);
e) cura i rapporti con l'Istituto nazionale di statistica (ISTAT), il raccordo con le istituzioni e le altre autorità statistiche a livello nazionale e il coordinamento con il livello interregionale;
f) promuove l'utilizzo degli archivi amministrativi per finalità statistiche e ne garantisce l'uso corretto a fini conoscitivi, di studio e di programmazione;
g) può accedere a tutte le banche dati dell'amministrazione regionale per le finalità statistiche previste dal PSR e dal PSN;
h) promuove le intese volte a consentire la partecipazione dei soggetti, pubblici e privati, al SISTAR di cui all'articolo 28;
i) svolge funzioni di raccordo con il SISTAR di cui all'articolo 28, promuovendo lo svolgimento di attività statistiche comuni, comprese la formazione, la condivisione di fonti e metodologie e il riuso di applicativi;
j) coordina le attività statistiche ufficiali dell'amministrazione regionale, raccordandosi con le relative strutture organizzative;
k) provvede all'applicazione di metodologie statistiche di campionamento a supporto del sistema dei controlli di competenza regionale e a supporto delle funzioni di audit;
l) realizza indagini statistiche rilevanti per le esigenze conoscitive dell'amministrazione regionale qualora i dati di interesse non siano disponibili presso il SISTAN;
m) esercita le azioni idonee a ottenere e trattare in modo disaggregato per genere, ove possibile, i dati contenuti nei registri, indagini statistiche o altri sistemi informativi disciplinati dalla presente legge;
n) approfondisce e studia i risultati delle rilevazioni previste nel PSN e PSR, anche in collaborazione con l'Istituto regionale per la programmazione economica della Toscana (IRPET) e con le università degli studi toscane;
o) pubblica e diffonde le informazioni statistiche prodotte dalla Regione;
p) partecipa alla definizione e allo sviluppo del SISTAR e dei vari osservatori regionali.
3. La Giunta regionale approva il PSR ed i relativi aggiornamenti. Il PSR:
a) pianifica le attività statistiche ufficiali della Regione;
b) è predisposto con cadenza triennale, ed è aggiornato annualmente;
c) identifica le attività statistiche obbligatorie per le pubbliche amministrazioni ai sensi dell'articolo 33.
4. Ai sensi del 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) e del D.Lgs. 196/2003, il dirigente preposto all'Ufficio regionale di statistica agisce in qualità di delegato del titolare per il trattamento dei dati personali per gli scopi statistici previsti nel PSR.".

Articolo 30 Obbligo di fornire dati statistici. Sostituzione dell'articolo 33 della L.R. 54/2009.

In vigore dal 2 gennaio 2025

1. L'articolo 33 della L.R. 54/2009 è sostituito dal seguente:
"Articolo 33
Obbligo di fornire i dati statistici
1. Fatto salvo quanto previsto dall'articolo 7, comma 2, del D.Lgs. 322/1989, le pubbliche amministrazioni, gli enti ed organismi pubblici e privati, nonché le persone fisiche, forniscono i dati e le notizie richiesti per le rilevazioni concernenti:
a) le informazioni statistiche ufficiali delle rilevazioni, dei progetti e delle elaborazioni di interesse regionale e locale affidati al SISTAR;
b) le priorità in relazione alle indagini e alle analisi statistiche da effettuare a livello regionale, nonché le specifiche risorse finanziarie da destinare alle medesime.
2. Nel quadro della normativa vigente, la Giunta regionale disciplina la trasmissione dei dati e delle notizie di cui al comma 1 tra i diversi soggetti adottando, in via generale, modalità telematiche di trasmissione, secondo quanto previsto dalla presente legge.
3. Per le statistiche di cui al comma 1 aventi ad oggetto di indagine i settori per i quali sono previsti contributi o finanziamenti regionali, gli strumenti per lo sviluppo delle infrastrutture e dei servizi digitali previsti dalla L.R. 57/2024, nonché i relativi atti attuativi della Giunta regionale, possono prevedere la sospensione o la revoca dei finanziamenti nei confronti dei soggetti pubblici e privati che non adempiono gli obblighi di cui ai commi 1 e 2.".

CAPO VI

Disposizioni finali

Articolo 31 Abrogazioni.

In vigore dal 2 gennaio 2025

1. Sono o restano abrogate le seguenti disposizioni:

a) la legge regionale 26 gennaio 2004, n. 1 (Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale. Disciplina della "Rete telematica regionale toscana");

b) gli articoli della L.R. 54/2009:

1) da 1 a 27;

2) da 36 a 44.

Articolo 32 Clausola di neutralità finanziaria.

In vigore dal 2 gennaio 2025

1. Dall'attuazione della presente legge non derivano nuovi o maggiori oneri a carico del bilancio regionale rispetto alla legislazione previgente. Il finanziamento degli interventi di cui alla presente legge è assicurato con le risorse regionali già stanziate sul bilancio regionale come segue:

a) euro 12.197.362,12 per l'anno 2024, euro 11.445.750,17 per l'anno 2025 ed euro 11.943.066,75 per l'anno 2026, disponibili nell'ambito della Missione 1 "Servizi istituzionali, generali e di gestione", Programma 08 "Statistica e sistemi informativi", Titolo 1 "Spese correnti" del bilancio di previsione 2024 - 2026;

b) euro 3.543.167,25 per l'anno 2024, euro 4.079.457,75 per l'anno 2025, euro 3.354.640,30 per l'anno 2026, disponibili nell'ambito della Missione 1 "Servizi istituzionali, generali e di gestione", Programma 08 "Statistica e sistemi informativi", Titolo 2 "Spese in conto capitale" del bilancio di previsione 2024 - 2026;

c) euro 8.000,00 per ciascuno degli anni 2024, 2025 e 2026, disponibili nell'ambito della Missione Servizi istituzionali, generali e di gestione", Programma 02 "Segreteria generale", Titolo 1 "Spese correnti" del bilancio di previsione 2024 - 2026;

d) euro 590.000,00 per ciascuno degli anni 2024, 2025 e 2026, disponibili nell'ambito della Missione 15 "Politiche per il lavoro e la formazione professionale", Programma 01 "Servizi per lo sviluppo del mercato del lavoro", Titolo 1 "Spese correnti" del bilancio di previsione 2024 - 2026.

2. Agli oneri per gli esercizi successivi si fa fronte con legge di bilancio.

La presente legge è pubblicata sul Bollettino Ufficiale della Regione.

È fatto obbligo a chiunque spetti di osservarla e farla osservare come legge della Regione Toscana.

Regione Umbria - Legge regionale n. 25 del 04/11/2024 - Art. 16

Modificazioni e integrazioni di leggi regionali per la semplificazione, la digitalizzazione e il taglio di adempimenti.

(…)

Art. 16

Modificazioni all'articolo 1 della legge regionale 29 aprile 2014, n. 9.

CAPO VI

Modificazioni alla legge regionale 29 aprile 2014, n. 9 (norme in materia di sviluppo della società dell'informazione e riordino della filiera ict (information and communication technology) regionale)

1. All' articolo 1 della legge regionale 29 aprile 2014, n. 9 (Norme in materia di sviluppo della società dell'informazione e riordino della filiera ICT (Information and Communication Technology) regionale) sono apportate le seguenti modificazioni:

a) alla lettera f) del comma 1 il segno di punteggiatura: "." è sostituito con il seguente: ";";

b) dopo la lettera f) del comma 1 sono aggiunte le seguenti:

"f-bis) l'innalzamento dei livelli di cybersicurezza delle pubbliche amministrazioni e della consapevolezza in materia di cittadini e imprese;

f-ter) la sostenibilità digitale;

f-quater) la diffusione della sanità digitale e della telemedicina;

f-quinquies) l'uso dell'intelligenza artificiale, secondo modalità etiche e responsabili;

f-sexies) l'impiego del cloud computing, dell'automazione dei processi, dell'intelligenza artificiale, dell'internet delle cose e di altre tecnologie emergenti;

f-septies) la semplificazione amministrativa secondo gli obiettivi della legge regionale 16 settembre 2011, n. 8 (Semplificazione amministrativa e normativa dell'ordinamento regionale e degli Enti locali territoriali).";

c) alla fine della lettera c) del comma 2, il segno di punteggiatura: "." è soppresso e dopo le parole: "privato (eleadership)" sono aggiunte le seguenti: ", le competenze necessarie per una piena cittadinanza digitale;";

d) dopo la lettera c) del comma 2 è aggiunta la seguente:

"c-bis) istituisce un osservatorio sulla trasformazione digitale, per il monitoraggio dello stato della digitalizzazione del settore pubblico e privato nonché dei risultati ottenuti dall'agenda digitale. La Giunta regionale con apposito atto definisce la composizione, le modalità di funzionamento e i compiti dell'Osservatorio medesimo. Ai componenti dell'Osservatorio non spetta alcuna indennità, compenso e rimborso spese comunque denominato.".

(…)

Regione Campania - Legge regionale 15/05/2024, n. 6 – Art.17

Ordinamento e organizzazione degli uffici della Giunta regionale.

(…)

Art. 17 Istituzione degli Uffici Speciali.

1. Sono istituiti i seguenti Uffici speciali:

a) Ufficio per l'amministrazione digitale.

Ambiti di competenza: transizione alla modalità operativa digitale; attività relative a infrastrutture digitali, fonia fissa e mobile, servizi ed ecosistemi digitali, piattaforme abilitanti e sicurezza informatica, intelligenza artificiale; politiche regionali di sviluppo della banda ultralarga; politiche di e-government, comunità intelligenti e patrimonio pubblico informativo; ufficio statistica;

b) Ufficio Appalti - Centrale di committenza regionale.

Ambiti di competenza: stazione appaltante per l'acquisizione di beni, servizi e lavori da parte delle strutture della Giunta regionale; Programmazione triennale dei servizi e dei lavori di competenza regionale; Osservatorio regionale degli appalti pubblici e prezzario regionale dei lavori pubblici; sulla base di apposite convenzioni, in conformità alla disciplina in materia, può svolgere funzioni di centrale di committenza per il Consiglio regionale, per gli enti strumentali della Regione e per gli enti locali;

c) Ufficio Opere pubbliche e interventi strategici.

Ambiti di competenza: edilizia scolastica, edilizia sanitaria, interventi di riqualificazione urbana e ambientale, altri interventi strategici di interesse regionale. Autorità espropriante ai sensi del decreto del Presidente della Repubblica 8 giugno 2001, n. 327 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche);

d) Ufficio Legalità e sicurezza integrata, sistemi territoriali, immigrazione.

Ambiti di competenza: ufficio del responsabile della prevenzione della corruzione e della trasparenza (RPCT), accesso civico; politiche per la promozione della legalità, della sicurezza e per l'immigrazione; beni confiscati; rapporti con il sistema delle autonomie locali e con gli enti di diritto privato. Aree interne;

e) Ufficio Controlli.

Ambiti di competenza: vigilanza e controllo sugli enti in house e partecipati dalla Regione Campania, in raccordo con le Direzioni generali competenti per materia; controlli interni; controllo di gestione;

f) Ufficio Valutazioni Ambientali.

Ambiti di competenza: Autorità competente in materia di Valutazione di Impatto Ambientale (PAUR-VIA), di Valutazione Ambientale Strategica (VAS) e di Valutazione di Incidenza (VIncA);

g) Autorità di Gestione Fondo sociale europeo - Autorità responsabile piano per lo sviluppo e la coesione.

Ambiti di competenza: responsabile del programma regionale del Fondo Sociale Europeo e Attività previste dai regolamenti UE. Programmazione, gestione e controllo degli interventi previsti e coordinamento delle attività. Gestione del Fondo per lo sviluppo e la coesione;

h) Autorità di Gestione Fondo Europeo di Sviluppo Regionale (FESR).

Ambiti di competenza: responsabile del programma operativo regionale del FESR e attività previste dai Regolamenti UE. Programmazione, gestione e controllo degli interventi e coordinamento delle attività.

(...)

CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

23/214/CR08/C14

POSIZIONAMENTO SULL'INTELLIGENZA ARTIFICIALE DELLE REGIONI E PROVINCE AUTONOME

In occasione dell'**AI Safety summit 2023**, tenutosi lo scorso Novembre nel Regno Unito, i governi di 28 paesi, tra cui l'Italia, hanno sottoscritto un documento (c.d. dichiarazione di Bletchley) in cui si evidenzia come l'intelligenza artificiale abbia *"il potenziale per trasformare e migliorare il benessere umano, la pace e la prosperità"*, ma perché ciò avvenga è necessario che la tecnologia sia "*progettata, sviluppata, implementata e utilizzata in modo sicuro, in modo da essere centrata sull'essere umano"*. Sempre nella stessa occasione il nostro Presidente del Consiglio ha dichiarato: *"Serve un quadro normativo adeguato in cui innovazione e regolazione vadano di pari passo… Vogliamo una tecnologia che garantisca inclusione e uguaglianza"*. Inoltre, il Governo italiano nel 2024 si appresta a svolgere un importante ruolo guida per la discussione del tema AI in ambito G7.

Come Conferenza delle Regioni e delle Province autonome ci siamo già espressi anche in sede di Comitato interministeriale per la transizione digitale (CITD), **condividendo la necessità di rivedere la Strategia nazionale sull'intelligenza artificiale (2022-2024)** per portarla al passo dei grandi investimenti che altri Paesi stanno già facendo in questa nuova opportunità tecnologica. Abbiamo quindi accolto con favore l'istituzione, lo scorso 23 ottobre, del **Comitato di esperti sull'Intelligenza Artificiale** e auspichiamo che al lavoro della relativa **Segreteria tecnica sull'intelligenza artificiale** possano contribuire, già nell'immediato, anche le Regioni e le Province autonome, all'interno di un percorso collaborativo per la definizione di questa nuova strategia, portando a valore anche le nascenti esperienze regionali in questo ambito.

In virtù di quanto premesso, gli aspetti su cui le Regioni e le Province autonome richiamano l'attenzione del Governo - aspetti sui quali la stessa commissione ITD sta ragionando, anche nell'ambito della *community* inter-regionale "Dati & AI" - sono i seguenti:

1. **Riconoscere il ruolo delle Regioni rispetto alla definizione di criteri e casi d'uso** in cui l'impiego dell'intelligenza artificiale sia davvero fattore di miglioramento dei processi interni alla PA. Il gap tecnologico in materia AI del nostro Paese è evidente sia nel settore privato che nel pubblico, ma siamo consapevoli che gli algoritmi di intelligenza artificiale possono portare grandi benefici alle attività delle organizzazioni, alla loro efficienza e produttività e, di conseguenza, alla competitività e al benessere del Paese.

2. **Riflettere sulla straordinaria opportunità dello sviluppo dell'intelligenza artificiale, di un'importanza cruciale da conciliarsi con l'aspetto etico dei suoi utilizzi tenendo conto, però, che questo non può bloccarne lo sviluppo anche a livello nazionale e l'impiego in ogni settore**. Temi come la trasparenza e la conoscibilità della logica degli algoritmi, la non discriminazione, la responsabilità e il contributo/controllo umano nelle decisioni automatizzate (c.d. "riserva di umanità") sono da considerarsi nel procedere con la modernizzazione e l'evoluzione della tecnologia e delle sue applicazioni al mondo della Pubblica Amministrazione e del privato. È fondamentale garantire che

l'azione amministrativa, portata avanti anche con gli algoritmi, rispetti i principi previsti dalla Costituzione. In questo senso, le Regioni possono contribuire a definire linee guida e normative specifiche per l'implementazione dell'AI e a darne una contestuale attuazione, anche in forma sperimentale, nel rispetto dei valori e delle specifiche esigenze delle comunità territoriali. Le Regioni possono, inoltre, promuovere un approccio etico all'AI incoraggiando la collaborazione tra settore pubblico, privato e accademico per sviluppare soluzioni tecnologiche che rispettino standard e processi di digitalizzazione condivisi nei territori anche nell'ottica di abbattimento del *digital divide*. Le Regioni infine possono promuovere la creazione di registri pubblici relativi all'uso di algoritmi da parte delle Pubbliche Amministrazioni per garantire la trasparenza nel loro uso nei confronti dei cittadini.

3. **Attivare investimenti con fondi nazionali, che vedano Regioni e Province autonome come soggetti attuatori**, per avere **"dati pubblici pronti per la AI"**, anche, ove possibile, come dati aperti utili per lo sviluppo di algoritmi AI nell'ambito della ricerca e del settore privato. La gestione dei dati pubblici (metadatazione/bonifica/valorizzazione) è un fattore abilitante per costruire degli algoritmi di addestramento davvero efficaci ed efficienti, e non è finanziato in modo specifico all'interno delle misure PNRR. Risulta di fondamentale importanza, di conseguenza, guardare anche alla qualità del dato e non solo al numero di dataset disponibili. Ad oggi, i dati delle PA sono spesso poco curati e di scarsa qualità, mancano processi strutturati di *"data governance",* e di conseguenza, il rischio è quello di non farci trovare pronti per sfruttare gli algoritmi AI nelle PA. Inoltre, come già sottolineato in altri posizionamenti, molti dati pubblici sono "irraggiungibili" in quanto ancora su carta; allo stesso modo, va affrontato il tema della "dematerializzazione" degli archivi, che non vede finanziamenti specifici nelle misure PNRR. Una simile strategia permetterebbe anche di rendere sinergica l'attuazione di *"data spaces"* nazionali/europei, sfruttando e applicando tanto le previsioni sugli Open Data quanto nel Data Governance Act EU e nel Data Act EU. Occorre quindi supportare, attraverso investimenti con fondi nazionali, la formazione **di nuclei di aggregazione territoriale** su "*data governance* e intelligenza artificiale" affinché nessun ente pubblico rimanga indietro nel progresso tecnologico, partendo da subito nel sostenere tali processi in modo condiviso a livello territoriale, invece di rincorrere in seguito le innovazioni introdotte in modo scoordinato ed episodico. Le Regioni, utilizzando l'esperienza e le buone pratiche di enti sperimentatori e delle proprie centrali di committenza, possono redigere delle linee guida e delle clausole contrattuali standard per l'approvvigionamento di una AI etica e conforme alla normativa nazionale e comunitaria. **Regioni e Province autonome possono fare da "rete neurale" del Paese rispetto a questi temi, ed anche per questo bisogna accelerare rispetto ai principi dell'Accordo Butti/Fedriga firmato a Perugia nel luglio 2023, per arrivare a definire il "cloud federato" e il "sistema nazionale per la trasformazione digitale"**.

4. Valutare l'implementazione nella PDND (Piattaforma Digitale Nazionale dei Dati, sia per gli scopi di cui al CAD art.50-ter comma 2 che per gli scopi del comma 4) di funzionalità necessarie a definire le modalità e i limiti di utilizzo dei dati fruiti e/o erogati tramite interoperabilità tra PA e verso altri soggetti abilitati in ottica AI; si tratterebbe di taggare i dati, come già avviene nella compilazione delle informazioni relative alle finalità delle richieste di fruizione e di erogazione, aggiungendo un valore informativo che definisca i possibili utilizzi in ambito AI, conforme a quanto sarà disposto nel prossimo AI Act EU e per quanto attiene i *"data spaces*" previsti dal Data Act EU.

5. Evitare che si arrivi a un "***AI divide***" **in cui le PA non sono in grado di comprendere e sfruttare queste tecnologie**. Quindi, è necessario, come già sottolineato in altri posizionamenti, un **reclutamento d'urgenza di specialisti ICT nella PA**. In un numero importante di (piccoli) enti NON c'è personale ICT, e non si tratta semplicemente della

mancanza di persone con le competenze necessarie, ci riferiamo in particolare proprio dell'assenza di personale informatico per gestire adeguatamente i propri sistemi informativi e la sicurezza… chi dovrebbe quindi presidiare l'introduzione dell'automazione attraverso l'intelligenza artificiale? Non sono ormai sufficienti generiche iniziative per lo sviluppo delle competenze digitali, bisogna strutturare percorsi formativi specifici per gli specialisti ICT nelle PA, definire forme di reclutamento adatte, definire una precisa famiglia professionale degli specialisti ICT con una specificità a livello di CCNL, definire la carriera degli specialisti ICT all'interno delle pubbliche amministrazioni. Il gravissimo "gap" delle PA è ben rappresentato dalla Corte dei conti nella "Relazione sullo stato di attuazione del PNRR" (novembre 2023) ove si legge quanto segue: *"11. Il ruolo della Pubblica amministrazione per agevolare il processo di transizione digitale è cruciale; non solo perché fornisce servizi digitali a imprese e famiglie, migliorandone l'accessibilità, ma anche perché può contribuire a diffondere buone pratiche e a stimolare processi di acquisizione di competenze. (..) La PA italiana risulta in grave ritardo, nei confronti con gli altri Paesi europei, circa la dotazione di personale specializzato in ambito digitale nei propri organici:* ***per portare il peso nell'occupazione della PA delle figure qualificate come "scientists and engineers" agli standard medi europei occorrerebbe aumentarne il numero di ben 65mila occupati****. D'altra parte, nel 2022 gli occupati laureati in ambito STEM, ovvero con lauree nel gruppo scientifico e tecnico****, erano poco meno di 37mila persone****. (..)*" Peraltro, in tale contesto andrebbero valorizzate e coordinate le eccellenze dirette e quelle in controllo pubblico già esistenti, strutturando una rete unica e non dispersiva che permette ai centri di competenza presenti sul territorio di agire a supporto delle rispettive sfere territoriali di naturale influenza.

6. Occorre **potenziare il ruolo dell'Ufficio del Responsabile per la transizione digitale (RTD), che va espressamente individuato anche come presidio immediato del tema intelligenza artificiale negli enti** e il profilo professionale del RTD va qualificato con precisi criteri. Come evidenziato già nel 2017 dalla relazione della Commissione parlamentare di inchiesta sui livelli di digitalizzazione della PA: "(..) *L'analisi dei curricula dei responsabili della transizione digitale [RTD] rende difficile affermare che il comma 1-ter dell'articolo 17 del CAD sia rispettato, e cioè che <<il responsabile dell'ufficio è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali>> (..) Il tentativo di istituire la figura di Chief Digital Officer a costo zero è chiaramente fallito. È di tutta evidenza che le figure necessarie non sono presenti all'interno della PA, nonostante, come detto, la normativa prevedesse figure analoghe sin dal 1993 e quindi non vi è alcuna giustificazione per una mancata politica di assunzione in quasi 25 anni. "*

7. Oltre a promuovere la capacità della pubblica amministrazione di adottare soluzioni innovative di intelligenza artificiale, è necessario **favorire la capacità del sistema economico e dei suoi attori pubblici e privati di cogliere le opportunità offerte dall'AI** in termini di maggiori livelli di innovazione e di competitività, di benessere e per il miglioramento della qualità della vita, intervenendo su temi chiave quali l'accelerazione del trasferimento tecnologico, lo sviluppo delle competenze e il sostegno alle collaborazioni interdisciplinari, valorizzando il modello dell'*Open Innovation*.

8. L'AI è un potente strumento trasversale abilitante per molte attività per cui le Regioni possono diventare laboratori per attività di contaminazione tra diverse discipline in particolare (team multidisciplinari) e per coinvolgere tutto il partenariato istituzionale ed economico-sociale del territorio. Ad esempio, al fine di ottenere una nuova generazione di cittadini pronti all'utilizzo corretto ed efficace della AI occorre portare la sua conoscenza nella scuola primaria e secondaria, e anche per queste attività le Regioni possono garantire la necessaria omogeneità sui territori. Le Regioni possono svolgere un ruolo chiave nel

garantire la **disseminazione e la formazione** sia a livello pubblico che privato, e possono fare da promotori in sinergia con gli interventi di finanziamento della programmazione EU 21-27 di collaborazioni tra industria, istituzioni accademiche e *start-up*. Bisogna investire anche per sostenere gli obiettivi del "Decennio digitale 2030", tra i quali uno molto sfidante: nel 2030 il 75% delle imprese dell'UE dovrà utilizzare cloud, AI e big data, e inoltre il 90% delle PMI dovranno raggiungere almeno il "livello base di intensità digitale". Le politiche nazionali vanno coordinate in modo sinergico con quelle a livello regionale per raggiungere questo obiettivo estremamente importante per il settore produttivo. Le Regioni possono effettuare degli assessment delle PA locali per verificare che il 90% di queste ultime raggiungano livelli base del DII così come le PMI.

9. Tenere in considerazione il **ruolo che può svolgere il mondo delle Università e della Ricerca italiana**, un asset strategico per la promozione di un approccio etico, sicuro e consapevole alla AI in Italia, istituzioni che possono essere partner delle Regioni per sperimentare nuove applicazioni avanzate in ambito dei servizi pubblici, e coadiuvare le Regioni stesse nella introduzione di forme di AI che perseguono gli obiettivi europei di sovranità digitale anche nell'utilizzo e promozione di questo tecnologia, ed infine svolgono un'azione essenziale nella formazione dei nuovi profili specialistici ICT, di cui c'è forte carenza, insieme al mondo della formazione scolastica e post-diploma.

10. Addestrare e mantenere nel tempo **modelli di qualità nazionali sia general-purpose che specifici per settore (es. sanità, giustizia, etc.)** nel caso predisponendo - tramite una infrastruttura nazionale - un sistema di comune riuso e/o fornitura di modelli in modalità as-a-service, promuovendo una cultura della "AI aperta", anche sperimentando la possibile fusione con strategie *open source*, come via per la trasparenza dell'attività amministrativa. Questo consente di indirizzare temi critici quali l'affidabilità dei modelli e, quando si parla di AI generativa, le cosiddette allucinazioni rappresentano un tema di attenzione per l'implementazione di alcune tecniche all'interno della PA. La potenziale discriminazione di alcuni individui o fasce di popolazione può venire ereditata dai dati di addestramento (c.d. *"bias"*) con implicazioni etiche importanti. In secondo luogo, l'uso di fonti dati non certificate/garantite: l'assenza di consapevolezza e competenza circa la corretta selezione delle fonti, la gestione del relativo *licensing* e i criteri di set di dati di qualità e affidabili costituiscono in radice un "vulnus" alla possibilità di realizzare sistemi AI affidabili. L'imminente AI Act europeo, la Direttiva sulla responsabilità extracontrattuale da uso di sistemi di AI, e soprattutto le sfide che la già normativa vigente impone anche rispetto a detti sistemi (Direttiva NIS2, responsabilità da prodotto, *data mining* e ricerca, tutela dei dati e assistenza sanitaria, etc) richiedono di essere in grado di elaborare soluzioni già oggi adottabili, provando anche nuove soluzioni da condividere e verificare, avendo già un occhio a quello che verrà.

11. Occorre definire regole e **criteri standard di accettabilità delle decisioni algoritmiche**. L'utilizzo dell'AI di nuova generazione (es. machine learning, generative AI, etc) come ruolo attivo in processi della PA può essere indirizzato solo se sono stati normati a livello strutturale e standardizzati regole e criteri di accettabilità basati su analisi rischi/benefici applicati ai singoli settori, ambiti tematici e differenziati a livelli di processo. Il cambiamento in questo contesto è radicale. Si passa dall'implementazione della burocrazia (nell' accezione positiva, le cui finalità sono rivolte all'efficienza, imparzialità, protezione dei diritti dei cittadini, etc) con modelli procedurali deterministici (regole codificate) a modelli statistici e probabilistici.

12. Definire indirizzi specifici per la connessa **innovazione organizzativa del lavoro e personale PA**: in molti contesti organizzativi non sarà sufficiente introdurre tecnologie AI, ma sarà necessario sviluppare una consapevolezza e una mentalità adeguata in modo diffuso, per sfruttare appieno e in modo sicuro le opportunità offerte dall'intelligenza

artificiale. Si richiede infatti un *"mindset"* aperto a questi nuovi approcci mentre mancano negli organici le competenze necessarie per comunicare e interagire efficacemente e in modo critico con le tecnologie dell'AI, mettendo in evidenza anche gli aspetti etici di tali interazioni. Sono necessarie dimensioni di conoscenza, competenze tecniche e operative, nonché sensibilità giuridiche, ma anche valutazioni critiche ed etiche. Da un lato, ciò implica una comprensione delle funzioni fondamentali dell'AI e la capacità di applicarle in contesti diversi, dall'altro, richiede un'attenzione costante alle implicazioni della AI. Se da un lato l'AI può portare efficienza e aumentare la produttività dei dipendenti pubblici, andando in parte a coprire eventuali carenze di personale amministrativo, non si possono non considerare gli impatti sull'organizzazione degli stessi Enti. Il lavoro si trasforma certamente per la presenza di assistenti virtuali, di sistemi di automazione intelligente o di decisioni supportate dai dati. Le competenze devono evolvere, in quanto determinati profili nella PA non saranno più necessari nel nuovo scenario, portando la necessità di avere un piano di gestione del cambiamento e di *re-skilling / up-skilling*. Può essere una opportunità per la PA, a fronte di riduzione degli organici per raggiungimento dei limiti di età, di indirizzare modelli di lavoro innovativi che contemplino l'utilizzo delle tecniche di AI e nello stesso tempo contribuiscano alla revisione di profili professionali e forme organizzative delle PA.

In conclusione, le Regioni e le Province autonome esprimono la forte volontà di svolgere il ruolo di partner attivi nel plasmare e attuare la nuova strategia nazionale sull'intelligenza artificiale, collaborando attivamente e proattivamente, sulla base di specifiche azioni condivise, con il Governo per promuovere lo sviluppo e l'utilizzo etico e consapevole dell'AI, massimizzando l'impatto sull'intero Paese in termini di innovazione, occupazione e benessere.

***

Si allegano anche le proposte normative già elaborate dalla Commissione ITD per il redigendo "Decreto PNRR" che trattano, nella maggior parte dei casi, di modifiche urgenti riferite al tema intelligenza artificiale nella PA.

Roma, 20 dicembre 2023

07/12/2023

Oggetto: Proposte della Commissione ITD per redigendo decreto PNRR

Art. _ Classificazione della spesa cloud e ridefinizione di SPC nell'ottica cloud federata

Art. _ Coordinamento di processi di digitalizzazione condivisi a livello territoriale e semplificazione dei procedimenti relativi a regole tecniche e linee guida

Art. _ Coordinamento all'interno delle PA della migrazione al cloud e dell'intelligenza artificiale attraverso il potenziamento dell'Ufficio RTD

Art. _ Accelerazione e semplificazione dei controlli "once only" attraverso interoperabilità via PDND

Art. _ Estensione dei criteri delle soluzioni e del riuso per il cloud, per l'interoperabilità via PDND e per l'introduzione dell'intelligenza artificiale

Art. _ Classificazione della spesa cloud e ridefinizione di SPC nell'ottica cloud federata

1. Dopo il comma 5, dell'art. 33-septies, del decreto–legge 18 ottobre 2012, n. 179 convertito con modificazioni dalla legge 17 dicembre 2012, n. 221 è aggiunto il seguente comma: "6. Al fine di assicurare la trasformazione digitale dei servizi della pubblica amministrazione e l'omogeneità dei conti pubblici, a partire dall'anno finanziario 2024 e fino al 31 dicembre 2035, le spese per l'acquisizione di servizi cloud qualificati dall'Agenzia per la cybersicurezza nazionale ai sensi del regolamento di cui al comma 4, siano essi servizi cloud di tipo infrastrutturale (IaaS), servizi cloud per piattaforme computazionali (PaaS) o servizi cloud applicativi (SaaS), sono annoverate tra le spese di investimento di cui al comma 18 dell'articolo 3 della Legge 24 dicembre 2003, n. 350 e, conseguentemente, le Regioni e Province autonome e le Amministrazioni locali contabilizzano tali spese al titolo secondo della spesa dei propri bilanci, macroaggregato 02 "Investimenti fissi lordi e acquisto di terreni", in apposita voce del piano dei conti finanziario relativo alle immobilizzazioni immateriali, di cui all'allegato 6/1 del decreto legislativo 28 giugno 2011, n.118."
2. Al comma 2-quinquies, dell'articolo 27 , del decreto–legge 6 novembre 2021, n. 152 convertito con modificazioni dalla legge 29 dicembre 2021, n. 233 dopo le parole "servizi cloud infrastrutturali" sono inserite le seguenti", di piattaforma computazionale o applicativi"; le parole "fino al termine di attuazione del predetto Piano nazionale di ripresa e resilienza" sono sostituite dalle seguenti "fino al 2035"; dopo le parole "tra gli stanziamenti" viene inserito quanto segue: "e i finanziamenti".

3. La rubrica del capo VIII e la rubrica dell'articolo 73 del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" sono sostituite dalla seguente: "Sistema Pubblico Cloud (SPC)"
4. All'articolo 73, comma 3, del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" vengono apportate le seguenti modificazioni:
- alla lettera a) è aggiunto in fondo "attraverso l'impiego di standard internazionali di architettura enterprise e nel rispetto del quadro europeo di interoperabilità";
- alla lettera b) sono sostituite le parole "servizi in rete, di interoperabilità e di supporto alla cooperazione applicativa" con le parole "servizi di connettività, di gestione dei dati, di integrazione tra sistemi interni, nonché lo sviluppo di spazi di interoperabilità e cooperazione applicativa basati su interfacce applicative (API)";
- alla lettera b-bis) è aggiunto in fondo "in particolare per l'abilitazione al cloud quale accesso conveniente e su richiesta ad un insieme condiviso di risorse di calcolo configurabili, che possano essere rapidamente procurate ed utilizzate via rete, mediante un minimo sforzo di gestione o una minima interazione con il gestore e fornitore del servizio";
5. All'articolo 73 del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" al comma 3-ter, alla lettera a), sono sostituite le parole "architetture e interfacce tecnologiche" con le parole "piattaforme abilitanti indicate al comma 4 dell'art.13-bis ed interfacce applicative (API) esposte come da art.50-ter secondo schemi definiti da hub nazionali e/o regionali" ed alla lettera c) sono aggiunte in fondo le parole "cloud qualificate da ACN (compreso un marketplace con funzioni di acquisto diretto)".

Relazione

L'abilitazione al cloud della PA è un tassello fondamentale nel processo di modernizzazione del Paese e architrave della strategia di transizione digitale enunciata nel PNRR nella Missione 1. MIgrando i sistemi informativi della PA sul Cloud si trasformano investimenti in conto capitale (storicamente effettuati per i CED) in spese in conto corrente annuali per pagare i canoni del servizio cloud "as a service" nelle varie tipologie IaaS, PaaS o SaaS previste dalla strategia nazionale "Cloud Italia" e soggetti a percorso di qualificazione da parte di ACN. Si creano due potenziali problemi per la finanza pubblica e la contabilità degli enti:

- *scatto dei vincoli di spending review: aumentando la spesa corrente potrebbero scattare e/o farsi ancora più stringenti i vincoli di spending review introdotti nel passato e anche di recente, in particolare per gli enti locali, mentre le spese cloud non possono essere*

compresse proprio quando si chiede di effettuare una ambiziosa operazione di migrazione/abilitazione al cloud da parte delle PA;

- *limitata capacità di spesa corrente in molti enti locali, e quindi senza poter incrementare le spese correnti al di là dei vincoli esistenti, molti enti locali e PA non possono passare a cloud per assenza di risorse impegnabili in tale direzione anche dopo il periodo coperto dagli investimenti previsti nel PNRR.*

Tali interventi normativi, devono essere resi stabili anche oltre il 31 dicembre 2026, termine di durata del PNRR in quanto le spese per il passaggio al cloud non si esauriranno il 31 dicembre 2026 e si propone di coprire almeno il periodo fino al 2035 previsto dagli investimenti del PNRR legati al "Polo Strategico Nazionale" (PSN).

La modifica proposta da piena attuazione anche alle indicazioni del PNRR Missione 1) Componente 1) Digitalizzazione, innovazione e sicurezza nella PA per quanto riguarda la Riforma 1.3 "Cloud first e interoperabilità", che recita "Saranno anche riviste le regole di contabilità che attualmente disincentivano la migrazione (al momento, infatti, la migrazione al cloud comporta di "tradurre" CAPEX in OPEX)." e nell'allegato tecnico al PNRR trasmesso alla UE, testualmente, alla medesima riforma è previsto: "…. as part of the incentives for cloud migration, we plan to revise the current public accounting rules for expenses related to cloud services. In fact, the migration to the cloud currently involves a transfer of budgets from capital expenditures to operational expenditures. These mechanisms/rules will be revised in order to not disincentivize cloud migration for PAs."

Vengono anche riproposti gli emendamenti già approvati dalla Commissione Agenda digitale in data 29/06/2019 , per allineare al nuovo scenario cloud del PNRR il concetto di Sistema Pubblico di Connettività (SPC), ancora presente nel CAD all'art.73, e farlo evolvere considerando che, oggi, è proprio il cloud computing con la sua sua natura decentrata, policentrica e federata, a rendere possibile il disegno originario del SPC, anche per salvaguardare l'autonomia locale, la neutralità tecnologica e la concorrenza sulle soluzioni ICT destinate alle PA valorizzando al tempo stesso gli investimenti in infrastrutture fatti da Regioni, Province autonome e loro in house (ove presenti).

Art. _ Coordinamento di processi di digitalizzazione condivisi a livello territoriale e semplificazione dei procedimenti relativi a regole tecniche e linee guida

1. All'articolo 14 del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" sono aggiunti i seguenti commi:

"4. E' istituita la Commissione permanente del Sistema Nazionale per la Trasformazione Digitale, coordinata dal Dipartimento per la Trasformazione Digitale, che prevede la partecipazione di rappresentanti nominati da Agenzia per l'Italia Digitale, Agenzia per la cybersicurezza, Dipartimento della Funzione Pubblica, Conferenza delle Regioni e Province autonome e dalle Autonomie locali, quale forma di raccordo stabile delle rispettive politiche e per l'istruttoria di intese/accordi di cui al comma 2 nonché rispetto alla individuazione e dispiegamento di linee guida, regole tecniche e specifiche tecniche.
5. I processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, ovvero lo Stato deve intraprendere iniziative di digitalizzazione solo se sono più efficaci di quelle a livello regionale e locale, e in base alle esigenze espresse dalle amministrazioni stesse, limitandosi negli altri casi a quanto necessario per il coordinamento informatico dei dati, e al tempo stesso le singole amministrazioni devono garantire l'appropriatezza delle iniziative di digitalizzazione portate avanti autonomamente, cioè in forma non condivisa con altri enti a livello territoriale rispetto alle esigenze preminenti dell'azione amministrativa e degli utenti dei servizi pubblici, assicurando in ogni caso la piena sicurezza informatica e l'interoperabilità dei loro sistemi informativi e basi dati.".
2. All'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 il comma 1 è sostituito dal seguente: "1. Su proposta del Governo di concerto con la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, acquisito il parere della amministrazioni competenti e del Garante per la protezione dei dati personali nelle materie di competenza, nonché previa consultazione pubblica, viene emanato un regolamento attuativo unico per l'amministrazione digitale, contenente l'insieme delle linee guida vincolanti, regole tecniche ed indirizzi per l'attuazione del presente Codice. Il regolamento è aggiornato o modificato, anche parzialmente, con la procedura di cui al primo periodo. Il regolamento può rinviare a specifiche tecniche emanate da AgID, di concerto con la Commissione permanente del Sistema Nazionale per la Trasformazione Digitale di cui all'art.14, per gli aspetti di implementazione tecnologica soggetti a rapida evoluzione o che richiedono continuo adattamento nel tempo."

Relazione

E' necessaria per l'attuazione della missione 1 del PNRR, ma anche nella successiva fase a regime, una procedura agile di definizione e manutenzione nel tempo del corpus complessivo delle regole tecniche per la transizione digitale. Vengono riproposti gli emendamenti già

approvati dalla Commissione Agenda digitale in data 29/06/2019 tesi a ripristinare un meccanismo di coordinamento, in similitudine alla fu "Commissione di coordinamento SPC" prevista all'art. 79 del CAD ed ora abrogato, che aveva il compito di facilitare l'aggiornamento e l'emanazione delle regole tecniche in modo condiviso e unitario. Le stesse regole tecniche vanno riunite in un testo unico, coordinato e facilmente reperibile per gli enti, distinguendo tra le regole destinate agli uffici sistemi informativi e quelle destinate agli uffici che si occupano di erogazione di servizi, di procedimenti e altre attività amministrative. L'istituzione di una "Commissione permanente del Sistema Nazionale per la Trasformazione Digitale" permette anche di strutturare processi condivisi di digitalizzazione nei territori e definire agilmente specifiche tecniche di dettaglio per quegli aspetti di implementazione tecnologica soggetti a rapida evoluzione o che richiedono continuo adattamento nel tempo, che passano oggi da procedimenti normativi troppo rigidi e complessi per far fronte alla rivoluzione dell'intelligenza artificiale. Infine, con un nuovo comma aggiunto all'art.14 viene specificato che i processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, declinando nel caso specifico i principi generali già fissati dalla Costituzione

Art. _ Coordinamento all'interno delle PA della migrazione al cloud e dell'intelligenza artificiale attraverso il potenziamento dell'Ufficio RTD

1. Dopo il comma 5, dell'art. 17, del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale", al comma 1, lettera g) è aggiunto in fondo quanto segue: "con particolare riferimento ai processi di migrazione/abilitazione al cloud computing, governo dei dati dell'ente e degli algoritmi di intelligenza artificiale legati all'automazione dei processi, delle procedure e dell'azione amministrativa."; al comma 1-ter è aggiunto quanto segue "A tal fine, in base degli indirizzi generali del vertice politico il Responsabile per la transizione digitale fissa gli specifici obiettivi di semplificazione e digitalizzazione previsti nel PIAO dal DM 24 giugno 2022. AgID stabilisce con proprie linee guida i requisiti che deve possedere il responsabile dell'ufficio di cui al comma 1 e le caratteristiche minime per la strutturazione dell'ufficio stesso anche in relazione alla complessità dell'ente."; al comma 1-septies è aggiunto quanto segue "I soggetti di cui al comma 1-sexies possono esercitare le funzioni anche attraverso forme aggregative istituite a tale scopo da Regioni e Province autonome, anche tramite supporto delle loro eventuali società in house."

2. Il secondo periodo del comma 3, dell'art. 13-bis, del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale", è sostituito dal seguente: "Il codice di condotta tecnologica è attuato anche attraverso linee guida definite da AgID che fissano: le modalità di qualificazione degli esperti e le principali attività che possono svolgere in collaborazione con il Responsabile per la transizione digitale dell'amministrazione pubblica interessata; le forme di aggregazione per lo sviluppo di comunità di pratica a scala regionale per favorire la progettazione ICT di qualità e processi condivisi di digitalizzazione a scala territoriale; la definizione del numero di livelli di progettazione e i formati della documentazione progettuale, quale caso specifico, rispetto a quanto previsto dal comma 12 dell'art.41 del decreto legislativo 31 marzo 2023, n. 36, da utilizzare nel caso di progetti ICT di importo superiore a quello fissato dall'art. 50, comma 1, lettera e) del decreto legislativo 31 marzo 2023, n. 36; le metodologie per la valutazione dei costi ICT per l'intero ciclo di vita dei servizi digitali e per evitare il lock-in."

Relazione

L'abilitazione al cloud della PA, nonché la gestione dei dati pubblici e l'introduzione regolata dell'intelligenza artificiale, richiede nelle PA la strutturazione urgente di precise responsabilità di presidio e coordinamento. A tal fine la modifica del comma 1, lettera g), assegna indirizzo, coordinamento e monitoraggio sul tema ai compiti dell'Ufficio del Responsabile per la trasformazione digitale previsto dall'art.17 del CAD. per l'effettiva strutturazione di tale Ufficio nonché per potenziarne le funzioni vengono inoltre proposte modifiche ai commi 1-ter (prevedendo un ruolo dell'RTD nella definizione degli obiettivi nel PIAO) e 1-septies (nuove modalità di aggregazione a livello regionale).

Viene anche introdotta una modifica al comma 3, dell'art. 13-bis, per prevedere specifici livelli di progettazione nel caso di progetti ICT complessi, che devono garantire specifici livelli di progettazione e di qualità da definire con apposite linee guida AgID, per garantire la piena efficacia degli investimenti del PNRR e nella fase a regime che seguirà, compresa la valutazione dei costi per l'intero ciclo di vita dei servizi digitali e per evitare il "lock-in".

La modifica è pienamente sinergica anche agli interventi della missione 1 del PNRR e con la Riforma 1.3 "Cloud first e interoperabilità" per fissare un preciso centro di responsabilità e coordinamento rispetto ai processi di migrazione/abilitazione al cloud, ai dati e all'intelligenza artificiale in tutte le PA, comprese quelle più di dimensione più piccola in cui mancano specialisti ICT per affrontare tale sfida.

Art. _ Accelerazione e semplificazione dei controlli “once only” attraverso interoperabilità via PDND

1. Dopo il comma 6, dell’art. 50-ter, del decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale”, è aggiunto il seguente:
“6-bis. L'accesso ai dati attraverso la Piattaforma Digitale Nazionale Dati avviene in base ad una semplice dichiarazione, resa da parte dell’amministrazione procedente, che attesti di voler fruire di una interfaccia API per la finalità di effettuare i controlli di cui dell’articolo 71 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e in tal caso l’accesso non potrà essere assoggettato da parte dell’amministrazione certificante, che pubblica e rende disponibile l’interfaccia API stessa, ad alcun ulteriore aggravamento istruttorio che vada oltre la predetta dichiarazione, che siano richiesti sia attraverso la PDND stessa che attraverso altri canali di comunicazione.”
2. All'art. 64 del decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale”, è aggiunto il seguente comma:
“2-terdecies. A tutti i dipendenti delle pubbliche amministrazioni di cui all’articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, è fornita gratuitamente un'identità digitale finalizzata esclusivamente all'esercizio delle proprie funzioni con le modalità definite da AgID con apposite linee guida."

Relazione

L’interoperabilità tra le banche dati delle PA e la piena attuazione del principio “once only” rischia di trovare un ostacolo nei procedimenti di abilitazione all’uso delle interfacce API pubblicate nella infrastruttura nazionale PDND che si vanno ad aggiungere in merito alle finalità dell’amministrazione che chiede di fruire. La modifica propone che l’amministrazione procedente non dovrà indicare nel dettaglio le finalità, ma unicamente produrre una semplice dichiarazione che attesti di voler fruire di una interfaccia API per effettuare i controlli di cui dell’articolo 71 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 senza ulteriori aggravamenti. Si propone inoltre di fornire un’apposita identità digitale a tutti i dipendenti pubblici, per facilitare la loro identificazione nei processi di controllo dei dati e nella interoperabilità tra PA. La modifica è tesa ad accelerare e moltiplicare gli effetti degli ingenti investimenti previsti nella missione 1 del PNRR per l’interoperabilità e con la Riforma 1.3 “Cloud first e interoperabilità”.

Art. _ Estensione dei criteri delle soluzioni e del riuso per il cloud, per l'interoperabilità via PDND e per l'introduzione dell'intelligenza artificiale

1. Al comma 1, dell'art. 68, del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale", alla lettera d) le parole "in modalità cloud computing" sono sostituite dalle seguenti: "attraverso interfacce API;".
2. Al comma 1-bis, dell'art. 68, del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale", sono aggiunte le seguenti lettere:
"d) fruizione di servizi cloud qualificati come previsto dall'articolo 33-septies del decreto–legge 18 ottobre 2012, n. 179 convertito con modificazioni dalla legge 17 dicembre 2012, n. 221;
e) aspetti legati all'interazione della soluzione software con organizzazione, processi, regole, dati e tecnologie dell'ente, nonché dei processi condivisi di digitalizzazione coordinati a scala territoriale coma da articolo 14.;
f) automazione di processi e procedure, anche ricorrendo ad algoritmi di intelligenza artificiale, in cui sia garantito che le decisioni assunte rispettino i principi di conoscibilità e comprensibilità della logica utilizzata, non esclusività della decisione algoritmica prevedendo in ogni caso un contributo umano, non discriminazione algoritmica."

Relazione

L'introduzione del cloud e la realizzazione effettiva dell'interoperabilità richiede di rinnovare profondamente il vecchio concetto di "riuso" di cui all'art.68 del CAD, poiché occorre concentrarsi, più che su aspetti di mero riutilizzo di codice sorgente , su tutti gli aspetti che mettono in relazione il software con processi, procedimenti, organizzazione, regole e regolamenti, Inoltre, con il crescere di servizi digitali forniti ad uno stesso ente da una molteplicità di fornitori diversi, via cloud, cresce notevolmente la complessità della gestione del parco applicativo, rendendo cruciale la concreta integrazione tra i software dell'ente, l'effettiva possibilità di interoperabilità verso altri enti, la corretta gestione dei dati, ecc. Il nuovo scenario evolutivo, supera il concetto tradizionale di riuso (che oggi può essere anche chiamare una interfaccia API di un altro ente) e richiede processi condivisi a livello territoriale.
Nell'analisi comparativa delle soluzioni viene introdotta anche la necessità di considerare, in caso di soluzioni che impiegano algoritmi di intelligenza artificiale, i principi di conoscibilità e comprensibilità della logica utilizzata, non esclusività della decisione algoritmica prevedendo in ogni caso un contributo umano, non discriminazione algoritmica.
La modifica è tesa ad accelerare e moltiplicare gli effetti degli ingenti investimenti previsti nella missione 1 del PNRR per l'interoperabilità e con la Riforma 1.3 "Cloud first e interoperabilità".

COMMISSIONE
EUROPEA

Bruxelles, 19.2.2020
COM(2020) 65 final

LIBRO BIANCO

sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia

IT IT

Libro bianco sull'intelligenza artificiale
Un approccio europeo all'eccellenza e alla fiducia

L'intelligenza artificiale si sta sviluppando rapidamente. Cambierà le nostre vite migliorando l'assistenza sanitaria (ad esempio rendendo le diagnosi più precise e consentendo una migliore prevenzione delle malattie), aumentando l'efficienza dell'agricoltura, contribuendo alla mitigazione dei cambiamenti climatici e all'adattamento ai medesimi, migliorando l'efficienza dei sistemi di produzione mediante la manutenzione predittiva, aumentando la sicurezza dei cittadini europei e in molti altri modi che possiamo solo iniziare a immaginare. Al tempo stesso, l'intelligenza artificiale (IA) comporta una serie di rischi potenziali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite private o utilizzi per scopi criminali.

In un contesto di forte concorrenza globale, è necessario un solido approccio europeo, basato sulla strategia europea per l'IA presentata nell'aprile 2018[1]. Per sfruttare le opportunità e affrontare le sfide derivanti dall'IA, l'UE deve parlare con un'unica voce e definire il suo modo di promuovere lo sviluppo e la diffusione dell'IA basandosi sui valori europei.

La Commissione si impegna a favorire i progressi scientifici, a preservare la leadership tecnologica dell'UE e a garantire che le nuove tecnologie siano al servizio di tutti gli europei e ne migliorino la vita rispettandone i diritti.

La presidente della Commissione Ursula von der Leyen ha annunciato nei suoi orientamenti politici[2] un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale e una riflessione volta a migliorare l'uso dei big data per favorire l'innovazione.

La Commissione sostiene pertanto un approccio normativo e orientato agli investimenti con il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi associati a determinati utilizzi di questa nuova tecnologia. Lo scopo del presente libro bianco è definire le opzioni strategiche su come raggiungere tali obiettivi. Non vengono affrontate in questa sede le questioni dello sviluppo e dell'utilizzo dell'IA per scopi militari. La Commissione invita gli Stati membri, le altre istituzioni europee e tutti i portatori di interessi, compresi l'industria, le parti sociali, le organizzazioni della società civile, i ricercatori, il pubblico in generale e tutte le parti interessate, ad esprimersi in merito alle opzioni presentate di seguito e a contribuire al futuro processo decisionale della Commissione in questo settore.

1. INTRODUZIONE

Poiché la tecnologia digitale diventa una parte sempre più centrale di tutti gli aspetti della vita delle persone, queste ultime dovrebbero potersi fidare di tale tecnologia. L'affidabilità è inoltre un prerequisito per la sua adozione. Si tratta di un'opportunità per l'Europa, dato il suo forte attaccamento ai valori e allo Stato di diritto, nonché la sua comprovata capacità di costruire prodotti e prestare servizi affidabili, sicuri e sofisticati dal settore aeronautico a quello energetico, automobilistico e delle apparecchiature mediche.

La crescita economica sostenibile attuale e futura e il benessere sociale dell'Europa si basano sempre di più sul valore creato dai dati. L'IA è una delle più importanti applicazioni dell'economia dei dati.

[1] L'intelligenza artificiale per l'Europa, COM(2018) 237 final.
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_it.pdf.

Oggi la maggior parte dei dati riguarda i consumatori ed è conservata e elaborata in infrastrutture centrali basate su cloud. Un'ampia fetta dei dati di domani, ben più abbondanti di quelli di oggi, proverrà invece dall'industria, dalle imprese e dal settore pubblico e sarà conservata in vari sistemi, in particolare dispositivi di calcolo funzionanti ai margini della rete. Ciò apre nuove opportunità per l'Europa, che ha una posizione forte nel settore del digitale e delle applicazioni tra imprese (*business-to-business*), ma ha una posizione relativamente debole per quanto riguarda le piattaforme destinate ai consumatori.

Semplificando possiamo dire che l'IA è un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo. I progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono pertanto fattori determinanti per l'attuale crescita dell'IA. L'Europa può combinare i suoi punti di forza industriali e tecnologici con un'infrastruttura digitale di elevata qualità e un quadro normativo basato sui suoi valori fondamentali per **diventare un leader mondiale nell'innovazione nell'economia dei dati e nelle sue applicazioni**, come indicato nella strategia europea per i dati[3]. Su questa base l'Europa può sviluppare un ecosistema di IA che consenta alla sua società e alla sua economia nel loro complesso di godere dei benefici apportati dalla tecnologia:

- i **cittadini** potranno usufruire di nuovi vantaggi, ad esempio una migliore assistenza sanitaria, un minor numero di guasti degli elettrodomestici, sistemi di trasporto più sicuri e più puliti e servizi pubblici migliori;
- nello sviluppo delle **imprese** sarà possibile, ad esempio, avvalersi di nuove generazioni di prodotti e servizi nei settori in cui l'Europa è particolarmente forte (macchinari, trasporti, cibersicurezza, agricoltura, economia verde e circolare, assistenza sanitaria e settori ad alto valore aggiunto come la moda e il turismo); e
- i servizi di **interesse pubblico** potranno beneficiare, ad esempio, della riduzione dei costi di fornitura di servizi (trasporti, istruzione, energia e gestione dei rifiuti), migliorando la sostenibilità dei prodotti[4] e dotando le forze dell'ordine di strumenti appropriati per garantire la sicurezza dei cittadini[5], con adeguate garanzie quanto al rispetto dei loro diritti e delle loro libertà.

Dato l'impatto significativo che l'intelligenza artificiale può avere sulla nostra società e la necessità di creare maggiore fiducia, è essenziale che l'IA europea sia fondata sui nostri valori e diritti fondamentali quali la dignità umana e la tutela della privacy.

L'impatto dei sistemi di IA dovrebbe inoltre essere considerato non solo da una prospettiva individuale, ma anche dal punto di vista della società nel suo complesso. L'uso dei sistemi di IA può svolgere un ruolo significativo nel conseguimento degli obiettivi di sviluppo sostenibile e nel sostegno al processo democratico e ai diritti sociali. Con le sue recenti proposte nell'ambito del Green Deal europeo[6], l'Europa è in prima linea nella risposta alle sfide legate al clima e all'ambiente. Le tecnologie digitali quali l'IA sono fattori abilitanti fondamentali per conseguire gli obiettivi del Green Deal. Data la

[3] COM(2020) 66 final.

[4] L'IA e la digitalizzazione in generale sono fattori abilitanti fondamentali per gli ambiziosi obiettivi del Green Deal europeo. Tuttavia l'attuale impronta ambientale del settore delle tecnologie dell'informazione e della comunicazione è stimata a oltre il 2 % di tutte le emissioni globali. La strategia digitale europea che accompagna il presente libro bianco propone misure per la trasformazione verde del settore digitale.

[5] Gli strumenti di IA possono costituire un'opportunità per migliorare la protezione dei cittadini dell'UE dalla criminalità e dagli atti di terrorismo. Tali strumenti potrebbero, ad esempio, contribuire a individuare la propaganda terroristica online, scoprire transazioni sospette nelle vendite di prodotti pericolosi, individuare oggetti pericolosi o sostanze o prodotti illeciti nascosti, offrire assistenza ai cittadini in situazioni di emergenza e contribuire a guidare il personale di primo intervento.

[6] COM(2019) 640 final.

crescente importanza dell'IA, l'impatto ambientale dei sistemi di IA deve essere debitamente preso in considerazione durante il loro intero ciclo di vita e lungo l'intera catena di approvvigionamento, ad esempio per quanto riguarda l'uso di risorse per l'addestramento degli algoritmi e la conservazione dei dati.

È necessario un approccio comune europeo all'IA per raggiungere dimensioni sufficienti ed evitare la frammentazione del mercato unico. L'introduzione di iniziative nazionali rischia di compromettere la certezza del diritto, di indebolire la fiducia dei cittadini e di ostacolare l'emergere di un'industria europea dinamica.

Il presente libro bianco presenta opzioni strategiche che consentano uno sviluppo sicuro e affidabile dell'IA in Europa, nel pieno rispetto dei valori e dei diritti dei cittadini dell'UE. I principali elementi costitutivi del presente libro bianco sono i seguenti:

- il quadro strategico che stabilisce misure per allineare gli sforzi a livello europeo, nazionale e regionale. Tramite un partenariato tra il settore pubblico e privato, l'obiettivo di tale quadro è mobilitare risorse per conseguire un **"ecosistema di eccellenza"** lungo l'intera catena del valore, a cominciare dalla ricerca e dall'innovazione, e creare i giusti incentivi per accelerare l'adozione di soluzioni basate sull'IA, anche da parte delle piccole e medie imprese (PMI);
- gli elementi chiave di un futuro quadro normativo per l'IA in Europa, che creerà un **"ecosistema di fiducia"** unico. A tal fine, deve garantire il rispetto delle norme dell'UE, comprese le norme a tutela dei diritti fondamentali e dei diritti dei consumatori, in particolare per i sistemi di IA ad alto rischio gestiti nell'UE[7]. La costruzione di un ecosistema di fiducia è un obiettivo strategico in sé e dovrebbe dare ai cittadini la fiducia di adottare applicazioni di IA e alle imprese e alle organizzazioni pubbliche la certezza del diritto necessaria per innovare utilizzando l'IA. La Commissione sostiene con forza un approccio antropocentrico basato sulla comunicazione "Creare fiducia nell'intelligenza artificiale antropocentrica"[8] e terrà conto anche dei contributi ottenuti durante la fase pilota degli orientamenti etici elaborati dal gruppo di esperti ad alto livello sull'IA.

La strategia europea per i dati che accompagna il presente libro bianco ha l'obiettivo di far sì che l'Europa diventi l'economia agile basata sui dati più attraente, sicura e dinamica del mondo, mettendo a sua disposizione i dati necessari a migliorare le decisioni e la vita di tutti i suoi cittadini. La strategia definisce una serie di misure strategiche necessarie per raggiungere questo obiettivo, tra cui la mobilitazione degli investimenti pubblici e privati. Le implicazioni dell'intelligenza artificiale, dell'Internet delle cose e di altre tecnologie digitali per la legislazione in materia di sicurezza e responsabilità sono infine analizzate nella relazione della Commissione che accompagna il presente libro bianco.

2. TRARRE VANTAGGIO DAI PUNTI DI FORZA DEI MERCATI INDUSTRIALI E PROFESSIONALI

L'Europa si trova in una posizione ideale per beneficiare del potenziale dell'IA, non solo in quanto utente, ma anche come creatore e produttore di questa tecnologia. Dispone di centri di ricerca di eccellenza, start-up innovative, di una posizione di leadership a livello mondiale nella robotica e di settori competitivi dell'industria manifatturiera e dei servizi, dal settore automobilistico all'assistenza sanitaria, all'energia, ai servizi finanziari e all'agricoltura. L'Europa ha sviluppato una potente

[7] Potrebbero essere necessarie ulteriori disposizioni per prevenire e contrastare l'abuso dell'IA per scopi criminali, ma ciò non rientra nel campo di applicazione del presente libro bianco.
[8] COM(2019) 168 final.

infrastruttura di calcolo (ad esempio i computer ad alte prestazioni), essenziale per il funzionamento dell'IA. L'Europa dispone inoltre di grandi volumi di dati pubblici e industriali, il cui potenziale è attualmente sottoutilizzato, e di punti di forza industriali riconosciuti nell'ambito dei sistemi digitali sicuri a basso consumo energetico che sono essenziali per l'ulteriore sviluppo dell'IA.

Lo sfruttamento della capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione nonché nelle competenze digitali, come l'alfabetizzazione ai dati (*data literacy*), accrescerà la sovranità tecnologica dell'Europa nell'ambito delle tecnologie e infrastrutture abilitanti fondamentali per l'economia dei dati. Le infrastrutture dovrebbero sostenere la creazione di pool europei di dati che consentano lo sviluppo di un'IA affidabile basata su valori e regole europei.

L'Europa dovrebbe sfruttare i propri punti di forza per far crescere la propria posizione negli ecosistemi e lungo la catena del valore, da determinati settori della produzione di hardware al software e ai servizi. Ciò sta già avvenendo, in una certa misura. L'Europa produce più di un quarto di tutti i robot di servizio industriali e professionali (ad esempio per l'agricoltura di precisione, la sicurezza, la salute e la logistica) e svolge un ruolo importante nello sviluppo e nell'utilizzo di applicazioni software per le imprese e le organizzazioni (applicazioni *business-to-business* quali i software per l'ingegneria, il design, e la pianificazione delle risorse aziendali), nonché di applicazioni a sostegno dell'e-government e dell'"impresa intelligente".

L'Europa svolge un ruolo guida per quanto riguarda la diffusione dell'IA nell'industria manifatturiera: oltre la metà dei principali fabbricanti implementano almeno un'istanza di IA nelle operazioni di fabbricazione[9].

Uno dei motivi alla base della posizione forte dell'Europa nella ricerca è il programma di finanziamento dell'UE, che si è dimostrato fondamentale per mettere in comune le azioni, evitare duplicazioni e mobilitare gli investimenti pubblici e privati negli Stati membri. Nel corso degli ultimi tre anni i finanziamenti dell'UE per la ricerca e l'innovazione nell'IA sono saliti a 1,5 miliardi di EUR, ossia un aumento del 70 % rispetto al periodo precedente.

Tuttavia, gli investimenti nella ricerca e nell'innovazione in Europa sono ancora nettamente inferiori agli investimenti pubblici e privati in altre regioni del mondo. Nel 2016 sono stati investiti in Europa circa 3,2 miliardi di EUR nell'IA, rispetto a circa 12,1 miliardi di EUR in America settentrionale e 6,5 miliardi di EUR in Asia[10]. L'Europa ha quindi bisogno di aumentare in modo significativo i suoi livelli di investimento. Il piano coordinato sull'IA[11], sviluppato insieme agli Stati membri, si sta rivelando un buon punto di partenza per rafforzare la cooperazione in materia di IA in Europa e per creare sinergie al fine di massimizzare gli investimenti nella catena del valore dell'IA.

3. COGLIERE LE OPPORTUNITÀ FUTURE: LA PROSSIMA ONDATA DI DATI

Sebbene l'Europa sia attualmente in una posizione più debole per quanto riguarda le applicazioni destinate ai consumatori e le piattaforme online, che si traduce in uno svantaggio competitivo nell'accesso ai dati, sono in corso importanti cambiamenti nel valore e nel riutilizzo di dati tra diversi settori. Il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025[12]. Ogni nuova ondata di dati offre all'Europa l'opportunità di farsi spazio nell'economia agile basata sui dati e diventare un leader mondiale nel settore. Inoltre le

[9] Seguita dal Giappone (30 %) e dagli Stati Uniti (28 %). Fonte: CapGemini (2019).
[10] *10 imperatives for Europe in the age of AI and automation* (10 imperativi per l'Europa nell'era dell'IA e dell'automazione), McKinsey (2017).
[11] COM(2018) 795 final.
[12] IDC (2019).

modalità di conservazione e elaborazione dei dati cambieranno significativamente nei prossimi cinque anni. Attualmente l'80 % delle elaborazioni e delle analisi dei dati che hanno luogo nel cloud vengono effettuate in centri di dati e strutture di calcolo centralizzate e il 20 % in oggetti connessi intelligenti, quali automobili, elettrodomestici o robot di fabbricazione, e in strutture di calcolo vicine all'utente ("*edge computing*"). Entro il 2025 tali proporzioni cambieranno in modo significativo[13].

L'Europa è leader mondiale nel settore dell'elettronica a basso consumo, che è fondamentale per la prossima generazione di processori specializzati per l'IA. Tale mercato è attualmente dominato da soggetti extra UE, ma questa situazione potrebbe cambiare grazie sia a progetti quali l'iniziativa europea in materia di processori, che si concentra sullo sviluppo di sistemi di calcolo a basso consumo sia per l'*edge computing* ad alte prestazioni sia per la prossima generazione di calcolo ad alte prestazioni, sia al lavoro dell'impresa comune per le tecnologie digitali chiave, il cui avvio è stato proposto per il 2021. L'Europa è inoltre leader nelle soluzioni neuromorfiche[14], che sono ideali per l'automazione dei processi industriali (industria 4.0) e dei modi di trasporto e possono migliorare l'efficienza energetica di vari ordini di grandezza.

I recenti progressi nell'ambito del calcolo quantistico genereranno un aumento esponenziale della capacità di elaborazione[15]. L'Europa può essere all'avanguardia in questa tecnologia grazie all'alto livello accademico nell'ambito del calcolo quantistico, nonché alla forte posizione dell'industria europea nell'ambito dei simulatori quantistici e degli ambienti di programmazione per il calcolo quantistico. Le iniziative europee volte ad aumentare la disponibilità di strutture di prova e sperimentazione quantistica contribuiranno all'applicazione di queste nuove soluzioni quantistiche a numerosi settori industriali e accademici.

Parallelamente, l'Europa continuerà a guidare il progresso per quanto riguarda le basi algoritmiche dell'IA, basandosi sulla propria eccellenza scientifica. È necessario creare collegamenti tra discipline che attualmente lavorano separatamente, come l'apprendimento automatico (*machine learning*) e l'apprendimento profondo (*deep learning*), che sono caratterizzati da una limitata interpretabilità e dalla necessità di una grande quantità di dati per addestrare i modelli e apprendere mediante correlazioni, e gli approcci simbolici, in cui le regole sono create mediante l'intervento umano. Combinare il ragionamento simbolico con le reti neurali profonde può aiutarci a rendere maggiormente spiegabili i risultati dell'IA.

4. UN ECOSISTEMA DI ECCELLENZA

Per costruire un ecosistema di eccellenza che possa sostenere lo sviluppo e l'adozione dell'IA nell'economia e nella pubblica amministrazione dell'UE è necessario intensificare le azioni su più livelli.

A. COLLABORAZIONE CON GLI STATI MEMBRI

Nell'ambito dell'attuazione della strategia sull'IA adottata nell'aprile 2018[16], la Commissione ha presentato, nel dicembre 2018, un piano coordinato predisposto insieme agli Stati membri per promuovere lo sviluppo e l'utilizzo dell'intelligenza artificiale in Europa[17].

[13] Gartner (2017).
[14] Per soluzioni neuromorfiche si intendono tutti i sistemi di circuiti integrati su larghissima scala (VLSI) che imitano le architetture neurobiologiche presenti nel sistema nervoso.
[15] I computer quantistici avranno la capacità di elaborare in un tempo inferiore al secondo set di dati molto più grandi rispetto ai computer attuali con le più alte prestazioni, consentendo lo sviluppo di nuove applicazioni di IA in tutti i settori.
[16] L'intelligenza artificiale per l'Europa, COM(2018) 237 final.

Tale piano propone circa 70 azioni comuni per una cooperazione più stretta ed efficiente tra gli Stati membri e la Commissione in settori chiave quali la ricerca, gli investimenti, l'adozione da parte del mercato, le competenze e i talenti, i dati e la cooperazione internazionale. Si prevede che il piano durerà fino al 2027, con monitoraggi e revisioni periodiche.

L'obiettivo è di massimizzare l'impatto degli investimenti in ricerca, innovazione e diffusione dell'IA, valutare le strategie nazionali in materia di IA nonché sviluppare ed estendere il piano coordinato sull'IA in collaborazione con gli Stati membri.

- *Azione 1: la Commissione, tenendo conto dei risultati della consultazione pubblica sul libro bianco, proporrà agli Stati membri una revisione del piano coordinato da adottare entro la fine del 2020.*

Il finanziamento dell'IA a livello di UE dovrebbe attrarre e mettere in comune gli investimenti in settori in cui gli sforzi richiesti vanno al di là di quanto i singoli Stati membri possono ottenere. L'obiettivo è attrarre, nei prossimi dieci anni, oltre 20 miliardi di EUR[18] di investimenti totali annui nell'IA nell'Unione europea. Per stimolare gli investimenti pubblici e privati, l'UE metterà a disposizione risorse provenienti dal programma Europa digitale, da Orizzonte Europa e dai Fondi strutturali e di investimento europei per far fronte alle esigenze delle regioni meno sviluppate e delle zone rurali.

Il piano coordinato potrebbe inoltre considerare il benessere della società e dell'ambiente quale principio chiave per l'IA. I sistemi di IA promettono di contribuire ad affrontare le preoccupazioni più urgenti, tra cui i cambiamenti climatici e il degrado ambientale; è importante che ciò avvenga in modo compatibile con l'ambiente. La stessa IA può e dovrebbe esaminare in modo critico l'uso di risorse e il consumo di energia ed essere addestrata ad effettuare scelte positive per l'ambiente. La Commissione, in collaborazione con gli Stati membri, prenderà in considerazione le opzioni volte a incoraggiare e promuovere soluzioni di IA che svolgano tali funzioni.

B. CONCENTRARE GLI SFORZI DELLA COMUNITÀ DELLA RICERCA E DELL'INNOVAZIONE

L'Europa non può permettersi di mantenere l'attuale panorama frammentato dei centri di competenza, in cui nessuno di questi raggiunge le dimensioni necessarie per competere con i principali istituti a livello mondiale. È indispensabile creare più reti e sinergie tra diversi centri di ricerca europei sull'intelligenza artificiale e allineare i loro sforzi per migliorarne l'eccellenza, trattenere e attrarre i migliori ricercatori e sviluppare le migliori tecnologie. L'Europa ha bisogno di un centro di ricerca, innovazione e competenza di riferimento che coordini tali sforzi, che rappresenti un referente mondiale di eccellenza nell'IA e che possa attrarre gli investimenti e i migliori talenti nel settore.

I centri e le reti dovrebbero concentrarsi nei settori in cui l'Europa ha il potenziale per diventare leader a livello mondiale, come l'industria, la salute, i trasporti, la finanza, le catene del valore agroalimentari, l'energia/l'ambiente, il settore forestale, l'osservazione della Terra e lo spazio. In tutti questi settori si sta svolgendo la corsa alla leadership mondiale e l'Europa offre notevoli potenzialità, conoscenze e

[17] Piano coordinato sull'intelligenza artificiale, COM (2018) 795 final.
[18] COM(2018) 237 final.

competenze[19]. Altrettanto importante è la creazione di siti di prova e sperimentazione a sostegno dello sviluppo e della successiva diffusione di nuove applicazioni di IA.

- *Azione 2: la Commissione agevolerà la creazione di centri di prova e di eccellenza che possano combinare gli investimenti europei, nazionali e privati, eventualmente anche con un nuovo strumento giuridico. Nell'ambito del quadro finanziario pluriennale per il periodo 2021-2027 la Commissione ha proposto di dedicare un importo ambizioso a sostegno di centri di prova di riferimento a livello mondiale in Europa nel quadro del programma Europa digitale e di integrare tale misura, ove opportuno, con azioni di ricerca e innovazione nel quadro di Orizzonte Europa.*

C. COMPETENZE

L'approccio europeo all'IA dovrà essere sostenuto da misure fortemente incentrate sulle competenze al fine di sopperire alla loro mancanza[20]. La Commissione presenterà a breve un rafforzamento dell'agenda per le competenze, che mira a garantire che tutti in Europa possano beneficiare delle trasformazioni verde e digitale dell'economia dell'UE. Le iniziative potrebbero anche comprendere il sostegno alle autorità di regolamentazione settoriali per migliorare le loro competenze in materia di IA al fine di attuare in modo efficace e efficiente le norme pertinenti. Il piano d'azione per l'istruzione digitale aggiornato contribuirà a migliorare l'uso dei dati e delle tecnologie basate sull'IA, come l'apprendimento e l'analisi predittiva, al fine di migliorare i sistemi di istruzione e di formazione e renderli pronti per l'era digitale. Il piano contribuirà inoltre a far crescere la consapevolezza in merito all'IA a tutti i livelli di istruzione, al fine di preparare i cittadini a decisioni informate che saranno sempre più influenzate dall'IA.

Lo sviluppo delle competenze necessarie per lavorare nel settore dell'IA e il miglioramento del livello delle competenze della forza lavoro per prepararla a una trasformazione guidata dall'IA saranno le priorità della revisione del piano coordinato sull'IA che sarà effettuata insieme agli Stati membri. Ciò potrebbe includere la trasformazione della lista di controllo degli orientamenti etici in un "programma di studi" indicativo per gli sviluppatori di IA che sarà reso disponibile come risorsa per gli istituti di formazione. Occorre impegnarsi in modo particolare per aumentare il numero di donne che ricevono una formazione e sono impiegate in questo settore.

Inoltre un centro di ricerca e innovazione di riferimento per l'IA in Europa attirerebbe talenti da tutto il mondo, grazie alle possibilità che potrebbe offrire, oltre a sviluppare e diffondere l'eccellenza in competenze che si radicano e si sviluppano in tutta Europa.

- *Azione 3: istituire e sostenere, attraverso il pilastro relativo alle competenze avanzate del programma Europa digitale, reti che collegano le università e gli istituti di istruzione superiore principali, al fine di attrarre i migliori professori e scienziati e di offrire corsi di laurea magistrale di eccellenza a livello mondiale nel campo dell'IA.*

Oltre al miglioramento del livello delle competenze, i lavoratori e i datori di lavoro sono interessati direttamente dalla progettazione e dall'uso dei sistemi di IA sul luogo di lavoro. Il coinvolgimento delle parti sociali sarà un fattore cruciale per garantire un approccio antropocentrico all'IA sul lavoro.

[19] Anche il futuro Fondo europeo per la difesa e la cooperazione strutturata permanente (PESCO) offrirà opportunità per la ricerca e lo sviluppo in materia di IA. Tali progetti dovrebbero essere sincronizzati con i più ampi programmi civili dell'UE dedicati all'IA.

[20] https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu.

D. MAGGIORE ATTENZIONE ALLE PMI

Sarà inoltre importante garantire che le PMI possano accedere all'IA e utilizzarla. A tal fine, è opportuno rafforzare ulteriormente i poli dell'innovazione digitale[21] e la piattaforma di IA on demand[22] e promuovere la collaborazione tra le PMI. Il programma Europa digitale sarà determinante per conseguire questi obiettivi. Mentre tutti i poli dell'innovazione digitale dovrebbero fornire sostegno alle PMI affinché comprendano e adottino l'IA, sarà importante che almeno un polo dell'innovazione per Stato membro sia altamente specializzato in IA.

Le PMI e le start-up avranno bisogno di accedere ai finanziamenti al fine di adattare i loro processi o di innovare usando l'IA. Basandosi sul prossimo fondo pilota per gli investimenti di 100 milioni di EUR per l'IA e la blockchain, la Commissione rafforzerà ulteriormente l'accesso ai finanziamenti per l'IA nell'ambito di InvestEU[23]. L'IA è citata esplicitamente tra le aree ammissibili per l'utilizzo della garanzia InvestEU.

- *Azione 4: la Commissione collaborerà con gli Stati membri per garantire che almeno un polo dell'innovazione digitale per Stato membro sia altamente specializzato in IA. I poli dell'innovazione digitale possono ricevere sostegno nell'ambito del programma Europa digitale.*
- *La Commissione e il Fondo europeo per gli investimenti avvieranno un progetto pilota con un investimento di 100 milioni di EUR nel primo trimestre del 2020 per fornire finanziamenti con capitale di rischio per sviluppi innovativi nel campo dell'IA. Fatto salvo l'accordo definitivo sul QFP, l'intenzione della Commissione è di far crescere significativamente tale progetto a partire dal 2021 mediante InvestEU.*

E. PARTENARIATO CON IL SETTORE PRIVATO

È altresì essenziale garantire che il settore privato sia pienamente coinvolto nella definizione dell'agenda per la ricerca e l'innovazione e fornisca il necessario livello di coinvestimenti. Per far ciò è necessario istituire un ampio partenariato pubblico-privato, nonché assicurarsi l'impegno dei massimi dirigenti delle società interessate.

- *Azione 5: nel contesto di Orizzonte Europa, la Commissione istituirà un nuovo partenariato pubblico-privato per l'IA, i dati e la robotica, al fine di unire gli sforzi, garantire il coordinamento della ricerca e dell'innovazione nell'IA, collaborare con altri partenariati pubblico-privati di Orizzonte Europa e lavorare insieme alle strutture di prova e ai poli dell'innovazione digitale precedentemente menzionati.*

[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.
[22] www.Ai4eu.eu.
[23] Europe.eu/investeu.

F. PROMUOVERE L'ADOZIONE DELL'IA NEL SETTORE PUBBLICO

È essenziale che le amministrazioni pubbliche, gli ospedali, i servizi di pubblica utilità e di trasporto, le autorità di vigilanza finanziaria e altri settori di interesse pubblico inizino rapidamente a utilizzare nelle loro attività prodotti e servizi che si basano sull'IA. Un'attenzione particolare sarà rivolta ai settori dell'assistenza sanitaria e dei trasporti, in cui la tecnologia è abbastanza matura da consentire una diffusione su vasta scala.

- *Azione 6: la Commissione avvierà dialoghi settoriali aperti e trasparenti dando priorità agli operatori del servizio pubblico, delle amministrazioni rurali e dell'assistenza sanitaria, al fine di presentare un piano d'azione che faciliti lo sviluppo, la sperimentazione e l'adozione dell'IA. I dialoghi settoriali saranno utilizzati per elaborare uno specifico "Programma di adozione dell'IA", che sosterrà gli appalti pubblici di sistemi di IA e contribuirà a trasformare le procedure stesse degli appalti pubblici.*

G. GARANTIRE L'ACCESSO AI DATI E ALLE INFRASTRUTTURE DI CALCOLO

Le aree di intervento stabilite nel presente libro bianco sono complementari a quelle del piano presentato in parallelo nella strategia europea per i dati. Migliorare l'accesso ai dati e la gestione degli stessi è una questione fondamentale. Senza dati lo sviluppo dell'IA e di altre applicazioni digitali è impossibile. Questo enorme volume di nuovi dati che deve essere ancora generato rappresenta un'opportunità per l'Europa di assumere una posizione di primo piano nella trasformazione basata sui dati e sull'IA. La promozione di pratiche responsabili in materia di gestione dei dati e la conformità dei dati ai principi FAIR[24] contribuiranno a creare fiducia e a garantire la riutilizzabilità dei dati. Altrettanto importante è investire nelle tecnologie e nelle infrastrutture di calcolo chiave.

Nell'ambito del programma Europa digitale la Commissione ha proposto più di 4 miliardi di EUR di finanziamento a sostegno del calcolo quantistico e ad alte prestazioni, compresi l'*edge computing* e l'infrastruttura per l'IA, i dati e il cloud. La strategia europea per i dati sviluppa ulteriormente tali priorità.

H. ASPETTI INTERNAZIONALI

L'Europa si trova nella posizione ideale per esercitare una leadership mondiale costruendo alleanze attorno ai valori condivisi e promuovendo l'uso etico dell'IA. Il lavoro svolto dall'UE nel campo dell'IA ha già influenzato le discussioni a livello internazionale. Nell'elaborare i propri orientamenti etici, il gruppo di esperti ad alto livello ha coinvolto una serie di organizzazioni extra UE e vari osservatori governativi. Parallelamente l'UE è stata coinvolta da vicino nello sviluppo dei principi etici per l'IA dell'OCSE[25]. Il G20 ha successivamente approvato tali principi nella dichiarazione ministeriale sul commercio e l'economia digitale del giugno 2019.

Allo stesso tempo l'UE riconosce che sono in corso importanti lavori sull'IA in altri consessi multilaterali, tra cui il Consiglio d'Europa, l'Organizzazione delle Nazioni Unite per l'educazione, la scienza e la cultura (UNESCO), l'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), l'Organizzazione mondiale del commercio e l'Unione internazionale delle telecomunicazioni (UIT).

[24] *Findable, Accessible, Interoperable and Reusable*, cioè dati reperibili, accessibili, interoperabili e riutilizzabili, come indicato nella relazione finale e nel piano d'azione del gruppo di esperti della Commissione sui dati FAIR, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

[25] https://www.oecd.org/going-digital/ai/principles/.

Nell'ambito delle Nazioni Unite, l'UE sta lavorando per dare seguito alla relazione del gruppo ad alto livello sulla cooperazione digitale, anche per quanto riguarda la raccomandazione sull'IA.

L'UE continuerà a cooperare in materia di IA con i paesi che condividono gli stessi principi, ma anche con gli attori globali, seguendo un approccio che promuova le regole e i valori dell'UE (ad esempio sostenendo la convergenza normativa verso l'alto, garantendo l'accesso alle risorse fondamentali, compresi i dati, e creando condizioni di parità). La Commissione monitorerà da vicino le politiche dei paesi terzi che limitano i flussi di dati e affronterà le restrizioni indebite nei negoziati commerciali bilaterali e mediante iniziative nell'ambito dell'Organizzazione mondiale del commercio. La Commissione è convinta che la cooperazione internazionale sulle questioni riguardanti l'IA debba basarsi su un approccio che promuova il rispetto dei diritti fondamentali, tra cui la dignità umana, il pluralismo, l'inclusione, la non discriminazione e la protezione della privacy e dei dati personali[26], e si adopererà per esportare i suoi valori nel mondo[27]. È inoltre chiaro che lo sviluppo e l'uso responsabili dell'IA possono essere una forza trainante per conseguire gli obiettivi di sviluppo sostenibile e portare avanti l'Agenda 2030.

5. UN ECOSISTEMA DI FIDUCIA: QUADRO NORMATIVO PER L'IA

L'uso dell'IA, come l'uso di qualunque nuova tecnologia, comporta sia opportunità sia rischi. I cittadini temono di essere privati dei mezzi per difendere i loro diritti e la loro sicurezza di fronte alle asimmetrie informative del processo decisionale algoritmico, mentre le imprese sono preoccupate per l'incertezza giuridica. L'IA può contribuire a proteggere la sicurezza dei cittadini e consentire loro di godere dei diritti fondamentali, tuttavia i cittadini temono anche che l'intelligenza artificiale possa avere effetti indesiderati o essere addirittura utilizzata per scopi dolosi. A queste preoccupazioni occorre dare una risposta. Oltre alla mancanza di investimenti e di competenze, la mancanza di fiducia è infatti uno dei fattori principali che frenano una più ampia adozione dell'IA.

Per questo motivo il 25 aprile 2018 la Commissione ha definito una strategia per l'IA[28] che affronta gli aspetti socioeconomici parallelamente a un aumento degli investimenti nella ricerca, nell'innovazione e nelle capacità di IA in tutta l'UE, e ha concordato con gli Stati membri un piano coordinato[29] per l'allineamento delle strategie. La Commissione ha inoltre istituito un gruppo di esperti ad alto livello che, nell'aprile 2019, ha pubblicato orientamenti per un'IA affidabile[30].

La Commissione ha pubblicato una comunicazione[31] in cui accoglie con favore i sette requisiti fondamentali individuati negli orientamenti del gruppo di esperti ad alto livello:

- intervento e sorveglianza umani,
- robustezza tecnica e sicurezza,
- riservatezza e governance dei dati,
- trasparenza,
- diversità, non discriminazione ed equità,
- benessere sociale e ambientale, e

[26] Nell'ambito dello strumento di partenariato, la Commissione finanzierà un progetto di 2,5 milioni di EUR che agevolerà la cooperazione con i partner che condividono gli stessi principi, al fine di promuovere gli orientamenti etici dell'UE in materia di IA e di adottare principi comuni e conclusioni operative.
[27] Presidente Von der Leyen, Un'Unione più ambiziosa – Il mio programma per l'Europa, pag. 17.
[28] COM(2018) 237 final.
[29] COM(2018) 795 final.
[30] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.
[31] COM(2019) 168 final.

- accountability.

Negli orientamenti è compresa inoltre una lista di controllo per l'uso pratico da parte delle imprese. Nella seconda metà del 2019, oltre 350 organizzazioni hanno testato tale lista di controllo e hanno inviato un feedback che il gruppo ad alto livello sta utilizzando per rivedere i propri orientamenti; la conclusione di tale revisione è prevista per giugno 2020. Un risultato fondamentale emerso durante tale processo di feedback è che, sebbene i regimi giuridici o normativi esistenti prevedano già numerose prescrizioni, quelle relative alla trasparenza, alla tracciabilità e alla sorveglianza umana non sono contemplate dalla legislazione vigente in molti settori economici.

In aggiunta a questa serie di orientamenti non vincolanti del gruppo di esperti ad alto livello, e in linea con gli orientamenti politici della presidente, un quadro normativo europeo chiaro rafforzerebbe la fiducia dei consumatori e delle imprese nell'IA e accelererebbe quindi l'adozione della tecnologia. Tale quadro normativo dovrebbe essere coerente con altre azioni volte a promuovere la capacità di innovazione e la competitività dell'Europa in questo settore. Deve inoltre garantire risultati ottimali sul piano sociale, ambientale ed economico nonché il rispetto della legislazione, dei principi e dei valori dell'UE. Ciò è particolarmente importante negli ambiti che interessano direttamente i diritti dei cittadini, ad esempio nel caso delle applicazioni di IA per le forze dell'ordine e la magistratura.

Coloro che si occupano di sviluppare e applicare l'IA sono già soggetti alla legislazione europea in materia di diritti fondamentali (ad esempio per quanto riguarda la protezione dei dati, la privacy, la non discriminazione) e di protezione dei consumatori e alle norme in materia di responsabilità e di sicurezza dei prodotti. I consumatori si attendono lo stesso livello di sicurezza e di rispetto dei loro diritti, indipendentemente dal fatto che un prodotto o un sistema si basi sull'IA. Tuttavia determinate caratteristiche specifiche dell'IA (ad esempio l'opacità) possono rendere più difficile l'applicazione e il rispetto di tale legislazione. Per questo motivo è necessario esaminare se la legislazione attuale sia in grado di affrontare i rischi connessi all'IA e se possa essere applicata in modo efficace, se siano necessarie modifiche della legislazione o se sia necessaria una nuova legislazione.

Considerata la rapida evoluzione dell'IA, il quadro normativo deve lasciare spazio a ulteriori sviluppi. Tutte le modifiche dovrebbe essere limitate a problemi chiaramente individuati per i quali esistono soluzioni praticabili.

Gli Stati membri hanno rilevato l'attuale assenza di un quadro europeo comune. La commissione tedesca per l'etica dei dati ha chiesto un sistema normativo su cinque livelli basato sul rischio che spazi dall'assenza di regolamentazione per i sistemi di IA più innocui a un divieto totale per i più pericolosi. La Danimarca ha appena avviato il prototipo di un "marchio per l'etica dei dati". Malta ha introdotto un sistema di certificazione volontaria per l'IA. Se l'UE non riesce a fornire un approccio comune a livello di Unione, esiste un rischio reale di frammentazione del mercato interno, che comprometterebbe gli obiettivi di fiducia, certezza del diritto e adozione da parte del mercato.

Un solido quadro normativo europeo per un'IA affidabile proteggerà tutti i cittadini europei e contribuirà a creare un mercato interno senza attriti che favorirà l'ulteriore sviluppo e l'adozione dell'IA rafforzando la base industriale dell'Europa nel campo dell'IA.

A. DEFINIZIONE DEL PROBLEMA

L'IA può essere estremamente utile, ad esempio in quanto può rendere prodotti e processi più sicuri, ma può anche risultare dannosa. Tale danno può essere di natura sia materiale (quando incide sulla salute e sulla sicurezza delle persone, provocando perdite di vite umane o danni patrimoniali) sia immateriale (quando causa una perdita della privacy, restrizioni alla libertà di espressione, pregiudizi alla dignità umana o discriminazioni, ad esempio nell'accesso all'occupazione), e può riguardare

un'ampia gamma di rischi. Il quadro normativo dovrebbe concentrarsi su come ridurre al minimo i diversi rischi di danno potenziale, soprattutto quelli più significativi.

I rischi principali connessi all'uso dell'IA riguardano l'applicazione di norme intese a tutelare i diritti fondamentali (comprese la protezione dei dati personali e della privacy e la non discriminazione), nonché le questioni legate alla sicurezza[32] e alla responsabilità.

Rischi per i diritti fondamentali, comprese la protezione dei dati personali e della privacy e la non discriminazione

L'uso dell'IA può pregiudicare i valori su cui si fonda l'Unione e causare violazioni dei diritti fondamentali[33], compresi i diritti alle libertà di espressione e di riunione, la dignità umana, la non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale (ove applicabili in determinati settori), la protezione dei dati personali e della vita privata[34] o il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori. Tali rischi potrebbero derivare da difetti nella progettazione complessiva dei sistemi di IA (anche per quanto riguarda la sorveglianza umana) o dall'uso di dati senza che ne siano state corrette le eventuali distorsioni (ad esempio se un sistema è addestrato utilizzando solo o principalmente dati riguardanti gli uomini, il che comporta risultati non ottimali per quanto concerne le donne).

L'IA può svolgere molte funzioni che in precedenza potevano essere esercitate solo dagli esseri umani. I cittadini e le persone giuridiche saranno pertanto sempre più soggette ad azioni realizzate e a decisioni prese da sistemi di IA o con la loro assistenza; si tratta di un risultato non sempre facile da comprendere e cui è difficile opporsi in modo efficace ove necessario. L'IA aumenta inoltre le possibilità di seguire e analizzare le abitudini quotidiane delle persone. Vi è ad esempio il rischio potenziale che l'IA venga utilizzata, in violazione della normativa dell'UE sulla protezione dei dati e di altre norme, dalle autorità statali o da altri soggetti a fini di sorveglianza di massa, oppure dai datori di lavoro per osservare il comportamento dei loro dipendenti. Poiché permette di analizzare grandi quantità di dati e di individuare collegamenti tra di essi, l'IA può essere usata anche per ricostruire e deanonimizzare dati riguardanti le persone, il che implica nuovi rischi per la protezione dei dati personali anche in relazione a set di dati che di per sé non contengono dati personali. L'IA è utilizzata anche dagli intermediari online per stabilire priorità riguardo alle informazioni da fornire ai loro utenti oppure a fini di moderazione dei contenuti. I dati trattati, le modalità con cui vengono progettate le applicazioni e il margine di intervento umano possono incidere sui diritti alla libertà di espressione, alla protezione dei dati personali e alla privacy nonché sulle libertà politiche.

[32] Ivi comprese le questioni legate alla cibersicurezza, alle applicazioni dell'IA nelle infrastrutture critiche o all'uso illecito dell'IA.

[33] Una ricerca del Consiglio d'Europa dimostra che l'uso dell'IA potrebbe avere ripercussioni su numerosi diritti fondamentali, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

[34] Il regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR) e la direttiva relativa alla vita privata e alle comunicazioni elettroniche (il nuovo regolamento sull'e-Privacy è attualmente in fase di negoziazione) affrontano tali rischi, ma potrebbe esservi la necessità di valutare se i sistemi di IA comportino rischi ulteriori. La Commissione monitorerà e valuterà l'applicazione del GDPR in modo costante.

Alcuni algoritmi dell'IA, se usati per prevedere il rischio di recidiva di atti delittuosi, possono riflettere distorsioni legate alla razza e al genere, prevedendo probabilità di rischio di recidiva diverse per le donne rispetto agli uomini, oppure per i cittadini di un determinato paese rispetto agli stranieri. *Fonte: Tolan S., Miron M., Gomez E. e Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia" (Perché l'apprendimento automatico può portare a risultati iniqui: risultanze della valutazione dei rischi per la giustizia minorile in Catalogna), Best Paper Award, International Conference on AI and Law, 2019.*

Alcuni programmi di IA per l'analisi facciale riflettono distorsioni legate al genere e alla razza, in quanto identificano con maggiore facilità il genere degli uomini di carnagione chiara mentre commettono più errori nel determinare il genere delle donne di pelle più scura. Fonte: *Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency (Atti della 1ª conferenza sull'equità, sulla responsabilità e sulla trasparenza), PMLR 81:77-91, 2018.*

Le distorsioni e le discriminazioni rappresentano un rischio intrinseco di qualunque attività sociale od economica. Il processo decisionale umano non è immune da errori e distorsioni. Queste stesse distorsioni, se presenti nell'IA, potrebbero tuttavia avere effetti molto maggiori e colpire o discriminare numerose persone in assenza dei meccanismi di controllo sociale che disciplinano il comportamento umano[35]. Ciò può accadere anche quando il sistema di IA "apprende" nel corso del suo funzionamento. In tali casi, in cui i risultati non potevano essere evitati o anticipati in fase di progettazione, i rischi deriveranno non da difetti nella progettazione originale del sistema, bensì dagli effetti pratici delle correlazioni o dei modelli che il sistema individua all'interno di un ampio set di dati.

Le caratteristiche specifiche di molte tecnologie di IA, tra cui l'opacità (effetto "scatola nera"), la complessità, l'imprevedibilità e un comportamento parzialmente autonomo, possono rendere difficile verificare il rispetto delle normative dell'UE in vigore volte a proteggere i diritti fondamentali e possono ostacolarne l'applicazione effettiva. Le autorità preposte all'applicazione della legge e le persone interessate potrebbero non disporre dei mezzi per verificare come sia stata presa una determinata decisione con il coinvolgimento di sistemi di IA e, di conseguenza, se sia stata rispettata la normativa pertinente. Le persone fisiche e giuridiche possono incontrare difficoltà nell'accesso effettivo alla giustizia in situazioni in cui tali decisioni possono avere ripercussioni negative su di loro.

Rischi per la sicurezza e per il funzionamento efficace del regime di responsabilità

Le tecnologie di IA incorporate in prodotti e servizi possono presentare nuovi rischi per la sicurezza degli utenti. Ad esempio, a causa di un difetto della tecnologia di riconoscimento degli oggetti, un'auto a guida autonoma può erroneamente identificare un oggetto sulla strada e provocare un incidente causando lesioni e danni materiali. Analogamente ai rischi per i diritti fondamentali, questi rischi

[35] Il Comitato consultivo per le pari opportunità tra uomini e donne della Commissione sta attualmente preparando un parere sull'intelligenza artificiale, che dovrebbe essere adottato all'inizio del 2020, in cui si analizza tra l'altro l'impatto dell'intelligenza artificiale sulla parità di genere. Anche la strategia dell'UE per la parità di genere 2020-2024 affronta il rapporto tra IA e parità di genere. La rete europea di enti nazionali per le pari opportunità (Equinet) pubblicherà una relazione (elaborata da Robin Allen e Dee Masters) intitolata: "Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI" (Disciplinare l'IA: il nuovo ruolo degli enti per le pari opportunità – Affrontare le nuove sfide che l'aumento della digitalizzazione e l'uso dell'IA comportano per l'uguaglianza e la non discriminazione), pubblicazione attesa per l'inizio del 2020.

possono derivare da difetti nella progettazione delle tecnologie di IA, da problemi riguardanti la disponibilità e la qualità dei dati o da altri problemi inerenti all'apprendimento automatico. Sebbene alcuni di questi rischi non riguardino unicamente prodotti e servizi basati sull'IA, l'uso di quest'ultima può aumentare o aggravare i rischi.

La mancanza di disposizioni chiare in materia di sicurezza che affrontino tali rischi può creare, oltre a rischi per le persone interessate, incertezza giuridica per le imprese che commercializzano nell'UE prodotti che integrano sistemi di IA. È possibile che le autorità preposte alla vigilanza del mercato e all'applicazione della legge si trovino in situazioni in cui non sanno se possono intervenire, in quanto potrebbero non avere il potere di farlo oppure non disporre delle adeguate capacità tecniche per l'ispezione dei sistemi[36]. L'incertezza giuridica può quindi ridurre i livelli complessivi di sicurezza e pregiudicare la competitività delle imprese europee.

Qualora si materializzino i rischi per la sicurezza, la mancanza di prescrizioni chiare e le caratteristiche delle tecnologie di IA sopra citate rendono difficile risalire alle decisioni potenzialmente problematiche adottate con il coinvolgimento di sistemi di IA. Ciò a sua volta può creare problemi per le persone che intendano ottenere il risarcimento dei danni subiti in forza della legislazione UE e nazionale vigente in materia di responsabilità[37].

A norma della direttiva sulla responsabilità per danno da prodotti difettosi, il produttore è responsabile dei danni causati da un prodotto difettoso. Tuttavia, nel caso di sistemi basati sull'IA, come quelli delle auto a guida autonoma, può rivelarsi difficile provare che il prodotto è difettoso e dimostrare il danno cagionato e il nesso di causalità tra difetto e danno. In aggiunta non è chiaro come e in che misura si applichi la direttiva sulla responsabilità per danno da prodotti difettosi nel caso di alcuni tipi di difetti, ad esempio per quelli risultanti da carenze della cibersicurezza del prodotto.

Di conseguenza la difficoltà di risalire alle decisioni potenzialmente problematiche adottate da sistemi di IA, di cui si è trattato anteriormente in relazione ai diritti fondamentali, è pertinente anche alle questioni legate alla sicurezza e alla responsabilità. Ad esempio coloro che hanno sofferto danni potrebbero non avere accesso effettivo agli elementi probatori necessari per giustificare un'azione in giudizio, per cui le loro possibilità di ottenere un'effettiva riparazione del danno potrebbero essere inferiori rispetto alle situazioni in cui il pregiudizio è causato da tecnologie tradizionali. Tali rischi aumenteranno man mano che l'uso dell'IA diverrà più diffuso.

B. POSSIBILI ADEGUAMENTI DEL QUADRO LEGISLATIVO VIGENTE DELL'UE PER QUANTO CONCERNE L'IA

Esiste un vasto corpus di norme vigenti dell'UE in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi[38], comprendente norme settoriali ed integrato dalle legislazioni

[36] Un esempio può essere dato dagli smartwatch per bambini. Anche qualora non causino alcun danno diretto ai minori che li indossano, tali prodotti, in assenza di un livello minimo di sicurezza, possono facilmente essere utilizzati per avere accesso al minore. Può essere difficile per le autorità preposte alla vigilanza del mercato intervenire nei casi in cui i rischi non siano legati al prodotto in quanto tale.

[37] Le implicazioni dell'IA, dell'Internet delle cose e di altre tecnologie digitali per la legislazione in materia di sicurezza e responsabilità sono analizzate nella relazione della Commissione che accompagna il presente libro bianco.

[38] Il quadro giuridico dell'UE in materia di sicurezza dei prodotti è costituito dalla direttiva relativa alla sicurezza generale dei prodotti (direttiva 2001/95/CE), che funge da rete di sicurezza, e da una serie di normative settoriali che disciplinano diverse categorie di prodotti, dai macchinari agli aerei, dalle automobili ai giocattoli e ai dispositivi medici, con l'obiettivo di assicurare un elevato livello di salute e sicurezza. La disciplina della responsabilità per danno da prodotti difettosi è integrata da diversi sistemi di responsabilità civile per danni causati da prodotti o servizi.

nazionali; tale corpus di norme è pertinente e potenzialmente applicabile a una serie di applicazioni di IA emergenti.

Per quanto riguarda la protezione dei diritti fondamentali e dei diritti dei consumatori, il quadro legislativo dell'UE comprende atti normativi come la direttiva sull'uguaglianza razziale[39], la direttiva sulla parità di trattamento in materia di occupazione e di condizioni di lavoro[40], le direttive sulla parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e in materia di occupazione[41], una serie di norme sulla tutela dei consumatori[42], sulla protezione dei dati personali e sulla privacy, in particolare il regolamento generale sulla protezione dei dati, nonché altre normative settoriali riguardanti la protezione dei dati personali, come la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie[43]. Inoltre, a partire dal 2025 si applicheranno le norme sui requisiti di accessibilità dei beni e dei servizi previste dall'atto europeo sull'accessibilità[44]. I diritti fondamentali devono inoltre essere rispettati in sede di attuazione di altre normative dell'UE, anche nel settore dei servizi finanziari, della migrazione o della responsabilità degli intermediari online.

Se da un lato la legislazione dell'UE rimane in linea di principio pienamente applicabile, indipendentemente dal coinvolgimento dell'IA, dall'altro è importante valutare se tale normativa possa essere adeguatamente applicata per far fronte ai rischi derivanti dai sistemi di IA o se sia necessario apportare adeguamenti a determinati strumenti giuridici.

Ad esempio, gli operatori economici rimangono pienamente responsabili della conformità dell'IA alle norme vigenti a tutela dei consumatori: è vietato utilizzare algoritmi che sfruttano il comportamento dei consumatori in violazione delle norme vigenti, e qualunque infrazione a tale divieto è punita di conseguenza.

La Commissione ritiene che il quadro legislativo possa essere migliorato per affrontare le situazioni e i rischi descritti di seguito.

- *Effettiva applicazione e rispetto della normativa nazionale e dell'UE in vigore*: le caratteristiche principali dell'IA rendono difficile garantire la corretta applicazione e il rispetto della normativa nazionale e dell'UE. A causa della mancanza di trasparenza (opacità dell'IA) è difficile individuare e dimostrare eventuali violazioni delle disposizioni normative (comprese quelle che tutelano i diritti fondamentali), attribuire la responsabilità e soddisfare le condizioni per chiedere un risarcimento. Pertanto, al fine di garantire l'effettiva applicazione e il rispetto delle norme, può essere necessario adeguare o chiarire la legislazione in vigore in determinati settori, ad esempio in materia di responsabilità, come ulteriormente specificato nella relazione che accompagna il presente libro bianco.

- *Limiti dell'ambito di applicazione della legislazione dell'UE vigente*: un aspetto essenziale su cui si concentra la legislazione dell'UE in materia di sicurezza dei prodotti è l'immissione degli stessi sul mercato. Anche se, conformemente alla legislazione dell'UE in materia di sicurezza dei prodotti, il software, quando è parte del prodotto finale, deve rispettare le norme pertinenti

[39] Direttiva 2000/43/CE.
[40] Direttiva 2000/78/CE.
[41] Direttiva 2004/113/CE; direttiva 2006/54/CE.
[42] Come la direttiva sulle pratiche commerciali sleali (direttiva 2005/29/CE) e la direttiva sui diritti dei consumatori (direttiva 2011/83/CE).
[43] 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.
[44] Direttiva (UE) 2019/882 sui requisiti di accessibilità dei prodotti e dei servizi.

in materia di sicurezza dei prodotti, rimane da stabilire se il software indipendente (*stand-alone*) rientri nell'ambito di applicazione della normativa dell'UE in materia di sicurezza dei prodotti, al di là di alcuni settori in cui esistono norme esplicite al riguardo[45]. La normativa generale dell'UE in materia di sicurezza attualmente in vigore si applica ai prodotti ma non ai servizi, per cui in linea di principio non si applica nemmeno ai servizi basati sulla tecnologia di IA (ad esempio servizi sanitari, finanziari e di trasporto).

- *Funzionalità mutevole dei sistemi di IA*: l'integrazione del software, compresa l'IA, nei prodotti può modificare il funzionamento di tali prodotti e sistemi durante il loro ciclo di vita. Ciò vale in particolare per i sistemi che richiedono frequenti aggiornamenti del software o che si basano sull'apprendimento automatico. Tali caratteristiche possono dar luogo a nuovi rischi che non erano presenti quando il sistema è stato immesso sul mercato. Tali rischi non sono adeguatamente disciplinati dalla legislazione esistente, che si concentra prevalentemente sui rischi per la sicurezza presenti al momento dell'immissione sul mercato.

- *Incertezza in merito all'attribuzione delle responsabilità tra i diversi operatori economici lungo la catena di approvvigionamento*: in linea generale, la legislazione dell'UE in materia di sicurezza dei prodotti attribuisce al fabbricante la responsabilità del prodotto immesso sul mercato e di tutti i suoi componenti, ad esempio i sistemi di IA. In alcuni casi le norme possono però divenire poco chiare, ad esempio se l'IA è integrata nel prodotto dopo che quest'ultimo è stato immesso sul mercato da un soggetto diverso dal produttore. Inoltre la legislazione dell'UE in materia di responsabilità per danno da prodotti difettosi prevede la responsabilità dei produttori e lascia alle disposizioni nazionali in materia il compito di disciplinare la responsabilità di altri soggetti nella catena di approvvigionamento.

- *Evoluzione del concetto di sicurezza:* l'uso dell'IA nei prodotti e nei servizi può dar luogo a rischi che la legislazione dell'UE attualmente non affronta in modo esplicito. Tali rischi possono essere collegati alle minacce informatiche, possono riguardare la sicurezza personale (ad esempio i rischi collegati a nuove applicazioni dell'IA, come nel caso dell'IA applicata agli elettrodomestici), o ancora possono derivare dalla perdita di connettività, ecc. Tali rischi possono essere presenti al momento dell'immissione dei prodotti sul mercato, o derivare da aggiornamenti del software o dall'apprendimento automatico durante l'uso del prodotto. L'UE dovrebbe avvalersi appieno degli strumenti a sua disposizione per rafforzare la base di conoscenze scientifiche di cui dispone sui potenziali rischi connessi alle applicazioni di IA, sfruttando anche l'esperienza dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) al fine di valutare il panorama delle minacce dell'IA.

[45] Ad esempio, il software destinato dal fabbricante a essere impiegato per fini medici è considerato un dispositivo medico a norma del regolamento sui dispositivi medici [regolamento (UE) 2017/745].

Come indicato in precedenza, vari Stati membri stanno già valutando diverse opzioni per affrontare attraverso la legislazione nazionale le sfide poste dall'IA. Ciò comporta un rischio di frammentazione del mercato unico. Norme nazionali divergenti possono creare ostacoli per le imprese che intendono

Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità

La relazione che accompagna il presente libro bianco analizza il quadro giuridico pertinente, individuando le incertezze riguardanti l'applicazione di tale quadro giuridico in relazione ai rischi specifici derivanti dai sistemi di IA e da altre tecnologie digitali.

La conclusione è che la legislazione vigente in materia di sicurezza dei prodotti sostiene già un concetto ampio di sicurezza, con l'obiettivo di proteggere da tutti i tipi di rischi derivanti dal prodotto in funzione dell'uso dello stesso. Per garantire una maggiore certezza del diritto si potrebbero tuttavia introdurre disposizioni che contemplino esplicitamente i nuovi rischi derivanti dalle tecnologie digitali emergenti.

- Il comportamento autonomo che mostrano alcuni sistemi di IA durante il loro ciclo di vita può comportare modifiche significative dei prodotti, che a loro volta hanno ripercussioni sulla sicurezza e possono rendere necessaria una nuova valutazione dei rischi. Potrebbe inoltre rendersi necessaria, come misura di salvaguardia, la sorveglianza umana dalla fase di progettazione e durante tutto il ciclo di vita dei prodotti e dei sistemi di IA.
- Ove opportuno potrebbero essere presi in considerazione obblighi espliciti per i produttori anche in relazione ai rischi per la sicurezza mentale degli utenti (ad esempio dovuti alla collaborazione con robot umanoidi).
- La legislazione dell'Unione in materia di sicurezza dei prodotti potrebbe prevedere prescrizioni specifiche che affrontino i rischi per la sicurezza derivanti dall'uso di dati errati in fase di progettazione, nonché meccanismi per garantire che sia mantenuta la qualità dei dati durante l'intero periodo di utilizzo dei prodotti e dei sistemi di IA.
- Il problema dell'opacità dei sistemi basati su algoritmi potrebbe essere affrontato mediante prescrizioni in materia di trasparenza.
- Potrebbe essere necessario adeguare e chiarire le norme vigenti in relazione ai casi di software indipendente immesso sul mercato senza altri componenti, oppure integrato in un prodotto dopo che quest'ultimo è stato immesso sul mercato, qualora ciò abbia un impatto sulla sicurezza.
- Data la crescente complessità delle catene di approvvigionamento in relazione alle nuove tecnologie, disposizioni che richiedano specificamente una collaborazione tra gli utenti e gli operatori economici attivi lungo la catena di approvvigionamento potrebbero garantire la certezza del diritto.

Le caratteristiche delle tecnologie digitali emergenti, come l'IA, l'Internet delle cose e la robotica, possono mettere in discussione alcuni aspetti dei quadri giuridici relativi alla responsabilità e renderli meno efficaci. Alcune di queste caratteristiche potrebbero rendere difficile far risalire il danno alla condotta di una persona, condizione indispensabile per invocare la responsabilità per colpa conformemente alla maggior parte delle norme nazionali in materia. Ne deriva la possibilità che i costi per le vittime aumentino in maniera significativa, e la potenziale difficoltà di avviare azioni per responsabilità nei confronti di soggetti diversi dal produttore e di ottenere elementi di prova a sostegno di tali azioni.

- Le persone che hanno subito un danno provocato con il coinvolgimento di sistemi di IA devono godere dello stesso livello di protezione delle persone che hanno subito danni causati da altre tecnologie; nel contempo occorre che l'innovazione tecnologica possa continuare a svilupparsi.
- È opportuno valutare attentamente tutte le opzioni che consentano di raggiungere tale obiettivo, compresa la possibilità di modificare la direttiva sulla responsabilità per danno da prodotti difettosi e ulteriori possibili interventi mirati di armonizzazione delle norme nazionali in materia di responsabilità. Ad esempio, la Commissione sta valutando se e in quale misura sia necessario mitigare le conseguenze della complessità adeguando l'onere della prova richiesto dalle norme nazionali in materia di responsabilità in relazione ai danni provocati dal funzionamento delle applicazioni di IA.

vendere e gestire sistemi di IA nel mercato unico. Garantire un approccio comune a livello di UE consentirebbe alle imprese europee di beneficiare di un accesso agevole al mercato unico e favorirebbe la loro competitività sui mercati mondiali.

In base a quanto esposto in precedenza la Commissione conclude che, oltre agli eventuali adeguamenti della legislazione esistente, potrebbe essere necessaria una nuova normativa specifica sull'IA al fine di adeguare il quadro giuridico dell'UE agli sviluppi tecnologici e commerciali attuali e futuri.

C. AMBITO DI APPLICAZIONE DI UN FUTURO QUADRO NORMATIVO DELL'UE

La determinazione dell'ambito di applicazione del futuro quadro normativo specifico sull'IA rappresenta una questione essenziale. L'ipotesi di lavoro è che il quadro normativo si applichi a prodotti e servizi basati sull'IA. Ai fini del presente libro bianco e di qualsiasi eventuale iniziativa futura di elaborazione delle politiche dovrebbe essere stabilita una definizione chiara di IA.

Nella sua comunicazione dal titolo "L'intelligenza artificiale per l'Europa" la Commissione ha fornito una prima definizione di IA[46], che poi è stata ulteriormente perfezionata dal gruppo di esperti ad alto livello[47].

Qualunque nuovo strumento giuridico dovrà comprendere una definizione di IA abbastanza flessibile da accogliere il progresso tecnico, ma anche sufficientemente precisa da garantire la necessaria certezza del diritto.

Ai fini del presente libro bianco e di eventuali future discussioni su iniziative strategiche, sembra importante chiarire gli elementi principali da cui è composta l'IA, vale a dire i "dati" e gli "algoritmi". L'IA può essere integrata nell'hardware. Nel caso delle tecniche di apprendimento automatico, che costituiscono un sottoinsieme dell'IA, gli algoritmi vengono addestrati per dedurre determinati modelli partendo da un set di dati al fine di stabilire le azioni necessarie al conseguimento di un determinato obiettivo.

> Nel caso della guida autonoma, ad esempio, l'algoritmo utilizza in tempo reale dati forniti dall'automobile (velocità, consumo del motore, dati relativi agli ammortizzatori, ecc.) e dai sensori che rilevano tutti i dati dell'ambiente in cui si trova l'automobile (strada, segnali, altri veicoli, pedoni, ecc.) per stabilire quale direzione dovrebbe prendere l'automobile e con quale accelerazione e velocità al fine di raggiungere una determinata destinazione. L'algoritmo si basa sui dati rilevati e si adegua alla situazione della strada ed alle condizioni esterne, compreso il comportamento degli altri conducenti, al fine di ottenere la guida più sicura e più comoda.

Gli algoritmi possono continuare a imparare mentre vengono utilizzati. Sebbene i prodotti basati sull'IA possano agire in modo autonomo percependo il proprio ambiente senza seguire un insieme di istruzioni predeterminate, il loro comportamento è in larga misura definito e limitato dai loro

[46] COM(2018) 237 final, pag. 1: "Intelligenza artificiale (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)."

[47] Gruppo di esperti ad alto livello, Una definizione di IA, pag. 8: "I sistemi di intelligenza artificiale (IA) sono sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti."

sviluppatori. Gli esseri umani determinano e programmano gli obiettivi che un sistema di IA dovrebbe raggiungere nel modo più efficace.

L'UE ha istituito un quadro giuridico rigoroso i cui obiettivi sono, tra gli altri, garantire la tutela dei consumatori, far fronte alle pratiche commerciali sleali e proteggere i dati personali e la privacy. L'acquis prevede inoltre norme settoriali specifiche (ad esempio per il settore dell'assistenza sanitaria o dei trasporti). Tali disposizioni vigenti del diritto dell'UE continueranno ad applicarsi in relazione all'IA, ma potrebbero rendersi necessari determinati adeguamenti di tale quadro giuridico per tenere conto della trasformazione digitale e dell'uso dell'IA (cfr. sezione B). Di conseguenza, gli aspetti già trattati dalla legislazione orizzontale o settoriale in vigore (ad esempio per quanto riguarda i dispositivi medici[48] o i sistemi di trasporto) continueranno ad essere disciplinati da tale legislazione.

In linea di principio il nuovo quadro normativo per l'IA dovrebbe essere efficace nel raggiungimento dei propri obiettivi, senza tuttavia essere talmente prescrittivo da creare oneri sproporzionati, in particolare per le PMI. Per raggiungere tale equilibrio la Commissione ritiene opportuno seguire un approccio basato sul rischio.

Tale approccio basato sul rischio è importante per garantire la proporzionalità dell'intervento normativo, ma richiede che siano definiti criteri chiari per distinguere tra le diverse applicazioni di IA, in particolare per stabilire se tali applicazioni siano o meno "ad alto rischio"[49]. I criteri per stabilire che cosa sia un'applicazione di IA ad alto rischio dovrebbero essere chiari, facilmente comprensibili e applicabili a tutte le parti interessate. Le applicazioni di IA rimangono comunque interamente soggette al diritto vigente dell'UE, anche qualora non siano considerate ad alto rischio.

La Commissione ritiene che, per stabilire in generale se una determinata applicazione di IA debba essere ritenuta ad alto rischio, occorra valutare gli interessi in gioco e considerare se il settore interessato e l'uso previsto per tale applicazione implichino rischi significativi, in particolare per quanto concerne la protezione della sicurezza, dei diritti dei consumatori e dei diritti fondamentali. Più specificamente, un'applicazione di IA dovrebbe essere considerata ad alto rischio se soddisfa i due criteri cumulativi descritti di seguito.

- In primo luogo, l'applicazione di IA è utilizzata in un settore in cui, date le caratteristiche delle attività abitualmente svolte, si possono prevedere rischi significativi. Questo primo criterio garantisce che l'intervento normativo sia mirato ai settori in cui i rischi sono generalmente ritenuti più probabili. I settori interessati dovrebbero essere elencati in maniera specifica ed esaustiva nel nuovo quadro normativo. Ad esempio, settori dell'assistenza sanitaria, dei trasporti; dell'energia e parti del settore pubblico[50]. L'elenco dovrebbe essere periodicamente rivisto e modificato, ove necessario, in funzione dei pertinenti sviluppi nella pratica.
- In secondo luogo, l'applicazione dell'IA nel settore in questione è inoltre utilizzata in modo tale da poter generare rischi significativi. Questo secondo criterio riconosce il fatto che non tutti gli usi dell'IA nei settori selezionati comportano necessariamente rischi significativi. Ad esempio, per quanto l'assistenza sanitaria in genere possa essere certamente un settore

[48] Ad esempio vi sono diverse considerazioni in materia di sicurezza e varie implicazioni giuridiche riguardanti i sistemi di IA che forniscono ai medici informazioni sanitarie specializzate, i sistemi di IA che forniscono informazioni mediche direttamente al paziente e i sistemi di IA che svolgono essi stessi funzioni di carattere medico su un paziente. La Commissione sta esaminando queste sfide in materia di sicurezza e responsabilità, che caratterizzano il settore dell'assistenza sanitaria.

[49] La legislazione dell'UE può classificare i "rischi" in modo diverso da quanto qui descritto, in funzione del settore, come ad esempio per la sicurezza dei prodotti.

[50] Il settore pubblico potrebbe includere ambiti quali il diritto di asilo, la migrazione, i controlli alle frontiere e il potere giudiziario, la sicurezza sociale e i servizi per l'impiego.

rilevante, un eventuale difetto del sistema di prenotazione degli appuntamenti in un ospedale non presenta, in linea di massima, rischi tali da giustificare un intervento legislativo. La valutazione del livello di rischio derivante da un determinato uso potrebbe basarsi sull'impatto per i soggetti interessati. Ad esempio, usi delle applicazioni di IA che producono effetti giuridici, o effetti altrettanto rilevanti, sui diritti di una persona o di una società; usi che presentano il rischio di lesioni, morte o danni materiali o immateriali significativi; usi che producono effetti non ragionevolmente evitabili dalle persone fisiche o giuridiche.

L'applicazione dei due criteri cumulativi garantirebbe un ambito di applicazione del quadro normativo mirato e atto a garantire la certezza del diritto. Le prescrizioni obbligatorie contenute nel nuovo quadro normativo sull'IA (cfr. sezione D) si applicherebbero in linea di principio unicamente a quelle che siano state identificate come applicazioni ad alto rischio utilizzando i due criteri cumulativi sopra descritti.

Fatto salvo quanto precede, possono esistere anche casi eccezionali in cui, a causa dei rischi in gioco, l'uso di applicazioni di IA per determinati scopi deve essere considerato ad alto rischio di per sé, ossia indipendentemente dal settore interessato, per cui si applicherebbero comunque le prescrizioni di seguito indicate[51]. A titolo illustrativo si possono citare in particolare i seguenti usi:

- Alla luce dell'importanza che riveste per le persone, e tenendo conto dell'acquis dell'UE sulla parità in materia di occupazione, l'uso delle applicazioni di IA nei processi di selezione del personale e nelle situazioni che incidono sui diritti dei lavoratori sarebbe sempre considerato "ad alto rischio" e quindi si applicherebbero sempre le prescrizioni sotto indicate. Potrebbero essere prese in considerazione ulteriori applicazioni specifiche che incidono sui diritti dei consumatori.

- L'uso delle applicazioni di IA a fini di identificazione biometrica remota[52] e l'impiego di altre tecnologie di sorveglianza intrusive sarebbero sempre considerati "ad alto rischio", per cui si applicherebbero sempre le prescrizioni sotto indicate.

D. TIPI DI PRESCRIZIONI

In fase di elaborazione del futuro quadro normativo in materia di IA sarà necessario decidere quali tipi di prescrizioni giuridiche obbligatorie imporre ai soggetti interessati. Tali prescrizioni possono essere ulteriormente specificate mediante il ricorso a norme. Come osservato nella sezione C, e in aggiunta alla legislazione già in vigore, tali prescrizioni si applicherebbero soltanto alle applicazioni di IA ad alto rischio, in modo da garantire che qualsiasi intervento normativo sia mirato e proporzionato.

Tenendo conto degli orientamenti del gruppo di esperti ad alto livello e di quanto esposto in precedenza, le prescrizioni per le applicazioni di IA ad alto rischio potrebbero riguardare i seguenti elementi essenziali, ulteriormente discussi nelle sottosezioni che seguono:

- i dati di addestramento;
- la tenuta dei dati e dei registri;

[51] È importante sottolineare che potrebbero applicarsi anche altre normative dell'UE. Ad esempio, se le applicazioni di IA sono incorporate in un prodotto di consumo, la sicurezza di tali applicazioni può essere disciplinata dalla direttiva sulla sicurezza generale dei prodotti.

[52] L'identificazione biometrica remota dovrebbe essere distinta dall'autenticazione biometrica (quest'ultima è un processo di sicurezza basato sulle caratteristiche biologiche uniche di un individuo, utilizzato per verificare che quest'ultimo sia chi afferma di essere). L'identificazione biometrica remota serve a determinare l'identità di più persone utilizzando identificatori biometrici (impronte digitali, immagine del volto, iride, schema delle vene, ecc.) a distanza, in uno spazio pubblico e in modo continuo o permanente confrontandoli con i dati contenuti in una banca dati.

- le informazioni da fornire;
- la robustezza e la precisione;
- la sorveglianza umana;
- prescrizioni specifiche per determinate applicazioni particolari dell'IA, come quelle utilizzate a fini di identificazione biometrica remota.

Al fine di garantire la certezza del diritto, tali prescrizioni saranno ulteriormente precisate per fornire un chiaro punto di riferimento a tutti i soggetti chiamati a rispettarle.

a) Dati di addestramento

È più importante che mai promuovere, rafforzare e difendere i valori e le regole dell'UE, in particolare i diritti di cui i cittadini godono grazie al diritto dell'UE. Questi sforzi vanno senza dubbio estesi anche alle applicazioni di IA ad alto rischio qui in esame, commercializzate e utilizzate nell'UE.

Come discusso in precedenza, l'IA non può esistere senza i dati. Il funzionamento di numerosi sistemi di IA, nonché le azioni e le decisioni che ne possono derivare, dipendono in larga misura dai set di dati utilizzati per addestrarli. Occorre dunque adottare le misure necessarie per garantire che, nell'individuare i dati di addestramento dei sistemi di IA, siano rispettati i valori e le norme dell'UE, in particolare per quanto riguarda la sicurezza e le norme vigenti in materia di tutela dei diritti fondamentali. Si potrebbero prevedere le seguenti prescrizioni per quanto concerne i dati utilizzati per l'addestramento dei sistemi di IA:

- prescrizioni volte a fornire ragionevoli garanzie circa la sicurezza dell'uso successivo dei prodotti e dei servizi basati sull'IA; tale sicurezza è intesa come conformità agli standard stabiliti dalle norme dell'UE applicabili in materia di sicurezza (sia quelle vigenti, sia eventuali norme complementari). Si tratta ad esempio di prescrizioni volte a garantire che i sistemi di IA siano addestrati utilizzando set di dati sufficientemente ampi e che contemplino tutti gli scenari pertinenti, in modo da evitare situazioni pericolose;

- prescrizioni che impongano di adottare misure ragionevoli per garantire che tale uso successivo dei sistemi di IA non porti a risultati che implichino discriminazioni vietate. Tali prescrizioni potrebbero comportare, in particolare, l'obbligo di utilizzare set di dati sufficientemente rappresentativi, in particolare per garantire che rispecchino adeguatamente tutte le pertinenti dimensioni di genere, etnia e altri possibili motivi di discriminazione vietata;

- prescrizioni volte a garantire un'adeguata protezione della privacy e dei dati personali durante l'uso dei prodotti e dei servizi basati sull'IA. Tali questioni sono disciplinate dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie per la parte che rientra nel loro rispettivo ambito di applicazione.

b) Tenuta dei dati e dei registri

Tenuto conto di elementi quali la complessità e l'opacità di molti sistemi di IA, nonché delle conseguenti difficoltà che possono sorgere nel garantire l'effettiva applicazione e il rispetto delle norme pertinenti, sono necessarie prescrizioni per la tenuta di registri relativi alla programmazione dell'algoritmo, ai dati utilizzati per addestrare sistemi di IA ad alto rischio e, in alcuni casi, per la tenuta dei dati stessi. Tali prescrizioni consentono essenzialmente di risalire alle azioni o decisioni potenzialmente problematiche dei sistemi di IA e di verificarle. Ciò dovrebbe non solo agevolare la vigilanza e l'applicazione delle norme, ma anche aumentare gli incentivi affinché gli operatori economici interessati tengano conto sin dall'inizio dell'esigenza di rispettare tali norme.

A tal fine il quadro normativo potrebbe prescrivere l'obbligo di tenere:

- registri accurati dei set di dati utilizzati per addestrare e sottoporre a prova i sistemi di IA, compresa una descrizione delle principali caratteristiche e delle modalità di selezione di tali insiemi;

- in taluni casi giustificati, gli stessi set di dati;

- la documentazione relativa alle metodologie, alle procedure e alle tecniche di programmazione[53] e di addestramento utilizzate per costruire, sottoporre a prova e convalidare i sistemi di IA, ove opportuno anche in materia di sicurezza, evitando distorsioni che potrebbero dar luogo a discriminazioni vietate.

I registri, la documentazione e, se del caso, i set di dati dovrebbero essere conservati per un periodo di tempo limitato e ragionevole al fine di garantire l'effettiva applicazione della legislazione pertinente. È opportuno adottare misure per garantire che tali elementi siano messi a disposizione su richiesta, in particolare per essere sottoposti a prove o ispezioni da parte delle autorità competenti. Ove necessario, è opportuno prevedere modalità per garantire la tutela delle informazioni riservate, come i segreti commerciali.

c) Obblighi di informazione

La trasparenza è necessaria anche al di là degli obblighi di tenuta dei registri di cui al punto c). Al fine di conseguire gli obiettivi perseguiti, in particolare promuovere un uso responsabile dell'IA, rafforzare la fiducia e agevolare la riparazione del danno ove necessario, è importante che vengano fornite in maniera proattiva informazioni adeguate sull'uso dei sistemi di IA ad alto rischio.

Potrebbero pertanto essere prese in considerazione le seguenti prescrizioni volte a:

- garantire che vengano fornite informazioni chiare sulle capacità e sulle limitazioni dei sistemi di IA, in particolare per quanto riguarda l'obiettivo per il quale i sistemi sono stati concepiti, le condizioni alle quali ci si può attendere che funzionino come previsto e il livello di precisione previsto nel raggiungimento dell'obiettivo specificato. Tali informazioni sono importanti soprattutto per coloro che applicano i sistemi, ma possono essere rilevanti anche per le autorità competenti e le parti interessate;

- informare i cittadini separatamente e con chiarezza quando questi interagiscono con un sistema di IA e non con un essere umano. Anche se la normativa dell'UE in materia di protezione dei dati contiene già alcune disposizioni analoghe[54], potrebbero essere necessarie ulteriori prescrizioni per raggiungere gli obiettivi sopra indicati. In tal caso occorre evitare oneri inutili. Non è quindi necessario fornire tali informazioni, ad esempio, quando ai cittadini sia immediatamente evidente che interagiscono con sistemi di IA. È inoltre importante che le informazioni fornite siano obiettive, concise e di facile comprensione. Le modalità di presentazione delle informazioni dovrebbero essere adeguate al contesto specifico.

[53] Si tratta ad esempio della documentazione riguardante l'algoritmo, compresi l'obiettivo di ottimizzazione perseguito dal modello, le ponderazioni inizialmente concepite per determinati parametri, ecc.

[54] In particolare, a norma dell'articolo 13, paragrafo 2, lettera f), del GDPR, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento è tenuto a fornire agli interessati ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente in relazione all'esistenza di un processo decisionale automatizzato, oltre a determinate informazioni aggiuntive.

d) Robustezza e precisione

Per essere affidabili, i sistemi di IA (ed in particolare le applicazioni di IA ad alto rischio) devono essere tecnicamente robusti e precisi. Ciò significa che tali sistemi devono essere sviluppati in modo responsabile e con la debita e adeguata valutazione ex ante dei rischi che possono generare. Il loro sviluppo e funzionamento devono essere tali da garantire che tali sistemi si comportino in modo affidabile secondo le previsioni. Dovrebbero essere adottate tutte le misure ragionevoli per ridurre al minimo il rischio di danni.

Potrebbero pertanto essere presi in considerazioni i seguenti elementi:

- prescrizioni che garantiscano la robustezza e la precisione dei sistemi di IA, o che almeno riflettano correttamente il loro livello di precisione, durante tutte le fasi del ciclo di vita;

- prescrizioni atte a garantire la riproducibilità dei risultati;

- prescrizioni atte a garantire che i sistemi di IA possano gestire adeguatamente gli errori o le incongruenze in tutte le fasi del ciclo di vita;

- prescrizioni volte a assicurare la resilienza dei sistemi di IA sia agli attacchi palesi sia ai tentativi meno evidenti di manipolare i dati o gli stessi algoritmi, e a garantire che in tali casi siano adottate misure di attenuazione.

e) Sorveglianza umana

La sorveglianza umana aiuta a garantire che un sistema di IA non comprometta l'autonomia umana o provochi altri effetti negativi. L'obiettivo di un'IA affidabile, etica e antropocentrica può essere raggiunto solo garantendo un adeguato coinvolgimento degli esseri umani in relazione alle applicazioni di IA ad alto rischio.

Sebbene tutte le applicazioni di IA prese in considerazione nel presente libro bianco per un regime giuridico specifico siano ritenute ad alto rischio, il tipo e il livello adeguati di sorveglianza umana possono variare da un caso all'altro. Dipende in particolare dall'uso previsto dei sistemi e dagli effetti che potrebbero derivarne per le persone giuridiche e i cittadini interessati, senza pregiudizio per i diritti stabiliti dal GDPR in relazione al trattamento di dati personali da parte di sistemi di IA. La sorveglianza umana potrebbe ad esempio essere esercitata nei modi descritti di seguito a titolo meramente indicativo:

- il risultato del sistema di IA non diviene effettivo prima di essere stato rivisto e convalidato da un essere umano (ad esempio, la decisione di respingere una richiesta di prestazioni di sicurezza sociale può essere presa unicamente da un essere umano);

- il risultato del sistema di IA diviene immediatamente effettivo, ma successivamente è garantito l'intervento di un essere umano (ad esempio, la decisione di respingere la richiesta di una carta di credito può essere adottata da un sistema di IA, ma successivamente deve essere possibile il riesame da parte di un essere umano);

- il sistema di IA può essere monitorato durante il suo funzionamento da un essere umano che può intervenire in tempo reale e disattivarlo (ad esempio, prevedendo su un'auto a guida autonoma un pulsante o una procedura di arresto che un essere umano può attivare qualora decida che il funzionamento dell'auto non è sicuro);

- in fase di progettazione, imponendo vincoli operativi al sistema di IA (ad esempio, in determinate condizioni di scarsa visibilità in cui i sensori divengono meno affidabili, un'auto a guida autonoma deve cessare di funzionare, oppure in qualunque condizione tale veicolo deve mantenere una determinata distanza rispetto al veicolo che lo precede).

f) Prescrizioni specifiche per l'identificazione biometrica remota

La raccolta e l'uso di dati biometrici[55] a fini di identificazione[56] remota, ad esempio mediante la diffusione di sistemi di riconoscimento facciale in luoghi pubblici, comporta rischi specifici per i diritti fondamentali[57]. L'uso di sistemi di IA per l'identificazione biometrica remota ha implicazioni sui diritti fondamentali che variano notevolmente a seconda dello scopo, del contesto e della portata del loro uso.

Le norme dell'UE in materia di protezione dei dati vietano in linea di principio il trattamento di dati biometrici allo scopo di identificare in modo univoco una persona fisica, salvo a determinate condizioni[58]. In particolare, ai sensi del GDPR, tale trattamento può essere effettuato solo per un numero limitato di motivi, principalmente per motivi di interesse pubblico rilevante. In tal caso, il trattamento deve essere effettuato sulla base del diritto dell'Unione o degli Stati membri, rispettare il requisito di proporzionalità e l'essenza del diritto alla protezione dei dati e prevedere appropriate misure di tutela. A norma della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, un simile trattamento deve essere strettamente necessario, autorizzato in linea di principio dal diritto dell'UE o degli Stati membri e soggetto a garanzie adeguate. Qualunque trattamento di dati biometrici finalizzato all'identificazione univoca di una persona fisica sarebbe soggetto alla Carta dei diritti fondamentali dell'Unione europea, in quanto rappresenterebbe un'eccezione a un divieto stabilito dal diritto dell'UE.

Ne consegue che, conformemente alle vigenti norme dell'UE in materia di protezione dei dati e alla Carta dei diritti fondamentali, l'IA può essere utilizzata a fini di identificazione biometrica remota unicamente ove tale uso sia debitamente giustificato, proporzionato e soggetto a garanzie adeguate.

Per affrontare eventuali preoccupazioni sociali relative all'uso dell'IA per tali fini in luoghi pubblici, e per evitare la frammentazione del mercato interno, la Commissione avvierà un ampio dibattito europeo

[55] Per dati biometrici si intendono "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 o l'autenticazione univoca, quali l'immagine facciale o i dati dattiloscopici [impronte digitali]." [Articolo 3, paragrafo 13, della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie; articolo 4, paragrafo 14, del GDPR; articolo 3, paragrafo 18, del regolamento (UE) 2018/1725].

[56] In relazione al riconoscimento facciale, per identificazione si intende il confronto tra il modello (*template*) dell'immagine del volto di una persona e i numerosi altri modelli contenuti in una banca dati al fine di stabilire una corrispondenza. D'altro canto l'autenticazione (o verifica) è spesso definita verifica uno a uno e consente il confronto tra due modelli biometrici, di solito ritenuti appartenenti alla stessa persona. Il confronto tra i due modelli biometrici permette di stabilire se la persona che figura in entrambe le immagini sia la medesima. Tale procedura è usata, ad esempio, alle porte di controllo automatizzate alla frontiera utilizzate per i controlli alle frontiere presso gli aeroporti.

[57] Ad esempio per la dignità delle persone. Analogamente, i diritti al rispetto della vita privata e alla protezione dei dati personali sono al centro delle preoccupazioni riguardanti i diritti fondamentali connesse all'uso della tecnologia di riconoscimento facciale. Vi è anche un impatto potenziale per quanto concerne la non discriminazione e i diritti dei gruppi speciali, come i bambini, gli anziani e le persone con disabilità. L'uso della tecnologia non deve inoltre compromettere i diritti alla libertà di espressione, di associazione e di riunione. Cfr. Facial recognition technology: fundamental rights considerations in the context of law enforcement (Tecnologia di riconoscimento facciale: considerazioni sui diritti fondamentali nell'ambito delle attività di polizia e giudiziarie), https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Articolo 9 del GDPR; articolo 10 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. Cfr. anche l'articolo 10 del regolamento (UE) 2018/1725 (applicabile alle istituzioni e agli organi dell'UE).

sulle circostanze specifiche che possano eventualmente giustificare tali usi, nonché sulle garanzie comuni.

E. DESTINATARI

Per quanto riguarda i destinatari delle prescrizioni giuridiche sopra descritte relative alle applicazioni di IA ad alto rischio, si devono considerare due questioni principali.

In primo luogo va affrontata la questione di come ripartire gli obblighi tra gli operatori economici coinvolti. Il ciclo di vita di un sistema di IA coinvolge numerosi operatori, tra cui lo sviluppatore, il soggetto che lo applica (il "deployer", ossia la persona che utilizza un prodotto o servizio dotato di IA) e potenzialmente altri soggetti (il produttore, il distributore o l'importatore, i prestatori di servizi, gli utenti professionali o privati).

La Commissione ritiene che in un futuro quadro normativo ciascun obbligo debba essere stabilito a carico dell'operatore o degli operatori che si trovano nella posizione migliore per affrontare eventuali rischi potenziali. Ad esempio, se da un lato gli sviluppatori dell'IA sono i più qualificati per affrontare i rischi derivanti dalla fase di sviluppo, dall'altro la loro capacità di controllare i rischi durante la fase di utilizzo può essere più limitata. In tal caso il pertinente obbligo dovrebbe essere stabilito a carico del soggetto che applica l'IA. Ciò lascia impregiudicata, ai fini della responsabilità nei confronti degli utenti finali o di altre parti che abbiano subito un danno nonché della garanzia di un accesso effettivo alla giustizia, la questione dell'individuazione del soggetto chiamato a rispondere dei danni eventualmente provocati dal sistema di IA. In base al diritto dell'UE in materia di responsabilità per danno da prodotti difettosi, tale responsabilità è attribuita al produttore, fatta salva la normativa nazionale, che può anche prevedere la possibilità di rivalersi su altri soggetti.

In secondo luogo va affrontata la questione dell'ambito di applicazione geografico dell'intervento legislativo. Secondo la Commissione, è fondamentale che le prescrizioni siano applicabili a tutti gli operatori economici interessati che forniscono prodotti o servizi basati sull'IA nell'UE, indipendentemente dal fatto che siano stabiliti o meno nell'Unione; in caso contrario, gli obiettivi dell'intervento legislativo di cui sopra potrebbero non essere pienamente raggiunti.

F. CONFORMITÀ E APPLICAZIONE DELLE NORME

Per avere un'IA affidabile, sicura e conforme alle norme e ai valori europei le prescrizioni giuridiche devono essere rispettate ed applicate efficacemente nella pratica, sia dalle autorità nazionali ed europee competenti sia dalle parti interessate. Le autorità competenti dovrebbero essere in grado di indagare sui singoli casi, ma anche di valutare l'impatto sulla società.

In considerazione dell'elevato rischio che talune applicazioni di IA presentano per i cittadini e la nostra società (cfr. la sezione A), in questa fase la Commissione ritiene che sia necessaria una valutazione preliminare e obiettiva della conformità per verificare e garantire il rispetto di talune prescrizioni obbligatorie sopra citate che disciplinano le applicazioni ad alto rischio (cfr. sezione D). La valutazione preliminare della conformità potrebbe includere procedure di prova, ispezione o certificazione[59], oltre a controlli degli algoritmi e dei set di dati utilizzati nella fase di sviluppo.

[59] Il sistema si baserebbe sulle procedure di valutazione della conformità nell'UE [cfr. la decisione n. 768/2008/CE o il regolamento (UE) 2019/881 (regolamento sulla cibersicurezza)], tenendo conto delle specificità dell'IA. Cfr. la guida blu all'attuazione della normativa UE sui prodotti, del 2014.

Le valutazioni della conformità per le applicazioni di IA ad alto rischio dovrebbero far parte dei meccanismi di valutazione della conformità già esistenti per un gran numero di prodotti immessi sul mercato interno dell'UE. Qualora non sia possibile avvalersi di tali meccanismi, potrebbe essere necessario istituire meccanismi analoghi, avvalendosi delle migliori prassi e di eventuali contributi dei portatori di interessi e delle organizzazioni europee di normazione. Tali nuovi meccanismi dovrebbero essere proporzionati e non discriminatori e utilizzare criteri trasparenti e obiettivi in conformità agli obblighi internazionali.

In fase di progettazione e realizzazione di un sistema sulla base di valutazioni preliminari della conformità, occorre considerare in particolare:

- che non tutti i requisiti sopra indicati possono essere verificati mediante una valutazione preliminare della conformità. Ad esempio, in generale l'adempimento dell'obbligo di fornire informazioni non si presta facilmente ad essere verificato mediante una simile valutazione;

- la possibilità che taluni sistemi di IA si evolvano e apprendano dall'esperienza: tale possibilità può rendere necessarie valutazioni ripetute per tutta la durata dei sistemi di IA in questione;

- la necessità di verificare i dati utilizzati per l'addestramento nonché le pertinenti metodologie, procedure e tecniche di programmazione e di addestramento utilizzate per costruire, sottoporre a prova e convalidare i sistemi di IA;

- che, qualora dalla valutazione della conformità emerga che un sistema di IA non rispetta alcune prescrizioni, ad esempio quelle relative ai dati utilizzati per l'addestramento, sarà necessario porre rimedio alle carenze individuate, ad esempio addestrando nuovamente il sistema nell'UE in modo tale da garantire il rispetto di tutte le prescrizioni applicabili.

Le valutazioni della conformità sarebbero obbligatorie per tutti gli operatori economici destinatari delle prescrizioni, indipendentemente dal loro luogo di stabilimento[60]. Al fine di limitare l'onere a carico delle PMI, potrebbero essere previste strutture di sostegno, anche attraverso i poli dell'innovazione digitale. Norme e strumenti online dedicati potrebbero inoltre agevolare il rispetto degli obblighi.

Lo svolgimento di valutazioni preliminari della conformità non pregiudica il controllo della conformità e l'applicazione ex post della legge da parte delle autorità nazionali competenti. Ciò vale per le applicazioni di IA ad alto rischio, ma anche per altre applicazioni di IA soggette a prescrizioni giuridiche, pur se le autorità nazionali competenti potrebbero prestare particolare attenzione alle prime, dato l'alto rischio che le contraddistingue. Un'adeguata documentazione delle pertinenti applicazioni di IA dovrebbe consentire i controlli ex post (cfr. la sezione E) e, ove opportuno, la possibilità che tali applicazioni siano sottoposte a prova da terzi, ad esempio dalle autorità competenti. Ciò può essere particolarmente importante quando sorgono rischi per i diritti fondamentali che dipendono dal contesto. Tale controllo della conformità dovrebbe essere inquadrato in un sistema di vigilanza continua del mercato. Gli aspetti relativi alla governance sono ulteriormente discussi nella sezione H.

È inoltre opportuno garantire, sia per le applicazioni di IA ad alto rischio sia per il resto delle applicazioni, un ricorso giurisdizionale effettivo per chiunque sia stato danneggiato dai sistemi di IA.

[60] Per quanto concerne la pertinente struttura di governance, compresi gli organismi incaricati di svolgere le valutazioni della conformità, cfr. la sezione H.

Le questioni relative alla responsabilità sono ulteriormente discusse nella relazione sul quadro di riferimento per la sicurezza e la responsabilità che accompagna il presente libro bianco.

G. ETICHETTATURA SU BASE VOLONTARIA PER LE APPLICAZIONI DI IA NON AD ALTO RISCHIO

Per le applicazioni di IA che non sono considerate "ad alto rischio" (cfr. sezione C) e che pertanto non sono soggette alle prescrizioni obbligatorie di cui sopra (cfr. le sezioni D, E e F), oltre alla legislazione applicabile vi sarebbe la possibilità di istituire un sistema di etichettatura su base volontaria.

Nel quadro di tale sistema, gli operatori economici interessati non soggetti alle prescrizioni obbligatorie potrebbero decidere, su base volontaria, di conformarsi a tali prescrizioni o di impegnarsi al rispetto di una serie specifica di prescrizioni analoghe, stabilite appositamente ai fini del sistema volontario. Agli operatori economici interessati sarebbe allora assegnato un marchio di qualità per le loro applicazioni di IA.

Il marchio volontario consentirebbe agli operatori economici interessati di mettere in evidenza l'affidabilità dei loro prodotti e servizi basati sull'IA, e consentirebbe agli utenti di riconoscere facilmente che i prodotti e i servizi in questione sono conformi a determinati parametri di riferimento obiettivi e standardizzati a livello dell'UE, che vanno oltre gli obblighi giuridici normalmente applicabili. Ciò contribuirebbe a rafforzare la fiducia degli utenti nei sistemi di IA e a promuovere l'adozione generale della tecnologia.

Tale opzione richiederebbe la creazione di un nuovo strumento giuridico che definisca il quadro relativo a un sistema di etichettatura su base volontaria per gli sviluppatori e/o i soggetti che applicano i sistemi di IA non considerati ad alto rischio. Sebbene la partecipazione al sistema di etichettatura sia facoltativo, una volta che gli sviluppatori o i soggetti che applicano l'IA hanno deciso di aderirvi le relative prescrizioni sarebbero vincolanti. La combinazione di attività di applicazione della legge ex ante ed ex post dovrebbe garantire il rispetto di tutte le prescrizioni.

H. GOVERNANCE

Occorre una struttura di governance europea in materia di IA, sotto forma di un quadro di cooperazione delle autorità nazionali competenti, per evitare la frammentazione delle responsabilità, aumentare la capacità degli Stati membri e garantire che l'Europa si doti progressivamente delle capacità necessarie per sottoporre a prova e certificare prodotti e servizi basati sull'IA. In tale contesto sarebbe utile sostenere le autorità nazionali competenti affinché possano adempiere il loro mandato nei casi di utilizzo dell'IA.

Una struttura di governance europea potrebbe essere investita di varie funzioni, tra cui permettere uno scambio regolare di informazioni e migliori prassi, individuare le tendenze emergenti e fornire consulenza sulle attività di normazione e sulla certificazione. Dovrebbe inoltre svolgere un ruolo essenziale nell'agevolare l'attuazione del quadro giuridico, ad esempio fornendo orientamenti, pareri e consulenze. A tal fine dovrebbe basarsi su una rete di autorità nazionali, nonché su reti settoriali e autorità di regolamentazione a livello nazionale e dell'UE. Un comitato di esperti potrebbe inoltre fornire assistenza alla Commissione.

La struttura di governance dovrebbe garantire la massima partecipazione dei portatori di interessi, fra cui organizzazioni dei consumatori e parti sociali, imprese, ricercatori e organizzazioni della società civile, che dovrebbero essere consultati in merito all'attuazione e all'ulteriore sviluppo del quadro di riferimento.

Considerando che vi sono strutture già esistenti, ad esempio nei settori finanziario, farmaceutico, dell'aviazione, dei dispositivi medici, della tutela dei consumatori o della protezione dei dati, la struttura di governance proposta non dovrebbe duplicare le funzioni esistenti, bensì stabilire stretti legami con altre autorità competenti a livello nazionale e dell'UE nei vari settori, al fine di integrare le competenze esistenti e aiutare le autorità nel monitoraggio e nella sorveglianza delle attività svolte dagli operatori economici in cui intervengono sistemi di IA nonché prodotti e servizi basati sull'IA.

Infine, qualora venga scelta questa opzione, lo svolgimento delle valutazioni della conformità potrebbe essere affidato agli organismi notificati designati dagli Stati membri. I centri di prova dovrebbero rendere possibili verifiche e valutazioni indipendenti dei sistemi di IA in conformità alle prescrizioni sopra descritte. Le valutazioni indipendenti rafforzeranno la fiducia, garantiranno l'obiettività e potrebbero anche facilitare il lavoro delle autorità competenti.

L'UE dispone di centri di prova e di valutazione eccellenti e dovrebbe sviluppare le proprie capacità anche nel settore dell'IA. Gli operatori economici stabiliti in paesi terzi che intendono entrare nel mercato interno possono ricorrere a organismi designati stabiliti nell'UE o, in forza di accordi di riconoscimento reciproco con paesi terzi, ricorrere a organismi di paesi terzi designati per effettuare tale valutazione.

La struttura di governance relativa all'IA e le possibili valutazioni della conformità qui discusse non inciderebbero sulle responsabilità e sui poteri riconosciuti dal diritto dell'UE in vigore alle autorità competenti in determinati settori o per questioni specifiche (ad esempio nei settori finanziario, farmaceutico, dell'aviazione, dei dispositivi medici, della tutela dei consumatori, della protezione dei dati, ecc.).

6. CONCLUSIONI

L'IA è una tecnologia strategica che offre molti benefici ai cittadini, alle imprese e alla società nel suo insieme, a condizione che segua un approccio antropocentrico, etico, sostenibile e rispettoso dei valori e dei diritti fondamentali. L'IA offre importanti vantaggi in termini di efficienza e produttività, che possono rafforzare la competitività dell'industria europea e migliorare il benessere dei cittadini. Può inoltre contribuire a individuare soluzioni ad alcune delle sfide sociali più urgenti, tra cui la lotta ai cambiamenti climatici e al degrado ambientale, le sfide legate alla sostenibilità e ai cambiamenti demografici, la protezione delle nostre democrazie e, ove tale uso sia necessario e proporzionato, la lotta alla criminalità.

Se vuole cogliere appieno le opportunità offerte dall'IA, l'Europa deve sviluppare e rafforzare le capacità industriali e tecnologiche necessarie. Come indicato nella strategia europea per i dati, che accompagna il presente libro bianco, ciò richiede anche misure che consentano all'UE di diventare un hub di dati globale.

L'approccio europeo all'IA mira a promuovere la capacità di innovazione dell'Europa nel settore dell'IA, sostenendo nel contempo lo sviluppo e la diffusione di un'IA etica e affidabile in tutta l'economia dell'UE. L'IA dovrebbe apportare vantaggi alle persone ed essere un fattore positivo per la società.

Con il presente libro bianco, accompagnato dalla relazione sul quadro di riferimento per la sicurezza e la responsabilità, la Commissione avvia un'ampia consultazione della società civile, dell'industria e del mondo accademico negli Stati membri in merito a proposte concrete per un approccio europeo all'IA. Tali misure comprendono sia strumenti strategici per promuovere gli investimenti nella ricerca e nell'innovazione, favorire lo sviluppo delle competenze e sostenere l'adozione dell'IA da parte delle PMI, sia proposte relative a elementi essenziali di un futuro quadro normativo. Questa consultazione

consentirà un dialogo globale con tutti i portatori di interessi, che informerà le prossime fasi del lavoro della Commissione.

La Commissione invita a formulare osservazioni sulle proposte presentate nel libro bianco mediante una consultazione pubblica aperta consultabile all'indirizzo: https://ec.europa.eu/info/consultations_en. Sarà possibile formulare osservazioni nel quadro della consultazione fino al 19 maggio 2020.

È prassi abituale della Commissione pubblicare le osservazioni pervenute in risposta a una consultazione pubblica. È tuttavia possibile chiedere che tali osservazioni rimangano in tutto o in parte riservate. In tal caso si prega di indicare tale richiesta sulla prima pagina della risposta e trasmettere alla Commissione anche una versione non riservata della risposta, che sarà pubblicata.

DELIBERAZIONE DELLA GIUNTA REGIONALE 30 ottobre 2023, n. 1488
Istituzione del Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione.

Il Presidente della Giunta Regionale, sulla base delle risultanze dell'istruttoria espletata da Ile Responsabili E.Q. e dal Responsabile per la Transizione al Digitale, riferisce quanto segue.

Visti:
- Il D. Lgs. 7 marzo 2005, n. 82 *"Codice dell'amministrazione digitale";*
- il Regolamento (UE) 2016/679 relativo alla *"protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", che abroga la Direttiva 95/46/CE (Reg. generale sulla protezione dei dati) e il D. Lgs. n. 196/2003 ("Codice Privacy");*
- la Legge 7 agosto 1990, n. 241 e ss.mm.ii. *"Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";*
- la D.G.R. 7 dicembre 2020, n. 1974, con la quale la Giunta regionale ha adottato la Macrostruttura del Modello organizzativo denominato **"**MAIA 2.0", quale atto di alta organizzazione che disciplina l'organizzazione amministrativa della Presidenza e della Giunta Regionale;
- il D.P.G.R. 22 gennaio 2021, n. 22, pubblicato sul BURP n. 15 del 28.01.2021, che ha emanato l'atto di alta organizzazione relativo alle strutture della Presidenza e della Giunta Regionale *"Adozione Atto di Alta Organizzazione - Modello organizzativo MAIA 2.0"* e successivamente modificato e integrato con i decreti del Presidente della Giunta Regionale del 10 febbraio 2021, n. 45 e del 15 settembre 2022, n. 380;
- la D.G.R. 10.05.2021, n. 773 con cui la Giunta Regionale ha individuato il ruolo di Responsabile per la Transizione Digitale (RTD), previsto dall'art. 17 del D. Lgs. 7 marzo 2005, n. 82, in capo al responsabile del Servizio Tecnico e Transizione Digitale della Direzione Amministrativa del Gabinetto, evidenziando la necessità di garantire l'unitarietà di azione strategica nello svolgimento dei compiti previsti dall'art. 17, comma 1, del D. Lgs. n. 82/2005 e s.m.i., nonché quelli previsti dalla Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione;
- la D.G.R. 22.07.2021, n. 1219 avente ad oggetto *"Riorganizzazione digitale dell'amministrazione regionale - Linee di indirizzo";*
- la D.G.R. 30.06.2022, n. 791 con cui la Giunta Regionale ha adottato il *"Piano triennale di Riorganizzazione Digitale della Regione Puglia 2022-2024";*
- la D.G.R. 31.07.2023, n. 1093 con cui la Giunta regionale ha approvato il *"Piano triennale di Riorganizzazione Digitale 2022-2024 -Aggiornamento 2023-2025";*

Viste altresì:
- la D.G.R. 15 settembre 2021, n. 1466, che reca l'approvazione della Strategia regionale per la parità di genere, denominata *"Agenda di Genere";*
- la D.G.R. 3 luglio 2023, n. 938 recante "D.G.R. n. 302/2022 *"Valutazione di impatto di genere. Sistema di gestione e di monitoraggio". Revisione degli allegati";*

Premesso che:
- la crescente disponibilità di computer sempre più potenti e performanti, dotati di una enorme potenza di calcolo, ha accelerato, negli ultimi decenni, gli sviluppi della automazione, migliorando la competitività in tutti i contesti [imprese, università, pubbliche amministrazioni, etc...] ed avviando un profondo percorso di trasformazione tecnologica, con ricadute positive sull'aumento della produttività e la riduzione dei divari;
- allo scenario così delineato, si aggiunge il grande interesse sollevato, negli anni più recenti, dallo sviluppi di sistemi basati sull'Intelligenza artificiale [artificial Intelligence, A.I., sistemi capaci di interagire con l'ambiente, apprendere, pianificare azioni con un certo grado di autonomia, per raggiungere specifici obiettivi], il cui potere di calcolo è sostenuto dalla contestuale disponibilità di enormi quantità di dati [data

economy, data space, etc...] e dallo sviluppo di nuovi algoritmi;

- tale sviluppo ha permeato tutti gli ambiti dell'azione umana, automatizzando alcuni processi standard e portando a ripensare e riorganizzare anche le attività e le metodologie di lavoro, comprese quelle specifiche della Pubblica Amministrazione, allo scopo di individuare soluzioni che possano sostenere la costante ricerca di efficienza ed efficacia dell'agire pubblico e, al contempo, semplificare i servizi resi al cittadino, con garanzia di trasparenza, celerità, economicità, inclusività;
- l'avvento massiccio di tali nuovi strumenti, compresa l'intelligenza artificiale generativa [una intelligenza artificiale che utilizza algoritmi per "generare" nuovi contenuti], ha suscitato notevole entusiasmo, da un lato, ma anche preoccupazioni e diffidenze, dall'altro, a causa dei timori di "de umanizzazione" dei processi e di supposte perdite di forza lavoro, posizioni di mercato, etc..., collegati anche alla scarsa conoscenza del fenomeno;
- nel 2018, con la comunicazione COM(2018)237 final del 25.04.2028 *"Intelligenza artificiale per l'Europa",* la Commissione europea ha introdotto la strategia europea sull'intelligenza artificiale, evidenziando la necessità di *"un approccio coordinato per sfruttare al massimo le opportunità offerte dall'IA e per affrontare le nuove sfide che comporta",* e sottolineando come i *"grandi volumi di dati dei settori industriale, della ricerca e pubblico"* possano fungere da abilitatori dell'alimentazione di tali sistemi, rendendo *"la condivisione dei dati più agevole"* e *"disponibili per il riutilizzo volumi maggiori di dati"* [servizi pubblici, ambiente, dati sanitari e della ricerca in primis]; tra i principi evidenziati, la necessità che le nuove tecnologie si basino sui valori, tappa fondamentale per costruire fiducia, con un approccio sostenibile alle tecnologie;
- nella predetta Comunicazione, la Commissione mostra anche di comprendere come alcune applicazioni dell'intelligenza artificiale possano *"far sorgere nuovi interrogativi etici e giuridici, che riguardano per esempio la responsabilità o processi decisionali potenzialmente inficiati da condizionamenti",* evidenziando la necessità di un quadro etico e normativo adeguato, che promuova l'innovazione e rispetti i valori dell'Unione e i diritti fondamentali;
- nella successiva Comunicazione COM(2018)795 final del 07.12.2018 *"Piano coordinato sull'intelligenza artificiale",* basata sulla Dichiarazione di cooperazione sull'intelligenza artificiale dell'aprile 2018, sono state individuate, tra gli Stati membri, una serie di azioni comuni per aumentare gli investimenti, condividere i dati, promuovere il talento e rafforzare la fiducia, dando priorità a settori di interesse pubblico, quali l'assistenza sanitaria, i trasporti e la mobilità, la sicurezza e l'energia;
- con Comunicazione COM(2019)168 final dell'08.04.2019 *"Creare fiducia nell'intelligenza artificiale antropocentrica",* la Commissione Europea ha ribadito la centralità dei *"valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani"* nell'attività delle istituzioni dell'Unione, anche riguardo all'intelligenza artificiale;
- con la Comunicazione COM(2020)65 fin al del 19.02.2020, Libro Bianco *"sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia",* con specifico riferimento al settore pubblico si sottolinea la necessità *"che le amministrazioni pubbliche, gli ospedali, i servizi di pubblica utilità e di trasporto, le autorità di vigilanza finanziaria e altri settori di interesse pubblico inizino rapidamente a utilizzare nelle loro attività prodotti e servizi che si basano sull'IA* ", evidenziando, altresì, l'attenzione particolare rivolta ai settori dell'assistenza sanitaria e dei trasporti, *"in cui la tecnologia è abbastanza matura da consentire una diffusione su vasta scala";* a tale indicazione è collegata l'azione 6, che prevede l'avvio di dialoghi settoriali aperti e trasparenti per presentare un piano d'azione che faciliti lo sviluppo, la sperimentazione e l'adozione dell'intelligenza artificiale, per elaborare uno specifico *"Programma di adozione dell'IA"* nel settore degli appalti pubblici;
- con la Comunicazione COM(2021)206 final del 21.04.2021, il Parlamento Europeo e il Consiglio hanno proposto un regolamento *"che stabilisce regole armonizzate sull'intelligenza artificiale",* conosciuto come Al Act - attualmente in attesa di approvazione definitiva dopo il trilogo - nel quale le applicazioni di intelligenza aritificiale vengono classificate in base al livello di rischio che rappresentano per gli utenti, e che comprende, dopo le ultime integrazioni, anche l'intelligenza artificiale cosiddetta "generativa";
- il 14 giugno 2023 è stato pubblicato sulla GUUE il Regolamento (UE) 2023/1230 *"relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio";*

Premesso altresì che:

– anche l'Italia, in linea con l'interesse dell'UE al tema, con il Programma Strategico "Intelligenza Artificiale" e la costituzione di un gruppo di lavoro permanente ha avviato azioni sull'intelligenza artificiale: in particolare, è stato evidenziato l'obiettivo degli interventi sulla Pubblica Amministrazione, volti alla creazione di infrastrutture dati sicure per l'utilizzo dei big data pubblici, alla semplificazione e personalizzazione dell'offerta dei servizi pubblici e all'innovazione delle amministrazioni;

– ulteriori previsioni sono inserite nei documenti strategici di programmazione, tra i quali il Piano Nazionale di Ripresa e Resilienza [sistemi integrati con intelligenza artificiale sono, per esempio espressamente previsti per il reclutamento; per l'analisi e la verifica dell'impatto della regolazione; per l'osservazione e l'analisi delle tendenze nell'uso degli strumenti di acquisto; per l'hub del turismo] e il P.R. 2021-2027 dell'Amministrazione regionale [con riferimento alla digitalizzazione dei soggetti pubblici, alla formazione, alla trasformazione digitale delle imprese, ai dati aperti];

Considerato che:

– le riflessioni sul tema si soffermano sulla dicotomia tra opportunità e rischi, evidenziando la necessità di un unico sistema normativo e regolamentare che garantisca l'utilizzo sicuro, responsabile e trasparente di tale tecnologia, scevra da pregiudizi e rispettosa dei diritti di tutti, nonchè della opportuna comprensione di tali dinamiche e di una adeguata formazione, che consenta di conquistare e mantenere la fiducia dei cittadini;

Considerato, altresì, che:

– l'Amministrazione regionale è da sempre vicina ai temi dell'intelligenza artificiale, nelle sue diverse forme, con l'obiettivo ultimo di sviluppare soluzioni utili alla semplificazione dell'attività amministrativa, con impatto diretto sulla vita dei propri cittadini;

– in tale ambito, l'Amministrazione regionale ha organizzato anche alcune iniziative pubbliche specifiche sull'Intelligenza Artificiale, servite da stimolo al confronto sul tema, soprattutto con riferimento agli aspetti di evoluzione dei servizi pubblici e di miglioramento del rapporto tra Pubblica Amministrazione e cittadini, fondato su un utilizzo sicuro, trasparente, tracciabile e non discriminatorio di tali "nuovi" servizi;

Rilevato che:

– lo sviluppo di servizi pubblici di tale tipologia permette non solo di accrescere il livello di soddisfazione dei cittadini, ma, soprattutto, la fiducia che gli stessi hanno nelle istituzioni, e che, come richiamato da atti e documenti delle istituzioni europee, è alla base dello sviluppo dell'Unione;

– per far ciò, i sistemi basati sull'intelligenza artificiale devono integrarsi con le attività svolte dal personale pubblico nel quotidiano, rendendo sempre più sostenibili i processi che ne sono alla base, senza sostituire integralmente i compiti loro assegnati;

– in tale scenario, le Pubbliche Amministrazioni hanno il compito di guidare e coordinare lo sviluppo di tali soluzioni, perseguendo i fini dell'azione pubblica e garantendo il rispetto di principi e diritti;

Ritenuto che:

– il processo di guida e coordinamento di cui al precedente alinea all'interno della Pubblica Amministrazione, con ricadute a beneficio dell'intero territorio regionale, richiede una riflessione congiunta sugli aspetti nevralgici ad oggi emersi, che parta da una valutazione preliminare dei principali punti di attenzione e di possibili strumenti e soluzioni individuati;

– a tale riflessione, si aggiunge la necessità di sperimentare tali eventuali strumenti e soluzioni, anche tramite confronto allargato tra le regioni, coinvolgendo le Università e i Centri di Ricerca sul territorio, e la stessa Agenzia per l'Italia Digitale [eventualmente, anche per il tramite del neonato Noto Territoriale di Competenza sul Riuso e Open Source - OR 26 del POR 2022-2024 e aggiornamento 2023-2025];

Tutto ciò visto, premesso, considerato, rilevato e ritenuto:

– la Regione Puglia, attraverso il Gabinetto di Presidenza, Ufficio per la Transizione al Digitale, propone

di costituire un *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione",* Allegato A) al presente atto e parte integrante dello stesso, il cui scopo è quello di:

1. indagare, analizzare, comprendere, monitorare e valutare tutte le implicazioni [etiche, normative, infrastrutturali, economiche] e la sostenibilità di applicazioni, sistemi, strumenti e soluzioni di intelligenza artificiale nella Pubblica Amministrazione regionale, promuovendo la redazione di linee di indirizzo, l'attività di ricerca, formazione e studio specifiche, anche tramite costituzione di tavoli di lavoro monotematici, sotto il coordinamento del RTD regionale;
2. sperimentare l'utilizzo di applicazioni, sistemi, strumenti e soluzioni di intelligenza artificiale in ambito regionale, all'interno di processi e sistemi dell'Ente, coinvolgendo, allo scopo, anche la Rete degli RTD delle Agenzie e delle in house regionali;

Garanzie di riservatezza

La pubblicazione sul BURP, nonché la pubblicazione all'Albo o sul sito istituzionale, salve le garanzie previste dalla legge 241/1990 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 679/2016 in materia di protezione dei dati personali, nonché dal D.Lgs. 196/2003 ss.mm.ii .. Ai fini della pubblicità legale, il presente provvedimento è stato redatto in modo da evitare la diffusione di dati personali identificativi non necessari ovvero il riferimento alle particolari categorie di dati previste dagli articoli 9 e 10 del succitato Regolamento UE.

Valutazione di impatto di genere
Ai sensi della D.G.R. n. 398 del 03/07/2023 la presente deliberazione è stata sottoposta a Valutazione di impatto di genere. *L'impatto di genere stimato risulta:* ❏ *diretto* ❏ *indiretto* x *neutro* ❏ *non rilevato*

Copertura Finanziaria ai sensi del D.Lgs. 118/2011 e ss.mm.ii.

La presente deliberazione non comporta implicazioni, dirette e/o indirette, di natura economico finanziaria e/o patrimoniale e dalla stessa non deriva alcun onere a carico del bilancio regionale.

Il Presidente relatore, ai sensi dell'art. 4, comma 4, lett. a) della L.R. n. 7/1997, propone alla Giunta di:

1. condividere quanto esposto in narrativa che qui si intende integralmente riportato;
2. approvare l'Allegato A *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione",* parte integrante del presente atto;
3. demandare al RTD regionale la costituzione del suddetto *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione";*
4. delegare espressamente il RTD regionale alla sottoscrizione degli accordi con altre Pubbliche Amministrazioni, nonchè degli ulteriori atti necessari per la costituzione del *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione";*
5. dare mandato all'Ufficio per la Transizione al Digitale di provvedere agli adempimenti di competenza;
6. dare mandato all'Ufficio per la Transizione al Digitale di notificare il presente provvedimento a tutte le strutture regionali, a lnnovaPuglia S.p.A, al Consiglio Regionale della Regione Puglia;
7. disporre la pubblicazione del presente provvedimento sul Bollettino Ufficiale della Regione Puglia.

I SOTTOSCRITTI ATTESTANO CHE IL PROCEDIMENTO ISTRUTTORIO LORO AFFIDATO E' STATO ESPLETATO NEL RISPETTO DELLA VIGENTE NORMATIVA REGIONALE, NAZIONALE E COMUNITARIA E CHE IL PRESENTE SCHEMA DI PROVVEDIMENTO, DAGLI STESSI PREDISPOSTO Al FINI DELL'ADOZIONEDELL'ATTO FINALE DA PARTE DELLA GIUNTA REGIONALE, E' CONFORME ALLE RISULTANZE ISTRUTTORIE.

Responsabile E.Q. " Supporto amministrativo-contabile
al Responsabile Transizione Digitale e Affari generali"
Ing. Federica Carrozzo

Responsabile E.Q. "Supporto giuridico specialistico
per la transizione alla modalità digitale"
Avv. M. Morena Rogane

Responsabile per la Transizione Digitale
Ing. Cosimo Elefante

Il Sottoscritto Capo di Gabinetto **NON** ravvisa la necessità di esprimere sulla proposta di delibera osservazioni ai sensi del DPGR n. 22/2021.

Il Capo di Gabinetto
Prof. Giuseppe Pasquale Roberto Catalano

Il proponente
Il Presidente
Dott. Michele Emiliano

LA GIUNTA

- udita la relazione e la conseguente proposta del Presidente;
- vista le sottoscrizioni poste in calce alla proposta di deliberazione;
- a voti unanimi espressi nei modi di legge;

DELIBERA

1. condividere quanto esposto in narrativa che qui si intende integralmente riportato;
2. approvare l'Allegato A *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione",* parte integrante del presente atto;
3. demandare al RTD regionale la costituzione del suddetto *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione";*
4. delegare espressamente il RTD regionale alla sottoscrizione degli accordi con altre Pubbliche Amministrazioni, nonchè degli ulteriori atti necessari per la costituzione del *"Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione";*
5. dare mandato all'Ufficio per la Transizione al Digitale di provvedere agli adempimenti di competenza;
6. dare mandato all'Ufficio per la Transizione al Digitale di notificare il presente provvedimento a tutte le strutture regionali, a InnovaPuglia S.p.A, al Consiglio Regionale della Regione Puglia;
7. disporre la pubblicazione del presente provvedimento sul Bollettino Ufficiale della Regione Puglia.

IL SEGRETARIO DELLA GIUNTA
ANNA LOBOSCO

IL PRESIDENTE DELLA GIUNTA
MICHELE EMILIANO

REGIONE PUGLIA Cosimo Elefante 27.10.2023 17:53:38 GMT+01:00

REGIONE PUGLIA

Allegato A

Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione

ART .1
(Istituzione)

1.1 Presso la Presidenza della Giunta Regionale, Gabinetto del Presidente, Ufficio per la Transizione al Digitale è istituito il "Centro di Competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione" (in seguito, Centro o CdC).

ART. 2
(Obiettivi e Caratteristiche)

2.1 Il Centro ha lo scopo di indagare, analizzare, comprendere, monitorare e valutare tutte le implicazioni [etiche, normative, infrastrutturali, economiche, etc…] e la sostenibilità di applicazioni, sistemi, strumenti e soluzioni di intelligenza artificiale nella Pubblica Amministrazione regionale;

2.2 Il Centro promuove la redazione di linee di indirizzo, l'attività di ricerca, formazione e studio specifiche, anche tramite costituzione di tavoli di lavoro;

2.3 Il Centro sperimenta l'utilizzo di applicazioni, sistemi, strumenti e soluzioni di intelligenza artificiale in ambito regionale, all'interno di processi e sistemi dell'Ente coinvolgendo, allo scopo, anche la Rete degli RTD delle agenzie e delle in-house regionali;

2.4 Il Centro relaziona, con cadenza semestrale alla Giunta Regionale e con cadenza trimestrale alla Conferenza dei Direttori, sulle attività effettuate durante l'anno e su quelle da avviare.

ART. 3
(Struttura del Centro di Competenza)

3.1 Il Centro è coordinato dal Responsabile della Transizione Digitale regionale, che ne presiede le riunioni, ed è composto da un Comitato Tecnico. Le funzioni di segreteria tecnica sono svolte dall'Ufficio del Responsabile per la Transizione al Digitale.

ART. 4
(Composizione)

4.1 Sono componenti di diritto del Comitato Tecnico:

- il Responsabile per la Transizione al Digitale di Regione Puglia;
- il Responsabile per la Transizione al Digitale di InnovaPuglia S.p.A;
- il Responsabile per la Transizione al Digitale del Consiglio Regionale pugliese;
- il Consigliere del Presidente per l'informatizzazione, l'e-government ed il social government;
- un componente dell'Ufficio RTD.

4.2 Nel rispetto dei principi di leale collaborazione tra amministrazioni pubbliche e, previe specifiche intese e accordi, possono far parte del Comitato tecnico:

- un rappresentante dell'Agenzia per l'Italia Digitale;
- un rappresentante di ciascuna delle Università pugliesi.

I rappresentanti degli enti sopra indicati, ciascuno dei quali designato e autorizzato ad assumere l'incarico dall'ente di appartenenza, assumono il ruolo di componenti del Comitato tecnico.

4.3. Il Comitato Tecnico, nell'esercizio della propria discrezionalità tecnica, può decidere di integrare la propria composizione con ulteriori membri esperti, anche appartenenti a Enti e Centri di ricerca, da individuare con criteri di selezione definiti in appositi avvisi pubblici.

4.4. Il Comitato Tecnico, nell'esercizio delle proprie funzioni, si avvale, inoltre, del supporto delle Rete degli RTD delle Agenzie e delle in house regionali di cui alla D.G.R. 2 agosto 2022, n. 1092.

4.5. La partecipazione al Comitato Tecnico è svolta a titolo gratuito.

ART. 5
(Attività)

5.1 Il Centro svolge le seguenti, principali, attività:

- studio sullo sviluppo delle tecnologie di intelligenza artificiale nel settore della Pubblica Amministrazione;
- monitoraggio delle soluzioni applicative di intelligenza artificiale da adottare, o eventualmente già adottate, all'interno dell'Amministrazione Regionale;
- individuazione e selezione, nel rispetto dei principi del D. Lgs. n. 36/2023, del D. Lgs. n.82/2005 e della L.R. n. 20/2012, di tecnologie e strumenti basati sull'intelligenza artificiale da implementare in bandi e avvisi per migliorare la performance dei sistemi regionali;
- comunicazione e divulgazione, alle strutture regionali e alle altre amministrazioni del territorio, su tutti gli aspetti dell'utilizzo delle tecnologie di intelligenza artificiale;
- adozione di linee di indirizzo per l'utilizzo di soluzioni tecnologiche di intelligenza artificiale in ambito regionale;
- formazione orientata ai dipendenti e alle altre Pubbliche Amministrazioni del territorio per l'utilizzo delle soluzioni tecnologiche di intelligenza artificiale.

ART. 6
(Relazioni con altre strutture regionali)

6.1 Il Centro ha autonomia operativa.
6.2 Per il raggiungimento dei propri obiettivi e delle specifiche linee di azione definite dal Comitato Tecnico, il Centro collabora con le altre strutture regionali che svolgono attività riconducibili a quanto previsto nel precedente art. 5.

ART. 7
(Disposizioni finali)

7.1 Il Centro potrà:

- dotarsi di un regolamento interno di organizzazione;
- avviare collaborazioni, formali e/o informali, con altri Enti, Organizzazioni, Università ed Enti di Ricerca sui temi rientranti nel proprio ambito di competenza;
- organizzare specifici tavoli tematici sui singoli aspetti dell'intelligenza artificiale.

7.2 La partecipazione al Comitato tecnico si considera svolta *ratione officii* e non da diritto alla corresponsione di qualsivoglia compenso, rimborso e/o indennità.

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

AGID Agenzia per l'Italia Digitale

STRATEGIA ITALIANA PER L'INTELLIGENZA ARTIFICIALE 2024-2026

SOMMARIO

PREMESSA	4
ANALISI DEL CONTESTO	6
PRINCIPI DELLA STRATEGIA	8
ARCHITETTURA DELLA STRATEGIA	13
STRATEGIA PER LA RICERCA	17
STRATEGIA PER LA PUBBLICA AMMINISTRAZIONE	21
STRATEGIA PER LE IMPRESE	25
STRATEGIA PER LA FORMAZIONE	29
MONITORAGGIO DELLA STRATEGIA	35
ORGANI REGOLATORI	37

PREMESSA

Le tecnologie basate sull'Intelligenza Artificiale (IA) hanno ampiamente rivelato, ormai già da alcuni anni a questa parte, il proprio impatto pervasivo e il proprio potenziale trasformativo delle dinamiche sociali e produttive. L'Intelligenza Artificiale sta rivoluzionando il mondo in cui viviamo e le modalità con cui produciamo valore in tutti i settori, sta impattando profondamente sul sistema dell'educazione, sulle attività professionali e sull'industria. Le radici di questa rivoluzione risalgono alla metà del secolo scorso, ma l'avvento del machine learning nei primi anni 2000 e, più recentemente, delle tecniche di deep learning ha segnato una vera svolta, centrata sulla loro capacità di estrarre valore e conoscenza dall'analisi di enormi moli di dati.

L'arrivo dei sistemi generativi ha poi, nell'ultimo anno, reso ancor più evidente la forza innovatrice e trasformativa dell'IA, abilitando lo sviluppo di processi di automazione contraddistinti da una facilità d'uso senza eguali. Spinta da grandi investimenti internazionali che non trovano precedenti nella storia dell'informatica, questa rivoluzione ha rapidamente travalicato il mondo accademico e dei centri di ricerca, assumendo la connotazione di un vero e proprio fenomeno sociale. Il lancio di ChatGPT, prodotto da OpenAI, ha contribuito in modo significativo a creare una consapevolezza diffusa, mai registrata prima, circa le potenzialità di un paradigma digitale capace di creare, in un futuro ormai imminente, un nuovo modello di supporto alle attività degli individui in una molteplicità di aree, contenuti e applicazioni. Il tutto all'interno di una cornice cognitiva che naturalmente alimenta dibattito e riflessione, in relazione ai limiti e ai rischi connessi all'utilizzo di tali piattaforme.

Nella sua forte e radicata tradizione industriale, l'Italia ha saputo sempre ben interpretare le opportunità offerte dalle nuove tecnologie, caratterizzandosi come una avanguardia nello sviluppo e nell'adozione di soluzioni per l'automazione di prodotti e processi. Il tessuto produttivo italiano si articola in ecosistema del tutto peculiare, animato da un nucleo rilevante di grandi imprese e da una diffusa rete di piccole e medie imprese, la cui vocazione manifatturiera ne rappresenta probabilmente il tratto maggiormente distintivo. La capacità di innovazione di questa filiera ha accompagnato, dal dopoguerra a oggi, lo sviluppo economico e sociale del nostro Paese, dall'adozione dei primi grandi macchinari industriali e dalla definizione delle prime linee di produzione automatizzata, fino all'era della robotica e delle soluzioni digitali che hanno abilitato il paradigma dell'Industria 4.0. La rivoluzione dell'Intelligenza Artificiale si innesta all'interno di questo terreno fertile e recettivo, che sa affondare le radici nella tradizione rivisitandola con slancio creativo e spinta all'innovazione. Non sorprende, pertanto, che l'Italia abbia iniziato ad affrontare le importanti sfide poste dall'Intelligenza Artificiale già nel 2018, definendo (a cura dell'Agenzia per l'Italia Digitale) un'analisi sull'impatto delle tecnologie di IA nella società e, in particolare, sulla Pubblica Amministrazione. Nel 2020, il Ministero per lo Sviluppo Economico ha poi prodotto un documento di "Proposte per una Strategia italiana per l'intelligenza artificiale", redatto con l'obiettivo di definire una strategia focalizzata sul sostegno alla produttività del Paese, in linea con gli obiettivi di sviluppo sostenibile indicati dall'Agenda 2030 delle Nazioni Unite. Tali indicazioni strategiche sono, infine, confluite nel 2021 all'interno del "Programma strategico Intelligenza Artificiale" (a cura del Ministero dell'Università e della Ricerca, del Ministero dello Sviluppo Economico e del Ministro per l'Innovazione tecnologica e la Transizione Digitale) con azioni programmate nell'orizzonte temporale 2022-2024.

L'orizzonte del programma strategico è, dunque, ormai giunto al termine; ma, soprattutto, dal 2021 a oggi è significativamente mutato il contesto di riferimento: una profonda rivoluzione è avvenuta negli ultimi anni nell'ambito dell'Intelligenza Artificiale. È cambiato il contesto normativo, si è innovata la tecnologia, con l'arrivo dei sistemi generativi e lo sviluppo dei cosiddetti Foundation Models, e si è fatta strada una nuova sensibilità verso l'Intelligenza Artificiale, sensibilità che convintamente abbraccia la necessità di una visione etica all'innovazione, che sappia porre al centro le persone e i loro bisogni. All'interno di uno scenario così complesso e dinamico, è giunto dunque il momento di aggiornare la nostra visione strategica sull'Intelligenza Artificiale, definendo un nuovo programma che muova dalle precedenti esperienze, condividendone i principi di riferimento per una Intelligenza Artificiale italiana che si inquadri in un contesto europeo e promuovendo lo sviluppo di soluzioni antropocentriche, affidabili e sostenibili.

Nell'approcciarsi a una rivisitazione della strategia italiana è, al contempo, essenziale sapere cogliere la necessità di innovazione, leggendo e analizzando le mutate condizioni di contesto, e valorizzando la maturata consapevolezza (i) dell'importanza strategica di accrescere la nostra capacità di realizzare e promuovere l'utilizzo di soluzioni di IA nel tessuto produttivo, imprenditoriale, formativo e sociale, nonché nella Pubblica Amministrazione, e (ii) che la promozione dei tratti distintivi del nostro Paese passerà sempre più attraverso la codifica e la disponibilità di dati e modelli di IA in grado di rappresentarne e valorizzarne le specificità. Per realizzare questa visione di sviluppo, la strategia si propone di perseguire i seguenti macro-obiettivi strategici:

- Sostenere la realizzazione e l'adozione di applicazioni di IA per supportare pratiche gestio-nali, modelli produttivi e progetti di innovazione. In particolare, sarà rilevante realizzare attività progettuali e infrastrutture dati finalizzate a sviluppare sistemi di IA in una pro-spettiva country-specific, in grado di preservare i differenziali competitivi delle nostre ec-cel-

lenze, evitando una loro diluizione conseguente all'importazione di sistemi sviluppati in altri Paesi.

- Promuovere l'attività di ricerca scientifica fondazionale e applicata, incentivando la con-nessione delle nostre unità di ricerca operanti su scala nazionale con le grandi piattaforme di sviluppo operative a livello internazionale, e favorendo lo sviluppo di applicazioni di IA coerenti con il fabbisogno di natura competitiva del sistema Paese; promuovere, al con-tempo, lo sviluppo e l'utilizzo dell'IA anche a sostegno di iniziative mirate al benessere so-ciale, con applicazioni – ad esempio – nel sistema del welfare, nella tutela del patrimonio ambientale e culturale italiano, nei processi educativi e nella salute.

- Creare le condizioni di contesto favorevoli per valorizzare il potenziale in termini di genera-zione di valore dell'IA. In particolare, la focalizzazione, grazie ad un sistema di formazione che punti all'eccellenza, sulla crescita di talenti in possesso di competenze coerenti con lo scenario emergente e l'efficientamento dei servizi della Pubblica Amministrazione grazie all'introduzione di soluzioni di IA rappresentano priorità trasversali e abilitanti.

La pianificazione e la realizzazione di progetti in grado di orientare il paese rispetto a questi punti cardinali richiede la presa di coscienza: (i) del ruolo chiave giocato dall'IA sul fronte geopolitico e (ii) dell'assoluta necessità del varo di un progetto unitario in grado di coordinare e finalizzare gli sforzi di tutti gli stakeholders. In questa prospettiva, è, in primo luogo, indispensabile gestire in modo bilanciato il trade-off tra il "rischio di non fare" e una sottovalutazione delle implicazioni etiche conseguenti a un utilizzo in chiave opportunistica dei sistemi di IA.

È infatti evidente come, da un lato, sia quantomai opportuno sostenere un rapido processo di introduzione dell'IA nel sistema socio-tecnico italiano, onde evitare rilevanti penalizzazioni sul fronte competitivo, ma come, dall'altro, sia indispensabile operare in stretto coordinamento con la comunità internazionale per favorire un sistema di regole coerenti con un principio di responsabilità sociale a tutto tondo (diritto alla privacy, gender balance, trasparenza nella catena del valore del dato, ...). La definizione della strategia richiede, infatti, di contemplare una serie fattori interconnessi, tra cui l'impatto sociale, la privacy, la sicurezza, l'impatto su questioni di genere, i temi ambientali e la sostenibilità. E, infine, è importante valutare con attenzione la dinamicità con cui evolvono le tecnologie e le applicazioni di IA, caratteristica che dovrà trovare riflesso nella progettazione e nelle modalità di attuazione della varie iniziative. In particolare, da una parte, le imprese e la Pubblica Amministrazione hanno necessità di reagire con prontezza ai nuovi stimoli e alle nuove sfide della competitività; in questi contesti, sarà cruciale pertanto promuovere l'adozione di soluzioni di IA già disponibili sul territorio nazionale o lo sviluppo di nuove soluzioni secondo tempistiche che dovranno risolversi in un orizzonte di breve periodo, portando dunque a tangibili e immediati riscontri. D'altra, sarà però importante aprire una finestra verso il futuro, affrontando sfide tecnologiche nella ricerca di base e applicata, con lo sviluppo di soluzioni più complesse e innovative, che ci consentano di acquisire un bagaglio di conoscenze e competenze spendibili in un orizzonte di medio-lungo periodo.

Per dettagliare le azioni strategiche secondo le linee qui brevemente delineate, il documento analizzerà preliminarmente il contesto globale e il posizionamento italiano, per articolare un quadro complessivo della visione e dei macro-obiettivi della strategia. Saranno poi definite le vere e proprie azioni strategiche che, in effetti, saranno strettamente interconnesse e correlate tra loro; al solo fine di semplificare l'esposizione, tali azioni saranno raggruppate in quattro macroaree: Ricerca, Pubblica Amministrazione, Imprese e Formazione. Tali aree saranno comunque legate tra loro da alcune importanti e specifiche azioni di natura trasversale, orientate alla definizione di elementi infrastrutturali e alla politica di attuazione e coordinamento dell'intera strategia. Su ciascuna area, la strategie saranno poi definite, associandovi anche opportuni target di riferimento: la strategia proporrà, infatti, anche un sistema di monitoraggio della relativa attuazione, che rappresenta un essenziale ingrediente per garantirne il successo. Infine, il documento analizzerà il contesto regolativo che definisce la cornice entro cui l'intera strategia dovrà essere dispiegata.

ANALISI DEL CONTESTO

L'Intelligenza Artificiale in uno scenario globale

L'intelligenza Artificiale (IA) è in una fase di straordinario sviluppo, in cui si sta caratterizzando come un catalizzatore di cambiamento del modo in cui viviamo, lavoriamo e interagiamo con il mondo che ci circonda. Tale sviluppo è animato dalla forza propulsiva di una intensa attività di ricerca, che ha portato a numerosi avanzamenti nella definizione delle architetture e nei modelli di IA, e che è stata sostenuta da enormi investimenti, in particolare di aziende private e leader nel settore. L'ammontare degli investimenti corporate (includendo fusioni e acquisizioni, partecipazioni minoritarie, investimenti privati e offerte pubbliche) si è ad esempio decuplicato in soli 7 anni, dal 2013 al 2020, raggiungendo un valore complessivo di 147 miliardi di dollari, per poi evidenziare un picco di 276 miliardi di dollari nel 2021 e attestarsi a 189 miliardi di dollari nel 2022[1]. Lo sviluppo delle tecnologie basate sull'Intelligenza Artificiale ha, però, ormai ampiamente travalicato i confini dell'accademia e dei centri di ricerca, caratterizzandosi per un profondo impatto sociale in relazione ai condizionamenti psicologicicomportamentali che può produrre.

Basti pensare che la piattaforma ChatGPT di OpenAI rilasciata nel novembre del 2022 ha raggiunto i primi cento milioni di utenti in soli due mesi, polverizzando i precedenti record di utilizzo stabiliti da popolari social networks. Ma l'Intelligenza Artificiale sta, soprattutto, già profondamente impattando l'economia globale, sia direttamente sui mercati e i processi produttivi sia attraverso l'incremento dell'innovazione e dei processi di trasformazione digitale in diversi ambiti applicativi. È stato stimato, ad esempio, che la sola IA generativa ha il potenziale di produrre valore equivalente a 4.4 trilioni di dollari ogni anno[2]; mentre i settori che registreranno i maggiori benefici saranno verosimilmente il commercio al dettaglio, i servizi finanziari, l'assistenza sanitaria e la formazione, ambiti nei quali si ritiene che l'IA possa aumentare la produttività, incrementare la qualità dei prodotti e favorirne il consumo[3].

Spinta da questa rivoluzione tecnologica, è naturale infine attendersi anche una profonda trasformazione nel mercato del lavoro. Già oggi è sempre più marcato il disallineamento tra le professionalità richieste dai datori di lavoro e quelle possedute da chi è in cerca di lavoro, e tra le competenze e le qualifiche richieste per la conduzione di un'attività specifica e quelle possedute da chi attualmente la gestisce[4], rendendo quindi essenziali lo sviluppo di programmi di upskilling e reskilling.

L'Intelligenza Artificiale in Italia

L'intelligenza Artificiale può vantare in Italia una solida tradizione accademica, che affonda le proprie radici nei primi anni Settanta e che nel tempo ha saputo generare un vivace ecosistema distribuito sull'intero territorio nazionale.

L'Università italiana non ha quindi assistito da spettatrice alle frenetiche innovazioni tecnologiche e alla rivoluzione dell'IA nell'ultimo decennio. Oltre 160 curricula universitari, incardinati in 53 Atenei, erogano già insegnamenti collegati all'IA[5]. Inoltre, dall'anno accademico 2020/2021, è attivo il Dottorato Nazionale in Intelligenza Artificiale[6], che si articola in cinque dottorati federati fra loro che raggruppano 61 università ed enti di ricerca. Queste importanti iniziative, tuttavia, non riescono ancora ad allineare l'Italia – in termini di numero di studenti laureati o con dottorato in ambito IA – alle richieste di un mercato del lavoro sempre più orientato verso le nuove tecnologie[7]. In effetti, l'Italia resta ultima assoluta tra gli stati membri per quanto riguarda il numero di laureati nel settore ICT (1,5%)[8]. Inoltre, si posizione al quartultimo posto in relazione alla percentuale di cittadini che possiedono competenze digitali di base (45,60%): un campanello di allarme importante sulla necessità di investire anche in politiche di educazione alla cittadinanza digitale, oltre che rafforzare ulteriormente i percorsi professionalizzanti nell'IA.

Per quanto attiene alla qualità e consistenza delle attività di ricerca nell'IA, l'Italia ben si posiziona a livello internazionale. Per numero di pubblicazioni in IA prodotte nel 2022 l'Italia si pone settima[9] con 3.261 pubblicazioni, sebbene molto distanziata dalle prime tre nazioni ossia Cina, India ed USA. Sul fronte della progettazione della ricerca, è significativo poi osservare che il 12% del totale dei progetti europei sull'IA vede coinvolte unità di ricerca italiane[10].
Va ricordato, in particolare, che università e centri di ricerca italiani sono presenti in tutti i progetti Europei sulle call "Center of excellence in AI" di Horizon 2020. Inoltre, nella Call Horizon CL4 2022, sulle European Lighthouse in AI, l'Italia coordina il progetto ELIAS, risul-

[1] *Artificial Intelligence Index Report 2023, Stanford University*
[2] *The economic potential of generative AI: The next productivity frontier, McKinsey Digital*
[3] *Report on Sizing the price, PwC*
[4] *Future of Jobs 2023, World Economic Forum*
[5] *Offerta Didattica in Italia sull'IA 2023, Associazione Italiana per l'Intelligenza Artificiale e Laboratorio Nazionale di Artiifcial Intelligence and Intelligent Systems del Consorzio Interuniversitario Nazionale per l'Informatica*
[6] *https://phd-ai.it*
[7] *Il Futuro delle Competenze nell'Era dell'Intelligenza Artificiale, EY, ManpowerGroup, Sanoma Italia*
[8] *https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators*
[9] *https://www.scimagojr.com/countryrank.php?category=1702*
[10] *Artificial Intelligence: l'era dell'implementazione, Osservatorio Artificial Intelligence del Politecnico di Milano*

tato primo tra i 128 progetti presentati. L'Italia è anche attiva nelle Associazioni Europee di Intelligenza Artificiale, e in particolare in Eu-rAI, CLAIRE, ELLIS e ADRA. L'Italia ha dunque una consolidata esperienza, in ambito scientifico, che si è recentemente strutturata con l'esperienza della Fondazione FAIR – Future Artificial Intelligence Research, referente unico nei confronti del MUR per l'attuazione, il coordinamento e la gestione del partenariato esteso relativo all'area tematica "Intelligenza Artificiale: Aspetti Fondazionali", finanziato nell'ambito del PNRR. FAIR coinvolge oltre 350 ricercatori, organizzati su 10 spoke cui contribuiscono 13 atenei italiani, i centri di ricerca del CNR, FBK, IIT e INFN, oltre che importanti stakeholder industriali.

A fronte di un ecosistema così dinamico nell'ambito dell'Università e della ricerca, le ricadute sul tessuto produttivo e imprenditoriale restano tuttavia ancora piuttosto limitate[11]. Solo il 15% delle piccole e medie imprese (PMI) italiane ha avviato un progetto pilota di IA nel 2022; un valore assolutamente troppo basso, seppure in crescita di 9 punti percentuali rispetto all'anno precedente[12]; inoltre, circa 600 sono i brevetti in AI e poco più di 350 risultano le start-up di IA fondate a partire dal 2017, dato che ci colloca quale fanalino di coda in Europa[13].

Un importante acceleratore potrebbe essere l'IA generativa, il cui potenziale potrebbe portare ad aumentare il PIL italiano fino al 18,2% annuo, rappresentando una opportunità unica per rafforzare l'economia nazionale[14]; infatti, ben il 78,2% delle aziende italiane prevede di utilizzare nel breve-medio periodo tecniche di IA generativa, in particolare per la ricerca di informazioni, per assistenti virtuali e chatbot, nell'efficientamento dei processi, nel supporto alla creatività e nella simulazione e modellazione di scenari.

Una prima importante spinta all'adozione di soluzioni innovative, anche basate sull'IA, nel contesto produttivo e imprenditoriale risale al 2018 con il Piano Nazionale Industria 4.0, che istituiva 8 centri di competenza nazionali. Il decreto ministeriale 10 marzo 2023 ha poi rifinanziato le attività degli otto centri fino a tutto il 2025, disponendo al contempo il finanziamento di 40 European Digital Innovation Hub di cui all'articolo 16 del Regolamento UE 2021/694. Affiancandosi ai Digital Innovation Hubs (sempre istituiti con il Piano Nazionale Industria 4.0) e talvolta caratterizzandosi per un preciso focus sull'erogazione di servizi basati su tecniche di IA, gli EDIH forniscono servizi a prezzi agevolati per la digitalizzazione non solo delle PMI ma anche della Pubblica Amministrazione.

In effetti, l'impiego di IA nella Pubblica Amministrazione è una delle principiali direttrici di innovazione per costruire una radicalmente nuova immagine dei servizi al cittadino, più efficace e di più immediata fruibilità. Alcune importanti esperienze sono state già maturate in tale direzione.

Tra di essi, si segnalano: la progettazione della piattaforma nazionale AGENAS a supporto dell'assistenza sanitaria primaria (a oggi, la procedura di gara dal maggiore importo pari a 57,57 milioni di euro); il progetto PRODIGIT, cui partecipano il Dipartimento delle Finanze e il Consiglio di Presidenza della Giustizia Tributaria e il cui obiettivo è l'adozione di strumenti innovativi per le attività dei giudici tributari; la sperimentazione dell'INPS su un sistema di IA generativa che permette agli utenti che accedono al portale di dialogare con un assistente virtuale intelligente, dopo aver effettuato una richiesta sul motore di ricerca del sito; l'utilizzo da parte dell'Agenzia delle Entrate di un software antievasione, che analizza i dati presenti nell'Anagrafe tributaria e nell'Archivio dei rapporti finanziari.

[11] *Il Digitale in Italia 2023 Vol. 1, Anitec-Assinform*
[12] *Artificial Intelligence: l'era dell'implementazione, Osservatorio Artificiale Intelligence del Politecnico di Milano*
[13] *https://sifted.eu/articles/which-european-countries-have-the-most-ai-startups*
[14] *AI 4 Italy: impatti e prospettive dell'Intelligenza Artificiale generativa per l'Italia e il Made in Italy, The European House – Ambrosetti, Microsoft*

PRINCIPI DELLA STRATEGIA

Visione generale

L'Intelligenza Artificiale (IA) offre un'ampia gamma di tecnologie che, già in un orizzonte di breve e medio periodo, potranno essere utilizzate per stimolare e accelerare lo sviluppo del nostro Paese. L'Intelligenza Artificiale è sempre più efficace, ad esempio, nel potenziare la produttività delle imprese e l'efficacia della Pubblica Amministrazione, ottimizzando i processi, riducendo gli errori e migliorando la qualità di prodotti e servizi. Essa sta già abilitando innovativi approcci nel campo della salute e delle cure mediche, garantendo una prevenzione più capillare e attenta, diagnosi più precoci e trattamenti più efficaci.

L'IA migliora l'esperienza dei cittadini nel rapporto con le Istituzioni; fornisce un prezioso supporto nei processi educativi e di apprendimento; è una preziosa alleata nel miglioramento della qualità della vita delle persone e della gestione sostenibile delle risorse, ottimizzando l'utilizzo di energia e materie prime; è un elemento determinante per garantire la sicurezza nazionale e la difesa del Paese. Lo sviluppo delle tecnologie di IA ha infatti avuto, e sempre più avrà nel prossimo futuro, ritmi frenetici che apriranno a opportunità e cambiamenti da saper ben governare. Proprio in questo dinamismo si deciderà gran parte della nostra competitività: la capacità di affrontare i cambiamenti non solo come spettatori passivi di una rivoluzione epocale, bensì come attori consapevoli e attenti, capaci di utilizzare e produrre nuove soluzioni tecnologiche, concepite e sviluppate in sintonia con i nostri valori e le peculiarità del nostro sistema-Paese.

Dall'analisi dello stato dell'arte dell'Intelligenza Artificiale in Italia, emerge la forte esigenza di consolidare e rafforzare le proprie posizioni di rilievo scientifico a livello globale, con la consapevolezza che in un sistema così dinamico qualsivoglia flessione porterebbe a dissipare rapidamente il prezioso bagaglio di competenze acquisite nel corso degli anni. Al contempo, emerge la necessità di saper interpretare queste tecnologie come un'opportunità per valorizzare la nostra forte tradizione industriale, innovando in sintonia con le peculiarità che ci rendono unici a livello internazionale. È un momento propizio per riflettere su di sé, per abbracciare il cambiamento e plasmare il futuro con la consapevolezza delle proprie identità e potenzialità distintive.

L'Italia è un grande paese industriale, il cui sistema produttivo – saldamente ancorato a una visione di eccellenza nella produzione e nel prodotto – può sfruttare le nuove potenzialità offerte dall'Intelligenza Artificiale per abilitare nuove e più efficaci soluzioni a vantaggio della competitività del Paese. D'altra parte, l'Intelligenza Artificiale può e deve essere anche orientata a supporto del benessere sociale degli italiani. Importanti impatti potrebbero aversi nel sistema del welfare, nella tutela del patrimonio ambientale e culturale, nei processi educativi e nella salute, intensa ad ampio spettro, non solo come diritto individuale ma come interesse collettivo a supporto - soprattutto - delle fasce più deboli. Essa potrà, ad esempio, diventare un prezioso strumento per contrastare le problematiche di una ageing sociecity (connesse con la decrescita demografica) proponendo una migliore qualità della vita.

La prospettiva dell'Intelligenza Artificiale quale leva di intervento che poggia sulle peculiarità del nostro sistema-Paese per migliorarne la competitività e la qualità della vita rende necessario attivare processi che consentano all'Italia di saper costruire le tecnologie di proprio interesse, non solo di essere importatrice e utilizzatrice di generiche soluzioni che mal si adattano al nostro contesto. Non si tratta solo della necessità di definire soluzioni maggiormente aderenti al tessuto produttivo e alla nostra Pubblica Amministrazione, ma anche di dare corpo a una visione in cui l'Italia – almeno su alcuni specifici verticali – possa giocare un ruolo da protagonista nell'ecosistema dell'Intelligenza Artificiale internazionale. Tale visione consente, peraltro, di interiorizzare nella tecnologia i nostri valori e il sentire della nostra comunità, aspetto che diventerà sempre più rilevante nei prossimi mesi in considerazione della crescente diffusione di tecnologie generative. Confinarsi in una posizione di meri utilizzatori dell'IA sancirebbe, infatti, sul lungo periodo non solo una dipendenza strategica da soluzioni che potrebbero non fornire adeguate garanzie[15], ma porterebbe finanche visto l'impatto che tali tecnologie hanno sulla nostra società a una omogenizzazione e stereotipizzazione culturale.

Per indirizzarci su questa nuova rotta dovremo saper sostenere sia l'attività di ricerca fondazionale sia quella applicata, creando virtuose sinergie con partenariati pubblico-privati; dovremo continuare a investire in infrastrutture sempre più efficienti per il calcolo e sempre più dedicate alle applicazioni dell'Intelligenza Artificiale; e dovremo saper sempre più riconoscere l'importanza e la centralità dei nostri talenti, puntando sui massimi standard qualitativi per la loro formazione e su azioni che sappiano poi trattenerli in Italia con concrete prospettive di crescita personale e professionale.

Settori e ambiti di applicazione

Per concretizzare la visione qui delineata, gli investimenti sull'Intelligenza Artificiale dovranno interessare tutte le aree e i possibili ambiti di applicazione, ponendo tuttavia particolare attenzione a quelli che

[15] *Do Foundation Model Providers Comply with the Draft EU AI Act?, Stanford CRFM*

hanno un ruolo prominente nel tessuto produttivo e sociale italiano. Per quanto attiene all'uso dell'IA per rafforzare la competitività del nostro Paese, ambiti di particolare interesse per sviluppare e promuovere l'utilizzo di nuove soluzioni di IA sia in ambito di ricerca applicata sia in ambito di soluzioni aziendali sono:

- l'industria del Made in Italy, con particolare attenzione all'identità manifatturiera e alle filiere dell'automazione, dell'agroalimentare, dell'arredo, dell'abbigliamento, nonché ai settori del turismo, chimico e farmaceutico, e aerospazio;
- l'industria del Digitale, con le imprese di servizi ICT e per lo sviluppo delle infrastrutture di rete digitale che consentono di abilitare le soluzioni di IA;
- l'industria Finanziaria, ambito nel quale l'utilizzo dell'IA è ormai una consolidata realtà a livello internazionale, includendo anche servizi di banking/assicurativi. Per quanto attiene invece all'utilizzo dell'IA quale leva di intervento per migliorare la qualità della vita degli individui e promuovere il benessere della società, ambiti di particolare interesse sono:
- la salute, intesa nella sua accezione di "one health", dunque non solo negli aspetti strettamente connessi alla promozione delle tecnologie digitali di IA in ambito medico, ma anche per tutto ciò che attiene alla prevenzione, alla definizione di stili di vita più sani, alla cura delle persone più fragili;
- l'educazione, ambito nel quale le tecnologie di IA stanno entrando prepotentemente con dinamiche che dovranno essere guidate, per preservare la qualità del complessivo sistema;
- la tutela del territorio, con riferimento ai beni culturali e ambientali, alle comunità e a tutti i fattori connessi con la sostenibilità ambientale della transizione digitale basata sull'IA, tenendo quindi anche in considerazione – ad esempio - aspetti legati alla gestione dell'energia, specie da fonti rinnovabili, e alla mobilità sostenibile;
- la tutela della privacy e della sicurezza delle persone, anche in relazione agli aspetti che interessano strategicamente il settore della difesa e la cyber security nazionale.

La Pubblica Amministrazione rappresenterà, infine, un dominio privilegiato di azione, per le sue ricadute su entrambi gli aspetti sopra delineati, sia per migliorare la competitività (ad esempio, con l'efficientamento delle procedure amministrative e in particolari ambiti come quello della giustizia) sia per migliorare le interazioni dei cittadini con le strutture periferiche e centrali.

Obiettivi e aree strategiche

La visione strategica per un Paese che inizia a giocare un ruolo da protagonista a livello internazionale potrà essere attuata definendo, in maniera analitica, specifiche azioni strategiche, strettamente interconnesse e correlate. Al solo fine di definire una schematizzazione concettuale, le azioni strategiche saranno raggruppate in quattro macroaree, ciascuna caratterizzata da specifici obiettivi strategici.

RICERCA

L'Italia dovrà rafforzare gli investimenti sulla ricerca fondazionale e applicata nell'Intelligenza Artificiale, promuovendo la creazione di competenze di ricerca e tecnologie specificamente calate nel contesto del nostro sistema-Paese e in linea con principi di affidabilità e responsabilità (Trustworthy AI) e antropocentrici, propri dei paradigmi Europei. La ricerca scientifica dovrà mantenere e rafforzare l'impatto dell'accademia italiana nel panorama internazionale. Particolare attenzione dovrà essere prestata all'ecosistema pubblico della ricerca e, comunque, alla ricerca finanziata dallo Stato, che potrà procedere con la massima libertà nella proprie attività di sperimentazione, utilizzando contenuti e dati per la creazione di dataset e l'addestramento di modelli resi disponibili in open source.

La ricerca fondazionale potrà puntare, ad esempio, allo sviluppo di nuovi algoritmi, modelli, sistemi di spiegabilità e per la robustezza in ambiti safety-critical, approcci per l'addestramento, paradigmi di privacy e riservatezza dei dati e architetture di calcolo, promuovendo in ogni caso la collaborazione tra diverse competenze e settori disciplinari, evitando di focalizzarsi su singole e specifiche tecnologie, e aprendo il campo all'esplorazione di nuove strade il cui potenziale potrebbe emergere nell'ottica del medio periodo. La ricerca applicata dovrà essere, invece, guidata dalle specifiche esigenze del breve periodo, articolandosi in iniziative co-progettate da partenariati pubblico-privati e che possano avere un concreto impatto sul tessuto produttivo e imprenditoriale, focalizzandosi sui contesti dal maggiore valore economico per l'Italia, per l'industria nazionale e dal maggiore impatto sul benessere dei cittadini. Sarà cruciale in questo contesto avviare anche iniziative progettuali su larga scala, che possano creare esperienze e competenze diffuse nelle diverse aree geografiche del nostro Paese.

PUBBLICA AMMINISTRAZIONE

L'Italia dovrà rendere più efficienti i propri processi amministrativi e migliorare la qualità dei servizi offerti ai cittadini attraverso l'impiego di tecnologie di Intelligenza Artificiale. Le Pubbliche Amministrazioni dovranno essere guidate nell'acquisizione di sistemi di IA e nella progettazione di nuove applicazioni specifiche per le proprie esigenze, attraverso percorsi di accompagnamento che sappiano prendere atto dell'attuale carenza di competenze professionali dedicate. Le tecnologie dovranno essere dispiegate identificando domini di particolare rilievo, nell'ottica di automatizzare ed efficientare i processi, di supportare la pianificazione strategica

e la gestione delle risorse pubbliche, di fornire supporti a livello decisionale, e di garantire la realizzazione di infrastrutture informatiche sicure che siano sviluppate da soggetti altamente qualificati e affidabili, anche attraverso piattaforme nazionali che assicurino la massima robustezza e efficienza delle tecnologie impiegate.

Tali presupposti essenziali dovranno comportare l'acquisizione di figure altamente specializzate e adeguatamente retribuite con una specifica responsabilità per ciascuna amministrazione. Altresì fondamentale sarà la formazione e la stesura di policy per il personale. In questo contesto, la realizzazione di servizi al cittadino che favoriscano la partecipazione e il coinvolgimento, garantendo la privacy e la trasparenza dei processi, sarà un obiettivo prioritario da perseguire con progetti pilota su larga scala.

In particolare, l'Italia dovrà saper garantire la neutralità tecnologica di software e piattaforme, evitando che il cittadino sia costretto a usare applicazioni proprietarie per accedere ai servizi.

IMPRESE

L'Italia dovrà agevolare lo sviluppo e l'adozione di soluzioni di Intelligenza Artificiale nelle imprese, con l'ottica non solo di efficientare gli attuali processi ma anche di abilitarne di nuovi che sappiano aprire altrettante nuove possibilità di crescita. Sarà necessario definire, al livello di sistema-Paese, un complesso di azioni che agevolino e accelerino lo sviluppo anche delle imprese, anche delle più piccole, tenendo conto delle barriere di competenze e infrastrutturali che ostacolano la diffusione delle nuove tecnologie. Particolare attenzione dovrà essere rivolta alla formazione del personale e alla creazione di sinergie con il mondo accademico e della ricerca. In effetti, lo sviluppo di una strategia per le imprese richiede di ragionare su un duplice livello di azione.

Da una parte, dovranno essere, infatti, intercettati i bisogni delle imprese utilizzatrici delle nuove tecnologie, prestando massima cura ai settori produttivi che caratterizzano l'economia italiana e individuando gli attori maggiormente capaci di colmare il divario tra la ricerca applicata e il tessuto produttivo e imprenditoriale. D'altra, dovranno essere invece potenziate le opportunità di crescita degli abilitatori dei processi di innovazione, cioè di tutte le imprese che hanno una specifica vocazione ICT e delle start-up che si caratterizzano nella realizzazione di sistemi di Intelligenza Artificiale.

FORMAZIONE

L'Italia dovrà promuovere una formazione di elevata qualità, allineata alle nuove competenze richieste per affrontare le sfide che l'Intelligenza Artificiale ci porrà negli anni a venire. Da un lato, sarà fondamentale incentivare l'insegnamento della disciplina a livello universitario in tutte le sue sfaccettature, con attenzione anche alle rilevanti questioni etiche, all'interno di una vasta gamma di percorsi formativi, promuovendo così la collaborazione interdisciplinare. Dall'altro lato, sarà cruciale concentrare gli sforzi su percorsi tecnici specializzati, come ad esempio il Dottorato Nazionale in Intelligenza Artificiale, mirando alla formazione dei ricercatori destinati a diventare i veri promotori dell'adozione dell'IA nelle imprese e nella Pubblica Amministrazione. Considerato il notevole ritardo dell'Italia nel campo delle competenze digitali di base e l'imminente impatto dell'Intelligenza Artificiale sulle professioni, diventa altresì essenziale promuovere percorsi educativi per le scuole e l'intera cittadinanza mirati a preparare la società italiana alla rivoluzione dell'Intelligenza Artificiale, oltre che iniziative di reskilling e upskilling in tutti i contesti produttivi, non necessariamente legati al mondo ICT.

Le quattro macroaree strategiche, oltre a differenziarsi per gli specifici ambiti di azione, hanno evidentemente differenti orizzonti temporali di riferimento. Le azioni nell'ambito della Ricerca dovranno essere sviluppate in un'ottica prospettica di medio-lungo periodo, con l'ambizione di esplorare soluzioni tecnologiche innovative e ancora poco battute; quelle invece rivolte alla Pubblica Amministrazione e alle Imprese dovranno essere orientate a fornire risposte dirette e immediate alle pressanti esigenze di innovazione, prediligendo soluzioni di IA sviluppabili in un'ottica di breve periodo. La Formazione, infine, estrinsecherà una duplice natura, da una parte, definendo azioni "pazienti" che mireranno a diffondere capillarmente competenze e conoscenze; dall'altra, sostenendo azioni che necessitano di tempi più brevi, come quelle legate ai percorsi di reskilling e upskilling.

Rischi della strategia

Le sorprendenti innovazioni tecnologiche degli ultimi anni continuano ad animare un fervente dibattito internazionale sui rischi collegati all'Intelligenza Artificiale, dibattito che, talvolta, ha finanche oscurato le riflessioni circa i benefici che possono apportare queste tecnologie non solo all'economia e alla competitività, ma anche all'intera società e alle persone. Ben sappiamo - dai numerosi studi centrati sulle questioni etiche e legali che emergono dall'utilizzo dell'IA - che una non appropriata gestione di una leva trasformativa di tale portata può rappresentare un fattore di accelerazione delle disuguaglianze sociali e addirittura un fattore di rischio per la tenuta democratica.

Le tecnologie – idealmente – nascono per essere imparziali, prive di pregiudizi, condizionamenti o influenze umane; in un contesto pubblico, le tecnologie dovrebbero agire in modo imparziale, senza favorire specifici interessi, gruppi sociali o prospettive. Una tecnologia come l'Intelligenza Artificiale, tuttavia, ben facilmente assume connotazioni percepibili come "non neutrali", per via della sua intrinseca connessione con le informazioni prodotte dalla società, dalle scelte umane che la guidano e la orientano, dalla complessità delle interazioni che può generare. Una strategia per l'Intelligenza Artificiale si assume dunque una grande responsabilità: orientare le tecnologie sapendo che qualsivoglia orientamento ha un impatto e specifici rischi.

Piuttosto che elaborare un quadro dei rischi legato a valutazioni di ordine generale, e in questo senso cross-nazionale, risulta pertanto essenziale comprendere i rischi dell'attuazione della nostra specifica strategia nazionale, delineata tenendo conto delle specificità del nostro sistema-Paese e orientata sugli obiettivi sopra delineati. Non è superfluo, tuttavia, ricordare che il complessivo contesto nel quale calare l'analisi di dettaglio resta, ovviamente, la regolazione completa e sistematica dell'Intelligenza Artificiale proposta dall'Unione Europea, orientata a fissare i limiti affinché nell'implementazione di queste tecnologie vengano rispettati i valori e i diritti fondamentali condivisi dalla Comunità Europea[16]. A questo contesto hanno fatto peraltro riferimento, direttamente o indirettamente, altri importanti atti o dichiarazioni di impegno internazionali, quali il recente *executive order* statunitense[17] (che cerca di incanalare gli sviluppi dell'Intelligenza Artificiale negli USA su un binario di sicurezza, affidabilità e trasparenza delle soluzioni) o la dichiarazione di *Bletchley*[18] (siglata dall'Unione Europea e da 28 Stati che si impegnano a collaborare per mitigare i rischi connessi all'impiego di tecnologie di IA, in special modo dei Foundation Model).
In una analisi che evidentemente non può essere estensiva, i principali rischi che si intravedono sono di seguito delineati, evidenziando per ciascuno di essi l'approccio metodologico proposto per mitigarli e affrontarli consapevolmente. Tali approcci saranno poi successivamente interiorizzati nella definizione delle specifiche azioni strategiche che verranno delineate per le aree della Formazione, della Ricerca, della Pubblica Amministrazione e delle Imprese.

- **IL RISCHIO DEL "NON FARE"**
  In un paese come l'Italia, storicamente refrattario alle tecnologie dell'informazione e della comunicazione e lento, approcci timidi al perseguimento degli obiettivi strategici rischiano di risolversi in uno spreco di risorse e in una ulteriore perdita di competitività. Il "non fare" può essere, in particolare, alimentato da un approccio all'innovazione che si limiti a importare/acquistare soluzioni esistenti, interpretando la rivoluzione dell'Intelligenza Artificiale come una semplice sfida a creare interfacce su un mondo tecnologico animato da altri; occorre dunque essere ambiziosi, evidenziando il valore economico dell'impiego di questi sistemi tecnologici nei servizi (anche pubblici o di pubblico interesse) e nei processi produttivi.

  Il "non fare" può, inoltre, alimentarsi anche da azioni e iniziative mal focalizzate e che non sono in grado di rispondere bene alle esigenze del contesto di riferimento; occorre, dunque, potenziare la capacità di produrre la nostra tecnologia su misura delle esigenze, dei valori, dei diritti e degli interessi del nostro Paese. Si dovrà investire in applicazioni e soluzioni che siano orientate a supportare le specificità del nostro sistema-Paese, privilegiando una dimensione di sviluppo applicativo interno e non figlio di una prospettiva di importazione. Questo anche in considerazione dell'attuale competizione geopolitica sulla tecnologia e in particolare sull'IA, una competizione alla quale l'Italia deve partecipare da protagonista, anche a supporto e stimolo della Unione Europea e degli Stati membri.

- **IL RISCHIO DELL'OMOGEINIZZAZIONE**
  Strettamente connesso ai punti sopra evidenziati è il rischio dell'omogeneizzazione culturale, che ha iniziato a prendere corpo a seguito dei significativi avanzamenti dell'IA generativa. Se da una parte la strategia italiana punta a incrementare la diffusione dei sistemi e modelli di IA, anche generativa, dall'altra deve prendere atto che la maggior parte di questi sistemi è oggi prodotta all'estero, portando quindi a riprodurre nel nostro differente contesto sociale, anzitutto italiano, ma altresì europeo, idee e valori sovente disomogenei. È questo un rischio assai rilevante che impatta fortemente sulla nostra società e i suoi diritti di libertà, e di cui non abbiamo ancora una piena percezione

[16] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206*
[17] *https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/*
[18] *https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023*

degli esiti su scala globale. Sviluppare un sistema secondo i valori e l'idea dei diritti di una nazione, porta con sé l'ineludibile interesse ad avere una tecnologia conforme ai valori costituzionali del suo ordinamento, allo stesso tempo riaffermandoli e preservandoli. Ecco perché le azioni strategiche indirizzate verso la promozione di modelli generativi, utilizzati in particolare nell'ambito della Pubblica Amministrazione e dei servizi ai cittadini, dovranno interiorizzare la necessità di sviluppare sistemi sviluppati nel rispetto dell'etica e della normativa, anche a difesa dei valori stessi della democrazia.

- **IL RISCHIO DELL'IPERREGOLAZIONE NAZIONALE**
  L'Intelligenza Artificiale è al centro della strategia "A Europe Fit for the Digital Age" definita dalla Commissione Europea, ma è (e verrà) impattata da una copiosa produzione normativa diretta a regolare l'impatto della nuova generazione di tecnologie: da un lato, dalle norme sulla protezione, la valorizzazione e la sicurezza dei dati – personali e non – (GDPR, Data Act, Data Governance Act, NIS, etc.); dall'altro da quelle dirette a disciplinare il ruolo dei fornitori di servizi (Digital Markets Act, Digital Services Act, European Digital Identity, etc.). In questo già complesso quadro regolatorio, in parte già vigente, si inserirà l'AI Act e la sua attuazione che gradualmente interesserà tutti gli Stati membri dai prossimi mesi. L'AI Act dovrà definire precisamente un quadro regolatorio armonizzato con i confini entro cui l'Intelligenza Artificiale dovrà essere utilizzata, delineando regole semplici ma certe per produttori e utilizzatori, anche con riferimento alle più recenti evoluzioni tecnologiche. Calando il contesto regolatorio europeo a livello nazionale, si dovrà evitare di costruire ulteriori sovrastrutture normative nella definizione delle azioni strategiche, adoperandosi invece nella direzione di promuovere l'AI Act con linee guida e percorsi agili e a misura di impresa e di cittadino.

- **IL RISCHIO PER IL MONDO DEL LAVORO**
  Nonostante i numerosi studi di settore condotti negli ultimi anni, non vi è una comune visione dell'impatto che i sistemi di Intelligenza Artificiale avranno sul mondo del lavoro. Non risultano probabilmente attendibili gli scenari catastrofici immaginati sul lungo periodo, mentre più verosimili appaiono, nel medio periodo, gli scenari in cui nuove competenze e professionalità andranno a sostituire quelle esistenti. Una strategia che spinge sull'adozione di sistemi di Intelligenza Artificiale accelererà evidentemente questo (inevitabile) processo di trasformazione. Ecco perché tale processo dovrà essere guidato e regolato, prevedendo - nelle sue azioni strategiche di maggiore impatto - la dovuta attenzione al capitale umano e alle persone. Cruciali saranno quindi le iniziative dell'area strategica della Formazione, e più nello specifico i percorsi di upskilling e reskilling, prestando grande attenzione a preservare e migliorare la qualità del lavoro a valle dell'adozione di sistemi di IA e del riposizionamento del personale.

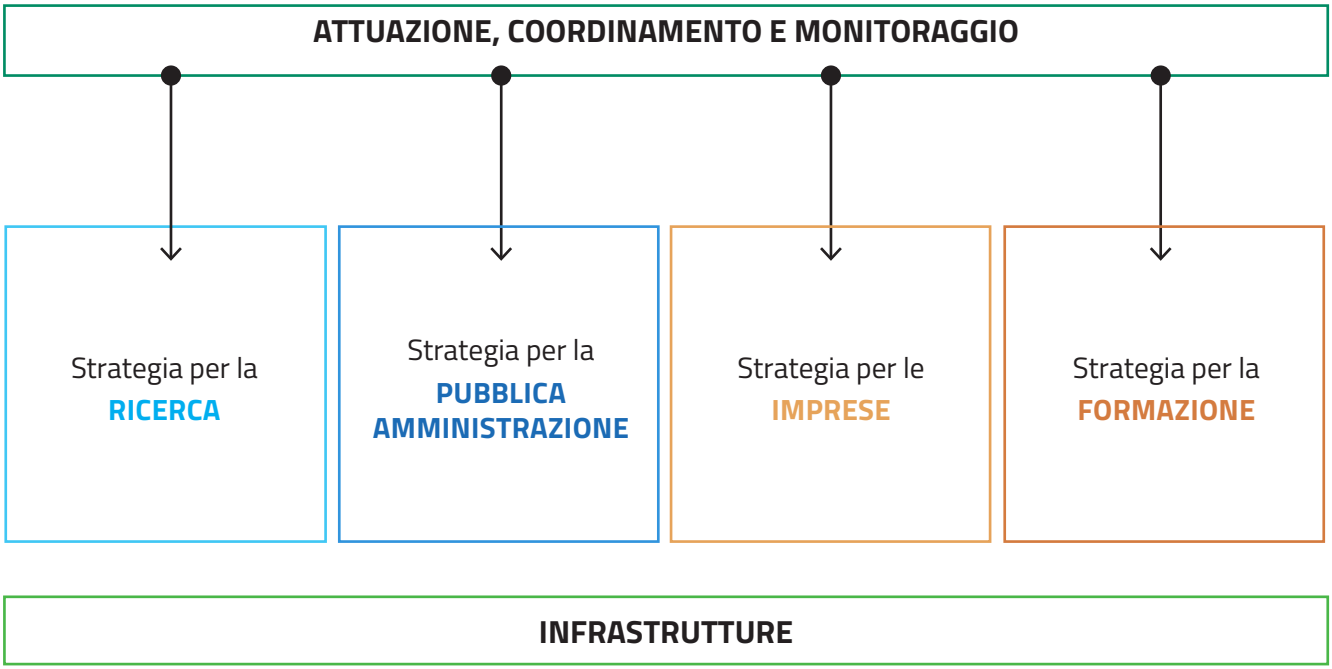
- **IL RISCHIO DEL DIGITAL DIVIDE**
  L'Italia è ancora caratterizzata da un non sufficiente livello di digitalizzazione e competenze digitali, sia nel pubblico, sia nel privato, ma in particolare nel tessuto sociale nazionale, con altresì evidenti disomogeneità territoriali tra regioni e città. Un ambizioso programma di innovazione sull'Intelligenza Artificiale, se non ben guidato e indirizzato, potrebbe portare all'effetto avverso di aumentare questi divari e queste disomogeneità. Gli investimenti previsti dalla strategia nazionale – cui già si accennava sopra - nel capitale umano, nei talenti, nei percorsi di upskilling e reskilling potrebbero, quindi, trasformarsi in pesanti boomerang sociali, se non definiti nell'ambito di iniziative trasparenti, pienamente accessibili e fruibili a qualunque latitudine del territorio nazionale. Le azioni strategiche – in particolare quelle legate al mondo della formazione, ivi inclusa quella aziendale – dovranno, pertanto, prediligere iniziative di sistema, che non si risolvano in progetti estemporanei o localizzati. La pubblicizzazione di queste iniziative e la sensibilizzazione sulla loro importanza dovrà rappresentare una linea strategica trasversale e comune a tutte le specifiche azioni.

- **IL RISCHIO DELL'INEFFICACIA**
  Non da ultimo bisogna considerare anche il rischio che la strategia nazionale manchi di efficacia nella sua attuazione, fallendo a raggiungere gli obiettivi che si prefigge. Si tratta di un rischio sempre concreto nella pianificazione, che è esacerbato in questo particolare scenario dinamico dell'Intelligenza Artificiale e dalla contingente necessità di gestire contemporaneamente numerose linee di azione, che richiedono anche importanti adeguamenti organizzativi e normativi. Infatti, le politiche per l'IA si connotano e si connoteranno sempre di più come un bersaglio mobile: la velocità delle dinamiche e dei cambiamenti, infatti, richiederà un continuo processo di revisione, con il rischio che anche una pianificazione accurata diventi rapidamente obsoleta. Per minimizzare questo rischio, si dispiegherà un opportuno meccanismo di coordinamento delle attività e un adeguato sistema di monitoraggio, avendo cura di associare ad ognuna delle azioni strategiche un indicatore e target specifici di raggiungimento di risultato.

ARCHITETTURA DELLA STRATEGIA

Infrastrutture e coordinamento

La visione complessiva della strategia sin qui delineata è molto ambiziosa. Centrare gli obiettivi strategici enucleati per ciascuna delle quattro macroaree (Ricerca, Pubblica Amministrazione, Imprese, Formazione) richiederà un grande sforzo organizzativo e, soprattutto, una sapiente e mirata azione di coordinamento, sia all'interno di ciascuna singola area sia trasversalmente tra le diverse aree. Al fine di evitare di affrontare i singoli obiettivi perdendo di vista la logica d'insieme che tiene legati i vari ambiti di interesse (e, quindi, anche al fine di mettere a fattore comune le buone pratiche e promuovere un proficuo scambio di conoscenze e competenze tra il mondo accademico, delle imprese e della Pubblica Amministrazione), elemento caratterizzante della strategia è la definizione di un contesto di azioni strategiche "abilitanti", che definiscono cioè la cornice entro cui le specifiche iniziative dovranno essere dispiegate nelle diverse macroaree. Tali azioni strategiche abilitanti sono raggruppate in due diverse tipologie (infrastrutturali e per l'attuazione, il coordinamento e il monitoraggio della strategia) per come sinteticamente rappresentato nel seguente diagramma.

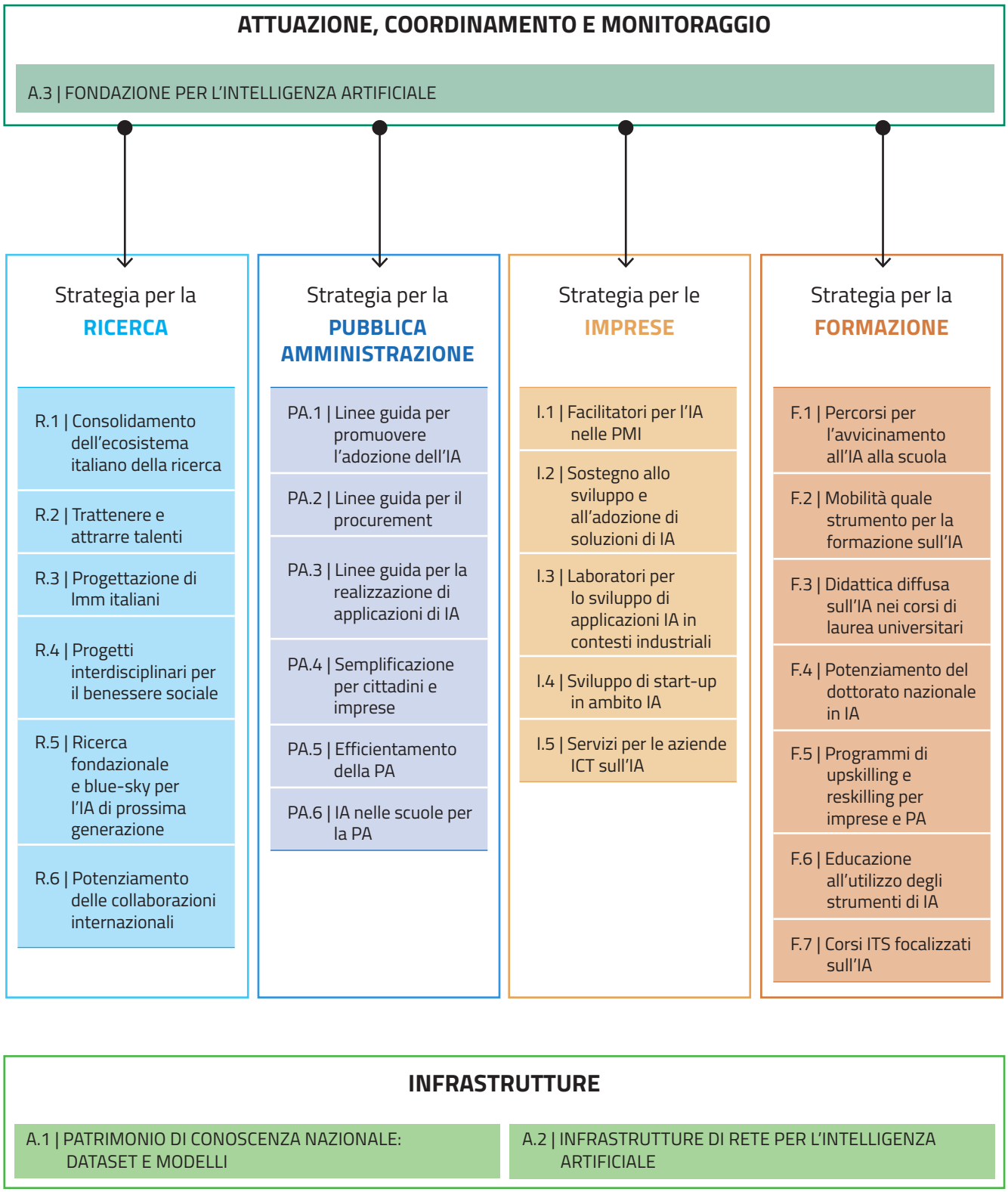


La necessità di azioni legate al potenziamento delle infrastrutture è del tutto evidente in un contesto applicativo così fortemente dipendente dalla disponibilità di grandi risorse di calcolo dedicate all'analisi di enormi moli di dati. In effetti, l'ambito infrastrutturale, da una parte, riguarda la necessità di continuare a investire su infrastrutture "fisiche" che consentano di sviluppare soluzioni di Intelligenza Artificiale sempre più all'avanguardia, mantenendo e migliorando il proprio livello di competitività a livello internazionale. Ma ancor più è necessario prendere oggi atto che i repository di dati e informazioni su cui i sistemi di IA possono essere addestrati rappresentano essi stessi una infrastruttura imprescindibile nello sviluppo di queste nuove tecnologie, una nuova dimensione infrastrutturale cui dovremo prestare crescente attenzione. Per concretizzare la propria ambiziosa visione strategica, l'Italia dovrà quindi investire nel promuovere una grande iniziativa di condivisione e riuso di dataset (ma anche di modelli) acquisiti in specifiche progettualità e contesti applicativi, non solo nell'ambito di iniziative di ricerca fondazionale, ma anche nei contesti produttivi delle imprese e della Pubblica Amministrazione. La definizione di un "registro" di dati e modelli sarà un elemento saliente della strategia (appunto un fattore abilitante) che potrà nel tempo favorire pratiche di standardizzazione e potrà accelerare i tempi di sviluppo di soluzioni, alimentandosi peraltro con dati e modelli che meglio caratterizzano i tratti distintivi del nostro Paese e che riflettono, quindi, meglio le nostre peculiarità ed esigenze.

Poggiando sulle azioni abilitanti infrastrutturali, la possibilità di conseguire degli obiettivi strategici delineati su Ricerca, Pubblica Amministrazione, Imprese e Formazione sarà poi affidata alla capacità di ben attuare le diverse iniziative. Da una parte, sarà essenziale poter definire un quadro di risorse economiche che renda la pianificazione sostenibile, attraverso la costituzione di un fondo che possa anche alimentarsi di eventuali rica-

vi provenienti dalle azioni stesse; dall'altra sarà necessario definire un soggetto cui vada in capo la responsabilità non solo della gestione di tale fondo, ma anche dell'implementazione delle diverse azioni strategiche, nell'ottica di promuovere sinergie tra i diversi attori dell'ecosistema dell'innovazione che ruotano attorno all'Intelligenza Artificiale. Tale soggetto dovrà inoltre supervisionare gli elementi infrastrutturali sopra delineati, configurarsi naturalmente come referente per il monitoraggio dell'andamento dell'implementazione delle strategie, nell'ottica di un sistema rivolto al miglioramento continuo, nonché avere in carico il budget delle azioni abilitanti.

Mappa delle azioni strategiche



Azioni strategiche abilitanti

A.1 | PATRIMONIO DI CONOSCENZA NAZIONALE: DATASET E MODELLI

Descrizione

Per mettere a sistema la conoscenza acquisita in specifiche progettualità e consentire il riuso di artefatti di IA, si realizzerà un programma mirato alla definizione di un registro di dataset e modelli, che siano costruiti secondo principi di trasparenza e fairness, che siano eticamente affidabili by design e che siano riusabili per accelerare le soluzioni delle aziende italiane. La definizione del progetto si articolerà secondo tre macro direzioni: (i) metodologica, al fine definire un protocollo nazionale per garantire che i dataset siano trustworthy-by-design e trusthworthy-by-default sia legalmente sia ingegneristicamente, definendo approcci per la mitigazione di rischi (in termini etici e di cyber sicurezza); (ii) realizzativa, al fine di implementare e rendere disponibile una piattaforma che integri moderni approcci MLops e di preparazione dei dati; (iii) applicativa, in cui la piattaforma sarà verticalizzata su specifici ambiti applicativi di interesse nazionale. Tutti i progetti finanziati nell'ambito della strategia nazionale o comunque che riceveranno finanziamenti pubblici saranno tenuti a riportare i dataset utilizzati e i modelli prodotti nel registro, in accordo a linee guida che definiranno i livelli di accesso e le modalità di riuso.

Il registro sarà, altresì, utilizzato nell'ambito di specifiche iniziative di verticalizzazione sulle Imprese e sulla Pubblica Amministrazione. La verticalizzazione sulle Imprese avrà come focus quello di identificare specifiche filiere produttive, promuovendo non solo la condivisione di dati reali, ma anche la definizione di approcci alla generazione di dataset sintetici utilizzabili in specifici contesti applicativi. In questo ambito, sarà cruciale promuovere l'utilizzo di Privacy-Enhancing Technologies (PET), ossia di soluzioni digitali che consentono di raccogliere, elaborare, analizzare e condividere informazioni proteggendo la riservatezza e la privacy dei dati, incentivando pertanto la partecipazione; tali tecnologie andranno promosse anche attraverso opportuni interventi formativi e di sensibilizzazione che mirino a creare una cultura di condivisione dei dati basata sulla fiducia e sulla tutela della privacy.
Per quanto attiene alla Pubblica Amministrazione, invece, l'obiettivo sarà quello di promuovere il riuso di soluzioni sviluppate con finanziamenti pubblici e di favorire la standardizzazione di procedure e piattaforme. Partendo dallo sviluppo di ecosistemi locali di competenze, con un processo bottom-up le soluzioni potranno essere infatti diffuse su scala nazionale, favorendo il coinvolgimento di altre comunità locali anche dimensionalmente diverse, rispondendo ai loro bisogni, sfruttandone disponibilità e creatività per costruire una soluzione a loro indirizzata. I problemi da affrontare sono ovviamente la disomogeneità dei progetti, legati alle contingenze locali e ai diversi livelli di scalabilità. La definizione del registro consentirà anche di attivare procedure di catalogazione dei vari database esistenti nell'ambito della Pubblica Amministrazione, annotandoli con fattori di qualità e di riservatezza utili anche per definirne l'uso all'esterno della struttura che ha generato i dati.

A.2 | INFRASTRUTTURE DI RETE PER L'INTELLIGENZA ARTIFICIALE

Descrizione

Il crescente utilizzo di soluzioni basate sull'Intelligenza Artificiale porterà, nel medio periodo, a un rischio di congestione delle attuali infrastrutture digitali di comunicazione, in considerazione dell'incremento significativo del traffico dati generato dalle più moderne soluzioni tecnologiche. Sarà quindi necessario prevedere specifiche azioni strategiche per il miglioramento e l'ampliamento dell'attuale infrastruttura di rete, specialmente nelle aree ad alta densità di traffico. Numerose azioni potranno essere dispiegate. Si promuoverà lo sviluppo di reti intelligenti che possano adattarsi dinamicamente alla domanda in tempo reale.

Si favorirà la collaborazione tra il settore pubblico e privato per garantire che gli operatori di rete e le aziende tecnologiche lavorino insieme per affrontare le sfide legate alla congestione di Internet; questa partnership includerà incentivi per gli investimenti nelle infrastrutture, nonché programmi di ricerca e sviluppo congiunti per soluzioni innovative. Si favorirà l'implementazione di soluzioni interoperabili, riducendo il carico di dati e mitigando la congestione, e investendo nella standardizzazione di soluzioni di rete per tecnologie di IA. Si promuoverà – infine – la consapevolezza e l'educazione sulla gestione responsabile dell'IA, incoraggiando le aziende a implementare pratiche che riducano l'impatto sulla rete, come l'ottimizzazione degli algoritmi, la compressione dei dati e l'utilizzo di tecnologie di edge computing.

A.3 | FONDAZIONE PER L'INTELLIGENZA ARTIFICIALE

Descrizione

Al fine di perseguire efficacemente gli obiettivi definiti nella strategia sarà essenziale definire un soggetto cui vada in capo la responsabilità dell'attuazione, del coordinamento e del monitoraggio delle singole iniziative. Per quanto attiene all'attuazione, sarà evidentemente necessario prevedere l'istituzione di un fondo che renda sostenibili le azioni strategiche e che, in chiave prospettica, possa essere anche alimentato da ricavi (di varia natura) provenienti dalle azioni stesse. Il soggetto si potrà, pertanto, ben caratterizzare come una Fondazione che, data la sua centralità nel complessivo ecosistema dell'innovazione, potrà essere posta sotto il

diretto controllo della Presidenza del Consiglio dei Ministri. La Fondazione avrà cura, in primo luogo, di gestire e mantenere il registro delle soluzioni di IA (di cui all'Azione A.1), anche valorizzandolo con un opportuno modello di business che ne consolidi la sostenibilità a regime.

In particolare, è opportuno prevedere forme di equo compenso per i titolari dei diritti sui dati e sui contenuti ove questi vengano utilizzati, nell'ambito del registro, per scopi di lucro. La Fondazione si caratterizzerà, inoltre, come nodo centrale di una complessa rete di attori, promuovendo lo sviluppo e l'adozione di sistemi di Intelligenza Artificiale nelle diverse macroaree strategiche e, in particolare, nelle Imprese e nella Pubblica Amministrazione. In effetti, occorre essere consapevoli che le politiche per l'IA sono e saranno nel medio periodo una sorta di bersaglio mobile: l'evoluzione tecnologica sottesa è tale infatti da richiedere un continuo adeguamento e/o revisione delle traiettorie tecnologiche di sviluppo dell'IA e la loro declinazione a supporto della competitività del Paese. In questa prospettiva, il coordinamento della Fondazione dovrà caratterizzarsi per attività volte a: (i) identificare un'agenda di sviluppo in termini di competenze, strumenti, processi e prodotti, in stretta sinergia con tutti gli attori dell'ecosistema; (ii) definire e promuovere iniziative di awareness, per fare prendere coscienza – specie alle PMI – delle opportunità di business create dall'IA, la cui carenza è una delle principali barriere all'adozione di queste tecnologie, stimolando così la domanda; (iii) definire criteri per la certificazione delle competenze digitali e di IA delle imprese; (iv) produrre un documento annuale di forecasting, che definisce elementi prospettici sull'utilizzo dell'IA nelle Imprese e nella Pubblica Amministrazione; (v) definire e incentivare iniziative strategiche per l'applicazione industriale dell'IA; (vi) raccogliere i bisogni delle Imprese nei diversi settori per le diverse tecnologie; (vii) coordinare la valutazione di progetti per l'accesso a specifici finanziamenti per PMI e start-up proposti nell'ambito della strategia nazionale; (viii) dare supporto alla compliance regolativa tramite linee guida e best practices. Infine, la Fondazione avrà responsabilità sull'intero processo di monitoraggio della strategia, valutando costantemente lo stato di avanzamento delle singole azioni e il raggiungimento dei target.

STRATEGIA PER LA RICERCA

Obiettivi	Investire sulla ricerca scientifica fondazionale sull'IA
	Valorizzare la ricerca applica dell'IA
Azioni strategiche	R.1 | Consolidamento dell'ecosistema italiano della ricerca
	R.2 | Trattenere e attrarre talenti
	R.3 | Progettazione di lmm italiani
	R.4 | Progetti interdisciplinari per il benessere sociale
	R.5 | Ricerca fondazionale e blue-sky per l'IA di prossima generazione
	R.6 | Potenziamento delle collaborazioni internazionali

Visione d'insieme

Obiettivo fondamentale della ricerca scientifica è quello di migliorare la qualità della vita delle persone e del contesto sociale in cui vivono. L'Intelligenza Artificiale, in un futuro prossimo, potrà offrire strumenti e tecniche sempre più efficaci per raggiungere questo obiettivo, grazie anche alla grande dinamicità e celerità con cui i risultati della ricerca riescono oggigiorno a trasformarsi in servizi e prodotti utili agli individui, alla società e al mondo produttivo. In questo scenario di rivoluzione continua, l'Italia deve puntare a mantenere e a intensificare la propria competitività nella ricerca a livello internazionale. Questo riguarda sia il posizionamento accademico sia la capacità di technology transfer, affinché la ricerca fondazionale possa diventare un volano per la realizzazione di tecnologie direttamente applicabili all'innovazione del Paese.

La ricerca nel campo IA supera necessariamente i confini nazionali e non può esimersi da una cooperazione in larga scala: sono quindi necessarie azioni che supportino l'ecosistema nazionale in un contesto di relazioni internazionali e principalmente europee, favorendo mobilità, il ritorno di talenti italiani dall'estero e l'attrattività delle università e dei centri di ricerca italiani per talenti stranieri.
La ricerca italiana dovrà, quindi, essere supportata con investimenti paragonabili a quelli del panorama internazionale, orientandosi sia alla ricerca fondazionale dell'IA in continua evoluzione e alla ricerca blue-sky ad alto rischio e a lungo termine, sia alla ricerca che privilegi la sostenibilità in termini ecologici, sociali, etici e legali propri dell'Italia e dell'Europa, sia infine alla ricerca multidisciplinare e alla ricerca applicata in diretta relazione con le imprese. Quest'ultimo ambito è, in effetti, particolarmente rilevante in considerazione del rischio che l'Italia possa perdere competitività a livello globale nelle sue eccellenze produttive, se non efficacemente supportate da tecnologie capaci di reggere la sfida con economie più forti e contesti più innovativi. A riguardo, dovrà essere favorita la creazione di sinergie sia con imprese utilizzatrici di tecnologie, sia con imprese che operano nel mondo ICT abilitando nuove soluzioni di Intelligenza Artificiale, al fine di creare di un forte ecosistema nazionale che sia anche terreno fertile anche per lo sviluppo di start-up innovative.

Obiettivi

- **Investire nella ricerca scientifica fondazionale** sull'IA, consolidando le iniziative esistenti quali il Partenariato Esteso sull'IA; promuovere la collaborazione tra diverse competenze, finanziando progetti a natura interdisciplinare; aprire il campo all'esplorazione di progetti fortemente ambiziosi e ad ampio spettro (blue-sky); sostenere un piano straordinario per trattenere e attirare i talenti, per sostenere la competitività nel contesto internazionale.

- **Valorizzare la ricerca applicata** dell'IA, attraverso iniziative coprogettate da partenariati pubblico-privati, anche con laboratori dedicati che coinvolgano imprese, atenei e centri di ricerca, focalizzandosi sui contesti dal maggiore valore economico e sociale per l'Italia e dal maggiore impatto sul benessere dei cittadini.

Azioni strategiche

R.1 | CONSOLIDAMENTO DELL'ECOSISTEMA ITALIANO DELLA RICERCA	
Descrizione	L'ecosistema della ricerca italiana in IA è estremamente vivace, dinamico, di riconosciuto valore internazionale, ma anche assai distribuito nel paese in molte università e centri di ricerca nazionali. I finanziamenti del PNRR hanno permesso la realizzazione della Fondazione FAIR, che è stata capace di sviluppare un ecosistema multicorale, a partire dal nucleo fondante di 15 università, di enti di ricerca accreditati in IA (CNR, IIT, FBK), di centri di importante rilievo scientifico (INFN) e di grandi imprese del territorio, esteso grazie alla presenza del Consorzio Interuniversitario Nazionale per l'Informatica (attraverso il Lab AIIS) a più di 50 centri di ricerca che di fatto coprono tutto il territorio nazionale. L'ecosistema si rafforzerà inoltre negli anni attraverso i finanziamenti a cascata, nell'ottica della massima inclusività delle eccellenze italiane e delle imprese. Si tratta dunque di un investimento in un ecosistema importante, che dovrà essere supportato e ulteriormente potenziato, anche analizzando bene le criticità ed eventualmente rimodulando o riprogettando l'attuale organizzazione. Sarà quindi essenziale per lo sviluppo della ricerca investire ulteriormente nella promozione dell'iniziativa, ragionando anche nell'ottica dell'estensione del partneriato. Sarà in particolare essenziale coinvolgere nel partenariato il tessuto produttivo e imprenditoriale, caratterizzando l'iniziativa come ecosistema pubblico-privato, luogo di incontro e di naturale scambio di competenze e conoscenze tra le università, i centri di ricerca, le imprese ICT che operano nello sviluppo di sistemi di IA e quelle che nelle loro specifiche attività possono beneficiare delle innovazioni tecnologiche. Si potrà, inoltre, puntare a sviluppare verticalizzazioni di tipo territoriale o tematico, e alla creazione di sinergie stabili con la Pubblica Amministrazione, mediante attività di ricerca mirata "su commissione pubblica", attività di benchmarking e di validazione di soluzioni, sia dal punto di vista tecnologico che etico-legale.

R.2 | TRATTENERE E ATTRARRE TALENTI	
Descrizione	Gli attuali finanziamenti del PNRR hanno consentito di incrementare, talvolta anche in maniera significativa, il numero di ricercatori dedicati all'Intelligenza Artificiale, sia nell'accademia sia negli enti di ricerca pubblici. Una volta esaurita la spinta propulsiva del PNRR, l'attuale impianto sarà verosimilmente insostenibile nelle dinamiche dei "normali" finanziamenti, portando alla fuoriuscita dall'ecosistema della ricerca proprio quei talenti che sono stati formati grazie al PNRR e che oggi ricoprono posizioni a tempo determinato. Per mantenere alto il livello di competitività sulla ricerca, sarà necessario un piano straordinario di assunzione nelle università, negli enti di ricerca e nelle imprese, su vari livelli. Servirà un piano straordinario di ricercatori Tenure Track, PA e PO (ed equivalenti posizioni EPR) su tematiche fondazionali e applicative legate alla IA, che permetta: (i) di assorbire i più eccellenti tra i molti RTDa/TD (formatisi grazie alle iniziative PNRR e non solo); (ii) di rispondere alle nuove necessità di formazione e ricerca che emergeranno nei prossimi anni; (iii) di ritenere e attrarre talenti dall'estero. In particolare, l'attrazione di talenti stranieri può contribuire a creare un effetto trainante sull'intera comunità, stimolando la formazione di competenze locali e facilitando lo scambio continuo di conoscenze nell'ambito dell'Intelligenza Artificiale; sarà dunque importante promuovere specifici incentivi per il "brain gain" nell'IA, anche in linea con le politiche europee (ad esempio, la Germania ha indicato un finanziamento di 500M€ solo nel 2024 per coprire nuove 150 posizioni di professorship in IA). In aggiunta alle posizioni specificamente dedicate all'IA, sarà importante definire posizioni per ricercatoti in ambiti multidisciplinari, nonché incentivare le imprese all'assunzione di ricercatori formatisi sull'IA nell'ambito delle iniziative PNRR promosse nell'ultimo biennio.

R.3 | PROGETTAZIONE DI LMM ITALIANI	
Descrizione	Lo sviluppo di Foundation Model è sempre più appannaggio di grandi centri di ricerca privati, con investimenti spesso fuori scala per l'ecosistema italiano. L'Italia non può tuttavia arretrare su questo importante fronte di competizione tecnologica, e deve rendersi competitiva in Europa, ove spiccano gli investimenti di Germania e Gran Bretagna, rispettivamente per 500 milioni di euro e 100 milioni di euro (in questo caso per modelli fondazionali "safe"). Si dovrà dunque dispiegare programmi su base competitiva per il finanziamento, anche in sinergia con soggetti privati, di progetti di ricerca collaborativa per la realizzazione di Large Language Model (LMM) e Large Multimodal Model (LLM) basati sull'italiano e multilingue. Lo sviluppo si dovrà concentrare su applicazioni specifiche e contestualizzate in importanti domini applicativi per il nostro Paese, ad esempio nella Pubblica Amministrazione o nell'ambito della salute, che rispondano pienamente ai valori e alle regolamentazioni europee in termini di: (i) trasparenza sui dati di training, per garantire il rispetto delle leggi sulla non discriminazione, la privacy (GDPR), la tutela dei diritti umani, fornendo informazioni affidabili sulle fonti in base alle quali vengono generati i contenuti; (ii) protezione dai contenuti generati falsi (allucinazioni); (iii) protezione dei diritti degli autori e dei creatori le cui opere sono utilizzate nei dati di addestramento; (iv) meccanismi di tracciamento dei contenuti generati dall'IA (quali watermarking); (v) sostenibilità ambientale, puntando a tecniche innovative di riduzione delle dimensioni dei modelli (anche con approcci di incremental e federated learning); (vi) valutazione degli impatti socio-economici a medio e lungo termine. Il programma potrebbe essere organizzato in fasi, con ente di monitoraggio che individua i progetti da ammettere alle fasi successive sulla base dei risultati raggiunti. In considerazione della complessità e della natura stessa dei sistemi di LMM, ogni iniziativa dovrà essere supervisionata da un Comitato Etico che ne approvi le linee generali e le metodologie realizzative. In particolare, il Comitato avrà cura di evidenziare i rischi connaturati alle specifiche iniziative, orientando le scelte progettuali verso approcci che garantiscano la sicurezza e l'affidabilità delle soluzioni.

R.4 | SINERGIE: PROGETTI INTERDISCIPLINARI PER IL BENESSERE SOCIALE	
Descrizione	Al fine di favorire la ricerca interdisciplinare legata all'IA, si dovrà prevedere l'attivazione di iniziative su base competitiva per progetti di ricerca sinergici medio-piccoli (da 2 a 5 partner), che puntino ad ambiziosi avanzamenti scientifici fondazionali in vari domini per i quali il ruolo dell'IA è fondamentale o nei quali essa stessa rappresenta l'oggetto della ricerca, ma per i quali si renda indispensabile il coordinamento di competenze multidisciplinari. La procedura di valutazione sarà basata su criteri di "eccellenza, interdisciplinarità e originalità", ispirata ai Synergy Grants dell'European Research Council publl(ERC). Gli ambiti di applicazione finalizzati all'utilizzo dell'IA per il benessere sociale (delineati nella Sezione "Principi della Strategia") dovranno essere primariamente considerati. Alcuni specifici domini applicativi, a titolo esemplificativo, riguardano progetti per: la tutela paesaggistica, del mare o dell'ambiente; la ricerca sulle nuove sfide create dall'IA su temi come il copyright, deepfake, disinformation online, e responsabilità; la ricerca su etica e IA; lo studio degli impatti socio-economici dell'IA su temi come disuguaglianza economica, discriminazione sociale e monopoli; l'applicazione del machine learning in altre discipline (con progetti di AI4Science); la sicurezza nazionale e delle persone; l'ottimizzazione delle risorse ambienti ed energetiche; pilot di sistemi di digitali/IA e sociali per guidare la trasformazione digitale centrata su persone e società ed abilitata dall'IA; soluzioni a supporto del patrimonio intellettuale e culturale digitalizzato (digital humanities).

R.5 | AI GRAND CHALLENGE: RICERCA FONDAZIONALE E BLUE-SKY PER L'IA DI PROSSIMA GENERAZIONE	
Descrizione	Nell'ottica di continuare a sostenere attività di ricerca fondazionale, in linea con quanto attualmente sviluppato nell'ambito del progetto FAIR, si dovrà lanciare un programma di ricerca ispirato alla struttura delle challenge di ricerca nordamericane, focalizzato su ricerca fondazionale con il potenziale di creare un salto generazionale a livello tecnologico-scientifico e generare innovazione dirompente. Il programma dovrà avere una natura bottom-up, prevedendo la selezione delle idee progettuali attraverso due fasi. Nella prima fase, i ricercatori potranno proporre tematiche per le challenge. Le idee saranno raccolte e saranno selezionate: i proponenti dei temi prescelti contribuiranno alla gestione della fase successiva, in cui si raccoglieranno le proposte coerenti con i temi e verranno selezionate le proposte vincenti. Le proposte saranno formulate da consorzi di piccole dimensioni.

R.6 | POTENZIAMENTO DELLE COLLABORAZIONI INTERNAZIONALI	
Descrizione	Al fine di incentivare la ricerca di qualità in Italia è essenziale favorire la collaborazione internazionale. A tal fine si finanzieranno programmi di ricerca per: (i) definire nuovi strumenti e soluzioni di IA; (ii) definire modalità comuni per una adozione efficace dell'IA (soprattutto per sfide sociali transazionali, e per mercati dove le aziende sono internazionali, o pur essendo nazionali insistono fortemente su mercati esteri); (iii) sviluppare strumenti giuridico-amministrativi per la tutela delle soluzioni; (iv) progettare e realizzare piattaforme informatiche avanzate in grado di rilevare e analizzare, sistematicamente e autonomamente, l'evoluzione delle minacce cibernetiche e le "anomalie" presenti nel traffico in rete che possono rappresentare un alert per la conduzione di un attacco imminente, con la capacità di attivare prontamente delle azioni proattive per mitigare o respingere le minacce riconosciute. I programmi di ricerca su base competitiva, di durata limitata a 2 anni, avranno come obiettivo di promuovere ricerche congiunte con almeno una altra nazione Europea o Extra Europea, prevedendo scambi di ricercatori in ingresso e in uscita e la realizzazione di documentazione che possa diventare un riferimento internazionale e nelle relazioni istituzionali dei paesi coinvolti.

STRATEGIA PER LA PUBBLICA AMMINISTRAZIONE

Obiettivi	Supportare i processi amministrativi
	Favorire la fruizione dei servizi della PA
Azioni strategiche	PA.1 | Linee guida per promuovere l'adozione dell'IA
	PA.2 | Linee guida per il procurement
	PA.3 | Linee guida per la realizzazione di applicazioni di IA
	PA.4 | Semplificazione per cittadini e imprese
	PA.5 | Efficientamento della PA
	PA.6 | IA nelle scuole per la PA

Visione d'insieme

L'Intelligenza Artificiale può diventare un fattore centrale nella trasformazione digitale della Pubblica Amministrazione, per il suo potenziale che può esprimere sia in termini di strumenti atti a rendere più efficienti le attività interne, sia in termini di servizi più vicini alle esigenze dei cittadini. Negli ultimi anni, diverse iniziative settoriali hanno iniziato a portare l'IA nella PA. Quello che occorre ora è saper dispiegare un approccio strutturato e sistematico che supporti tutti gli elementi che contribuiscono a un funzionamento efficace della PA. In particolare, sarà cruciale evitare la frammentazione delle soluzioni: da una parte, sviluppando alcune specifiche iniziative progettuali di interesse nazionale, che in quanto abilitatrici di nuovi processi di azione e interazione della PA meriteranno di essere sviluppate su larga scala; dall'altra, definendo i contorni nell'ambito dei quali i singoli enti e le singole amministrazioni potranno operare in autonomia le proprie scelte di innovazione, inquadrandosi tuttavia come soggetto collettivo, capace cioè di realizzare e mettere in opera soluzioni e applicazioni di IA che siano interoperabili e garantiscano precisi standard funzionali.

Nello sviluppare la strategia per la Pubblica Amministrazione sarà quindi necessario sviluppare un insieme coerente di azioni, con un approccio multidisciplinare, per sfruttare appieno le opportunità offerte dalle nuove tecnologie basate sull'Intelligenza Artificiale e con l'obiettivo di creare un circolo virtuoso tra: (i) la qualità, la privacy, la sicurezza e la corretta gestione dei dati funzionali all'utilizzo di tecniche di IA; (ii) lo sviluppo di tecnologie e strumenti software basati su IA per l'interoperabilità, la tracciabilità delle fonti, la loro credibilità, accuratezza, e pertinenza, al fine di creare fiducia negli strumenti decisionali che mettono a fattor comune ciò che è presente sulle piattaforme digitali; (iii) la formazione di competenze specifiche per il personale della PA sulle tecnologie e sugli strumenti di IA nel rispetto delle leggi, dei regolamenti e delle migliori pratiche ed esperienze; (iv) il monitoraggio e il miglioramento sistematico, con misure statistiche di qualità, delle prestazioni dei servizi in sviluppo e in esercizio; (v) il supporto per i processi decisionali strategici e la valutazione regolare delle prestazioni degli strumenti dell'IA; (vi) l'impegno contro pregiudizi e violazioni della proprietà intellettuale; (vii) lo sviluppo di strumenti a supporto dei cittadini, valutandone attentamente capacità abilitanti, vantaggi, e rischi. L'Intelligenza Artificiale ci sta sempre più mostrando il suo enorme potenziale. Come adattare il nostro modo di operare con le opportunità che l'IA offre rimane la domanda fondamentale a cui, in un momento storico denso di eventi e mutazioni socioeconomiche spesso imprevedibili, la PA deve rispondere. In questa direzione, oltre alle azioni più tecniche sarà essenziale attuare azioni di "affiancamento" – con una attenta e autorevole regia – che, tenendo conto delle competenze e conoscenze ancor non capillarmente diffuse nella Pubblica Amministrazione, sappiano promuovere un fruttuoso utilizzo dell'IA e sappiano incanalare azioni di procurement e sviluppo di soluzioni, valorizzando il loro riuso e la condivisione di buone pratiche.

Obiettivi

- **Supportare i processi amministrativi** attraverso le tecnologie dell'IA, aumentando l'efficienza e ottimizzando la gestione delle risorse pubbliche; finanziare alcuni progetti pilota su scala nazionale; sostenere le iniziative delle singole amministrazioni, inquadrate come soggetto collettivo, capace cioè di realizzare soluzioni e applicazioni di IA, e definite in ossequio a precise linee guida di interoperabilità e che garantiscano adeguati standard funzionali.

- **Favorire la fruizione dei servizi della Pubblica Amministrazione** per cittadini e imprese, attraverso soluzioni e tecnologie di IA, garantendo l'usabilità, la privacy, la trasparenza dei processi; promuovere la neutralità tecnologica di software e piattaforme della PA per offrire alternative all'utilizzo esclusivo di soluzioni proprietarie.

Azioni strategiche

PA.1 | LINEE GUIDA PER PROMUOVERE L'ADOZIONE DELL'IA NELLA PUBBLICA AMMINISTRAZIONE	
Descrizione	La Pubblica Amministrazione, che gestisce informazioni e servizi per cittadini e comunità, può beneficiare grandemente delle innovazioni portate dalla IA. Affinché questa leva trasformativa possa essere realmente dispiegata è però necessario che siano pienamente diffuse non solo adeguate competenze, ma anche una piena consapevolezza delle potenzialità tecnologiche dell'Intelligenza Artificiale, con particolare attenzione ai possibili rischi derivanti dal suo utilizzo e dalle rilevanti opportunità che può permettere. Un primo essenziale passo consisterà, dunque, nel guidare in maniera sistematica la Pubblica Amministrazione nell'orientarsi all'interno di un articolato panorama, attraverso linee guida che evidenzino le potenzialità e l'utilizzo delle piattaforme di IA anche attraverso case study specifici sull'utilizzo dell'Intelligenza Artificiale, promuovendo, nel contempo, la conoscenza di "best practices". A riguardo, sarà particolarmente rilevante sviluppare specifiche analisi verticali, come ad esempio la valutazione dell'impatto di tecniche di IA nell'ambito giuridico o in altri ambiti di specifico interesse per la Pubblica Amministrazione. Le linee guida definiranno altresì i passi metodologici da dispiegare per definire attività progettuali di innovazione nella Pubblica Amministrazione ove siano presenti strumenti di IA, sia in relazione alle questioni tecnologiche (tecnologie, competenze, rischi) sia in relazione alla definizione dei framework etici e regolatori. Inoltre, tali linee guida inquadreranno le diverse applicazioni in classi omogene, caratterizzandone gli standard minimi funzionali e i requisiti di interoperabilità, garantendo pertanto la possibilità di dispiegare soluzioni e applicazioni di IA che collochino ciascun cittadino italiano in una relazione con il proprio ente locale del tutto simile a quello di altri cittadini in altre città e regioni del territorio nazionale.

PA.2 | LINEE GUIDA PER IL PROCUREMENT NELLA PUBBLICA AMMINISTRAZIONE	
Descrizione	Condizione necessaria per la scelta degli strumenti tecnici e degli standard più adeguati per le esigenze della Pubblica Amministrazione, oltre a una solida conoscenza di dominio, è la conoscenza dei prodotti e dei servizi informatici disponibili, unitamente alla consapevolezza dei rischi di utilizzo e opportunità offerte. Orientarsi in un mondo così variegato e dinamico non è tuttavia semplice. Sarà dunque essenziale che vengano definite opportune linee guida che integrino quanto già attualmente previsto per l'ambito ICT, ma con un focus specifico sull'Intelligenza Artificiale. Tali linee guida dovranno, in particolare, saper orientare le Pubbliche Amministrazioni verso attività di procurement di soluzioni – nell'ambito di gare d'appalto o di specifici accordi quadro – che sappiano non solo ben rispondere a specifiche esigenze funzionali, ma garantire adeguati livelli di sicurezza oltre ad essere pienamente aderenti alle previsioni regolamentari in materia e alle generali linee guida sull'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione.

PA.3 | LINEE GUIDA PER LA REALIZZAZIONE DI APPLICAZIONI DI IA NELLA PUBBLICA AMMINISTRAZIONE	
Descrizione	Coerentemente con gli obiettivi generali della strategia nazionale, la Pubblica Amministrazione non solo dovrà acquisire competenze nel procurement di soluzioni già disponibili sul mercato, ma dovrà anche saper maturare competenze e attivarsi concretamente per sviluppare proprie soluzione. Si tratta di un processo molto elaborato, che dovrà basarsi preliminarmente sulla definizione di apposite linee guida indirizzate verso l'utilizzo di piattaforme sviluppate in Italia e orientate verso la realizzazione di progetti che promuovano: (i) la totale aderenza alle normative nazionali e dell'Unione Europea in termini di gestione delle classi di rischio e relativi adempimenti, con particolare riferimento alla tutela dei dati personali; (ii) la consapevolezza delle esigenze dettate dalle strategie nazionali e riconducibili allo sviluppo di tecnologie in settori altamente critici quali, ad esempio, energia e difesa, intelligence; (iii) la definizione di iniziative finalizzate alla formazione del personale che possano consentire di innalzare il livello delle competenze degli utenti su soluzioni tecnologiche avanzate e verticalizzate sullo sviluppo di processi certificabili, scalabili e condivisibili a livello nazionale.

PA.4 | SEMPLIFICAZIONE PER CITTADINI E IMPRESE	
Descrizione	Molteplici investimenti dovranno essere veicolati nelle attività di progettazione e realizzazione di strumenti e metodologie di interazione che possano consentire di agevolare il cittadino nella fruizione dei servizi offerti dalla Pubblica Amministrazione. Tali iniziative potranno essere definite in collaborazione con partner privati e con l'accademia e centri di ricerca, caratterizzandosi per un respiro nazionale. Le attività progettuali potranno essere orientate verso l'utilizzo di diverse tecnologie, come, ad esempio, meccanismi ontologici per l'integrazione di sorgenti informative, Multimodal Foundation Models e sistemi di deep learning, definendo specifici casi d'uso di ampio interesse, dalla compilazione automatica di moduli per i servizi minimi essenziali alla robotic process automation in specifici ambiti. Le attività dovranno prevedere anche specifici assessment sull'affidabilità dei sistemi, definendo altresì una precisa pianificazione sulle modalità di adozione degli stessi su larga scala. Le stesse potranno anche essere articolate in due fasi, prevedendo inizialmente lo sviluppo di pilot limitati a specifici contesti di sistemi amministrativi che potranno poi essere estesi su larga scala considerando i feedback acquisiti. In ogni caso, le specifiche funzionali e le esigenze dovranno essere chiaramente formalizzate dalla Pubblica Amministrazione, mentre le soluzioni che consentono di gestire al meglio tali specifiche andranno individuate – con appositi bandi – tra quelle già disponibili sul mercato, o tra quelle che possono essere sviluppate ad hoc, anche attraverso il coinvolgimento di società controllate o partecipate. Tra agli ambiti applicativi potranno essere prioritariamente considerati quelli di interesse sociale definiti nella sezione "Principi della strategia".

PA.5 | EFFICIENTAMENTO DELLA PUBBLICA AMMINISTRAZIONE	
Descrizione	Le tecnologie di Intelligenza Artificiale possono giocare un ruolo cruciale anche per efficientare i processi interni alla Pubblica Amministrazione. Similmente a quanto previsto per l'Azione PA.4, si tratterà quindi di definire iniziative per lo sviluppo e/o l'adozione di sistemi di IA (attraverso call pubbliche), partendo dalla mappatura dei sistemi già realizzati e dei relativi servizi offerti. Sarà cura della Pubblica Amministrazione individuare ambiti specifici di intervento, definendo le politiche da adottare e valutando l'impatto e i possibili rischi dei sistemi. Numerosi sono gli ambiti di possibile interesse. Sul fronte strettamente amministrativo, potranno essere definiti, ad esempio, sistemi per la verifica della conformità degli atti e delle decisioni amministrative alle leggi, alle procedure e ai regolamenti vigenti, ma soprattutto sistemi che siano in grado di fornire feedback e raccomandazioni automatizzate, in particolar modo, nella redazione degli atti da parte dei funzionari e dei dirigenti pubblici. Analogamente, ad esempio, anche le piattaforme per la digitalizzazione e annotazione automatica di documenti o dei sistemi di supporto ai RUP per la gestione e il monitoraggio dei Contratti Pubblici potrebbero consentire di efficientare in maniera significativa i processi della PA. Tutti i sistemi dovranno comunque avere un respiro nazionale e definire una infrastruttura e una operatività concretamente attiva su tutto il territorio.

PA.6 | IA NELLA SCUOLE PER LA PUBBLICA AMMINISTRAZIONE	
Descrizione	Per accompagnare i processi di innovazione della Pubblica Amministrazione, sarà necessario promuovere specifici percorsi di upskilling che consentano di ampliare le competenze e le conoscenze del personale attualmente in servizio. A tal fine, in seno alla Scuola Nazionale dell'Amministrazione dovrà essere istituito uno specifico Dipartimento dedicato all'Intelligenza Artificiale, prevedendo l'attivazione di corsi di formazione post-laurea di eccellenza per i dipendenti della Pubblica Amministrazione, con eventuale differenziazione sul livello e sui contenuti in relazione all'inquadramento delle figure coinvolte. L'iniziativa potrà essere inoltre propedeutica per avviare in prospettiva azioni di innovazione nella Pubblica Amministrazione, anche attraverso progetti in collaborazione con università e centri. Simili iniziative dovranno essere previste in tutte le scuole di formazione per la Pubblica Amministrazione, anche degli enti locali.

STRATEGIA PER LE IMPRESE

Obiettivi	Intercettare i bisogni di innovazione delle imprese italiane
	Sostenere il comparto italiano dell'ICT
Azioni strategiche	I.1 | Facilitatori per l'IA nelle PMI
	I.2 | Sostegno allo sviluppo e all'adozione di soluzioni di IA
	I.3 | Laboratori per lo sviluppo di applicazioni IA in contesti industriali
	I.4 | Sviluppo di start-up in ambito IA
	I.5 | Servizi per le aziende ICT sull'IA

Visione d'insieme

Il sistema delle imprese italiane si connota per una visione fortemente orientata all'eccellenza di processo e di prodotto. L'Italia è un grande paese industriale, con una forte vocazione manufatturiera, storicamente all'avanguardia nell'innovazione e nell'automazione. Abbracciare convintamente la rivoluzione dell'Intelligenza Artificiale rappresenta, pertanto, il naturale percorso di sviluppo per il sistema produttivo e imprenditoriale del nostro Paese. In questo percorso, sarà necessario articolare un progetto strategico che si muova su un duplice livello di azione. Da una parte, si dovrà puntare a valorizzare il ruolo delle imprese ICT italiane quale elemento abilitante lo sviluppo di nuove soluzioni e applicazioni di IA, accrescendone le possibilità di sviluppare iniziative progettuali, promuovendo la loro capacità di porsi in sinergia con le Università e i centri di ricerca, e facilitando la definizione di reti di relazioni nel contesto nazionale che possano creare livelli di competenze e massa critica, su specifici ambiti tecnologici e applicativi, tali da poter emergere a livello internazionale.

Parallelamente alle azioni rivolte al mondo ICT, la strategia per le imprese deve però saper rivolgersi al mondo che non opera direttamente nello sviluppo di soluzioni tecnologiche ma che, viceversa, da tale mondo riceve stimoli importanti per l'innovazione della propria catena del valore. La trasformazione digitale ha infatti posto, già da alcuni anni, imprenditori e manager di fronte alla necessità di riorientare le strategie verso una centralità del dato e dell'IA per la competitività di impresa, anche nell'ottica delle future sfide sulla sostenibilità ambientale. In questo quadro, sarà dunque sempre più rilevante saper affermare la necessità di un nuovo approccio operativo aziendale e di una nuova centralità – da affiancare a quella produttiva – riguardante la trasformazione dei dati in insight, azioni e decisioni e l'abilitazione di nuovi processi attraverso l'uso di sistemi di IA, anche di natura generativa. Nella definizione di strategie coerenti con questa visione, sarà inoltre necessario tenere conto delle peculiarità del tessuto produttivo italiano, progettando e affermando un ecosistema dell'innovazione guidata dall'IA, che sia in grado qualificare una prospettiva in cui l'eccellenza delle imprese italiane viene rafforzata da soluzioni innovative orientate a valorizzarne i tratti distintivi.

In questo senso, la progettazione di una strategia per l'IA in Italia deve essere fortemente ancorata alle specificità del nostro sistema sociotecnico e fare leva sulle iniziative già in corso di trasferimento tecnologico verso le PMI e sulla loro collaborazione con grandi imprese, università e organismi di ricerca.
Al fine di realizzare questa visione, la strategia nazionale prevede azioni di coordinamento, di rafforzamento dell'ecosistema dell'IA tra le PMI anche con fondi specificatamente dedicati, nonché iniziative per rafforzare il sistema ICT e per la creazione di start-up innovative.

Obiettivi

- **Intercettare i bisogni di innovazione delle imprese italiane**, finanziando e supportando un ecosistema centrato sull'IA, che sia in grado qualificare una prospettiva in cui l'eccellenza viene rafforzata da soluzioni tecnologiche orientate a valorizzarne i tratti distintivi
- **Sostenere il comparto italiano dell'ICT,** promuovendone il ruolo abilitante per la definizione di nuove applicazioni di IA, anche con iniziative che rispondano a precise domande di innovazione del tessuto produttivo; accrescere le possibilità di intercettare finanziamenti per sviluppare nuove iniziative progettuali in IA; sostenere e potenziare l'ecosistema delle start-up dell'IA, attraendo capitali pubblici e privati.

Azioni strategiche

I.1 | FACILITATORI PER L'INTELLIGENZA ARTIFICIALE NELLE PMI	
Descrizione	Per sfruttare appieno nel contesto produttivo e imprenditoriale le enormi potenzialità dell'Intelligenza Artificiale sarà necessario una pervasiva attività di promozione di soluzioni e sviluppo di applicazioni concretamente utilizzabili in specifici verticali, quali automazione, agroalimentare, arredo, abbigliamento, turismo, settori chimico e farmaceutico, e aerospazio. A tal fine, si definirà un ecosistema di facilitatori, radicati sul territorio, sotto il diretto controllo della Fondazione per l'Intelligenza Artificiale che gestisce l'attuazione, il coordinamento e il monitoraggio, e in forte sinergia con tutti gli attuali attori dell'ecosistema dell'innovazione, e di altre fondazioni rilevanti nel settore, quali FAIR, Chips.IT e AI4Industry. Ciascun facilitatore potrà avvalersi della collaborazione con università e centri di ricerca e coprirà una o più filiere produttive, divenendo un naturale punto di incontro tra le imprese ICT che offrono soluzioni per l'innovazione e le imprese che beneficiano di tali tecnologie. I facilitatori si caratterizzeranno quindi come: (i) soggetto che eroga servizi di innovazione basati sull'IA, quali assesment della maturità tecnologica delle aziende e caratterizzazione delle necessità/opportunità di innovazione; (ii) abilitatore di soluzioni utilizzabili, anche in una chiave di interoperabilità, dalle imprese delle filiera; in particolare, saranno coinvolte le imprese ICT italiane per sviluppare soluzioni di IA che portino a fattore comune le esigenze condivise almeno da una intera filiera, demandando poi ai singoli soggetti eventuali verticalizzazioni e ulteriori personalizzazioni; (iii) veicolo attraverso il quale collezionare e codificare i dati caratteristici delle arti e mestieri distintivi dei verticali, utilizzandoli per l'addestramento di soluzioni di Intelligenza Artificiale e alimentando il Patrimonio di Conoscenza Nazionale (Azione A.1); (iv) soggetto che sensibilizza e promuove la formazione delle risorse umane; (v) certificatore di competenze digitali e dell'IA all'interno delle imprese; (vi) creatore di sinergie fra le grandi imprese, aziende leader di mercato (tier 1) e le PMI, favorendo il trasferimento tecnologico; (vii) soggetto che sostiene lo sviluppo di start-up (anche attraverso sinergie con gli incubatori esistenti) e ne facilita l'interconnessione con il sistema delle imprese utilizzatrici di IA.

I.2 | SOSTEGNO ALLO SVILUPPO E ALL'ADOZIONE DI SOLUZIONI DI IA	
Descrizione	Elemento importante per sostenere lo sviluppo dell'ecosistema dell'Intelligenza Artificiale in Italia sarà la creazione di un serbatoio finalizzato di risorse finanziarie a sostegno di specifiche iniziative progettuali. Tale serbatoio sarà dedicato a finanziare progetti sia di imprese operanti nel settore ICT e finalizzate allo sviluppo di nuove soluzioni di IA, sia di imprese non ICT che vogliano innovare i propri processi produttivi adottando soluzioni di IA. I progetti potranno fare essere promossi da rete di imprese o da singole imprese e saranno agevolati con una pluralità di sistemi: finanza ordinaria a supporto di progetti di investimento in IA a livello di singola impresa; strumenti di corporate venture capital con riferimento, ad esempio, a iniziative IA-driven che riguardano catene di fornitura; eventuale supporto in termini di private equity; o voucher da spendere per attività di supporto all'innovazione basata sull'IA nei facilitatori di cui all'azione I.1.

I.3 | LABORATORI PER LO SVILUPPO DI APPLICAZIONI IA IN CONTESTI INDUSTRIALI	
Descrizione	Elemento importante per la crescita del tessuto produttivo in Italia è la capacità di sviluppare progetti coordinati che favoriscano la collaborazione tra le imprese e le università. Diverse grandi imprese (ad esempio in ambito manifatturiero, energetico o farmaceutico), aziende di consulenza e servizi, nonché associazioni di imprese hanno da tempo sviluppato in Italia centri di ricerca verticali per consolidare il proprio know-how tecnologico e per arricchirlo attraverso progetti con università e centri di ricerca. Sono iniziative singole e quasi sempre finanziate solo a livello privato o con finanziamenti regionali o europei. Nello specifico dominio dell'Intelligenza Artificiale, il connubio pubblico-privato (come testimoniano numerose esperienze internazionali) è imprescindibile, non solo nella definizione di attività progettuali, ma anche nella stessa definizione dei centri di ricerca in cui il contributo industriale ed accademico sia paritetico. Nell'ambito dell'IA, infatti, la ricerca universitaria deve essere fonte ispiratrice di nuove idee e sperimentazioni. In quest'ottica, si promuoverà la creazione di iniziative nuove nel nostro Paese, i "laboratori tematici in IA applicata" che coinvolgano una impresa e uno o più atenei o centri di ricerca pubblici, nonché i "centro/istituti tematici in IA applicata" che, invece, puntino a raggruppare più imprese dello stesso settore sempre nella logica di collaborazione con enti di ricerca pubblici. Tali centri saranno focalizzati su TRL maggiormente spinti verso le applicazioni di mercato, e avranno gli obiettivi di: (i) sviluppare ricerca applicata esplorativa, di interesse per le aziende o per la filiera con gestione condivisa della proprietà intellettuale, anche in relazione ai finanziamenti specifici; (ii) abilitare soluzioni esistenti in chiave di filiera, sperimentandone verticalizzazioni innovative che mantengano il know-how italiano; (iii) rappresentare un ponte tra le imprese, le università e il mondo della ricerca e dello sviluppo europeo ed internazionale, sfruttando i legami accademici soprattutto nelle aree obiettivo dell'export italiano; (iv) creare sinergie tra grandi imprese, aziende, PMI e start-up; (v) fornire un supporto alla certificazione e alla brevettazione, in collaborazione con l'ecosistema nazionale della ricerca (cf. Azione R.1) e con i centri di competenza e gli EDIH di matrice più industriale; (vi) supportare la formazione dei prossimi esperti in IA con il finanziamento non solo di dottorandi, ma anche di ricercatori e di professori in IA, di figure votate al technology transfer e, soprattutto, di tecnici e professionisti da inserire immediatamente nel mercato del lavoro.

I.4 | SVILUPPO DI START-UP NELL'AMBITO IA

Descrizione

Nell'ambito dello sviluppo e dell'applicazione di tecnologie per l'Intelligenza Artificiale, le start-up rappresentano un elemento chiave per la complessiva competitività del tessuto produttivo e imprenditoriale. L'Italia è, però, attualmente fanalino di coda in Europa sul numero di start-up di IA (0.68 start-up per milioni di abitanti, a fronte – ad esempio – di 2.05 e 1.99, rispettivamente, di Francia e Germania). Importanti attori sono già presenti in Italia con competenze consolidate nell'incubazione e accelerazione e nella raccolta di investimenti, sia nell'ambito privato sia nel contesto di importanti esperienze accademiche. I numeri sopra riportati evidenziano, tuttavia, la necessità di ulteriori e forti investimenti in questo settore. Da una parte, dovranno essere consolidate e supportate queste iniziative, con l'obiettivo di creare tra loro sinergie, non solo dunque puntando su programmi di finanziamento diretti alle nuove imprese ad altro contenuto tecnologico o su iniziative di defiscalizzazione, ma anche supportando articolati programmi che possano accompagnare le start-up in tutte le fasi del loro sviluppo. Di particolare rilievo, sarà la promozione di queste iniziative in ambito accademico, ove esse si configurano come spin-off universitari. A tal fine, potrà essere incentivata la creazione negli Atenei di laboratori di AI-Enterprise (sulla base, ad esempio, del modello del Regno Unito) che offrono un ambiente dinamico in cui i ricercatori possono lavorare assieme a professionisti aziendali, usufruendo di programmi di accelerazioni, supporto finanziario e consulenza specializzata. Questi laboratori aiuteranno, quindi, a comprendere le dinamiche del mercato e le esigenze dell'industria dell'IA, contribuendo quindi a trasformare le idee accademiche basate I in soluzioni commerciali. In questo contesto, dovranno essere promosse, inoltre, pratiche comuni per la concessione di licenze sulla proprietà intellettuale e per la creazione stessa degli spin-off, in particolare in relazione ai rapporti economici e alle partecipazioni azionarie.

D'altra parte, l'azione sarà volta a favorire l'interconnessione tra start-up e sistema delle imprese utilizzatrici di applicazioni di IA, fattore spesso decisivo in virtù delle difficoltà di interazione tra mondo delle imprese innovative e gli incumbent. Sarà rilevante mantenere un approccio integrato e coordinato, mettendo in rete attori istituzionali, privati e accademici; sarà necessario fare massa critica individuando una serie di progettualità in grado di essere un vero catalizzatore e riferimento nazionale per l'attrazione di investitori; si dovranno promuovere le partnership pubblico-privato, facilitando azioni di capitalizzazione; si dovrà promuovere il coinvolgimento dei talenti formati in ambito accademico, incoraggiando progetti congiunti; si dovranno valorizzare in ambito internazionale le soluzioni IA definite dalle start-up; si dovranno infine incentivare progetti mirati all'implementazione di sandboxes.

I.5 | SERVIZI PER LE AZIENDE ICT SULL'IA

La competitività dell'industria nazionale nel campo dell'Intelligenza Artificiale sarà fortemente condizionata dalla capacità delle imprese italiane di sviluppare soluzione e servizi in un contesto normativo europeo e globale fortemente dinamico, in cui i costi della compliance costituiscono una barriera all'ingresso nel mercato. A livello comunitario e internazionale, singoli Stati hanno sentito l'esigenza di definire "spazi di sperimentazione normativa" per l'IA (sandbox) con l'obiettivo di fornire un ambiente controllato che agevoli lo sviluppo e la validazione di soluzioni di Intelligenza Artificiale.

L'AI Act prevede la marcatura CE per i sistemi di IA ad alto rischio; e ulteriori requisiti di certificazione sono richiesti in specifici contesti applicativi. È, quindi, opportuno prevedere misure di sostegno, da una parte, per ridurre gli oneri della compliance normativa e delle certificazioni per le applicazioni specie ad alto rischio e, dall'altra, per incentivare le piccole e medie imprese e le start-up ad accedere alle sandboxes. Queste forme di sostegno potrebbero essere implementate attraverso bandi di finanziamento o mediante la fornitura di servizi di consulenza. Analogamente si dovrà supportare le aziende nel riconoscimento di sistemi IA nel riconoscimento della certificazione in settori specifici (ad es. rispetto a ENAV, ASA, EASA per l'aerospazio) anche alla luce dei nuovi regolamenti EU 2023/988 e 2023/1230.

STRATEGIA PER LA FORMAZIONE

Obiettivi	Promuovere una formazione universitaria capillare sull'IA
	Realizzare percorsi educativi sull'IA
Azioni strategiche	F.1 | Percorsi per l'avvicinamento all'IA alla scuola
	F.2 | Mobilità quale strumento per la formazione sull'IA
	F.3 | Didattica diffusa sull'IA nei corsi di laurea universitari
	F.4 | Potenziamento del dottorato nazionale in IA
	F.5 | Programmi di upskilling e reskilling per imprese e PA
	F.6 | Educazione all'utilizzo degli strumenti di IA
	F.7 | Corsi ITS focalizzati sull'IA

Visione d'insieme

L'Intelligenza Artificiale può avere un impatto trasformativo sul sistema socio-economico del Paese, giovando anche dei rapidi progressi e dalle grandi opportunità offerte dell'IA generativa. Per sfruttare i benefici dell'IA, sono tuttavia necessarie elevate competenze professionali in grado di sviluppare e gestire algoritmi e sistemi di Intelligenza Artificiale. La disponibilità di queste competenze è, però, di gran lunga inferiore alla domanda in Italia, fattore che determina un forte rallentamento nell'adozione di queste soluzioni. Preliminarmente a qualsiasi azione strategica, è quindi necessario saper affrontare questo strutturale problema, dispiegando un grande piano per rafforzare, integrare e diffondere la conoscenza dell'IA, e delle relative competenze digitali, nel sistema di istruzione: dagli Istituti Tecnologici Superiori (ITS) alle università, con particolare attenzione ai Dottorati di ricerca. L'investimento in queste attività dovrà, inoltre, saper coniugarsi con importanti tematiche sociali, quali la necessità di ridurre il gender gap nelle discipline STEM e di tener conto dell'intrinseca multidisciplinarietà della disciplina, che impone la definizione di percorsi che sappiano essere aperti a veri ambiti e competenze.

L'impatto trasformativo dell'IA sta, tuttavia, portando anche a cambiamenti che necessitano azioni che vanno ben oltre al tradizionale ambito dell'istruzione. Sempre più avanzate sono le competenze richieste nei luoghi di lavoro, e sempre più concreto diventa il rischio di allontanamento di non adeguatamente formati e non capaci di affrontare le sfide delle nuove tecnologie. Lo sviluppo di una strategia nazionale per l'Intelligenza Artificiale deve essere basata sul presupposto che, in questo eccezionalmente dinamico contesto, nessun lavoratore potrà essere lasciato indietro. L'Italia, sia nell'ambito del settore pubblico sia nel settore privato, dovrà dispiegare un forte programma di incentivazione di percorsi di reskilling e upskilling, per aggiornare e riqualificare i lavoratori, per reinserirli efficacemente nel ciclo produttivo e, più in generale, per renderli utilizzatori consapevoli dei nuovi strumenti tecnologici. L'Intelligenza Artificiale può rappresentare una importante risorsa per la creazione di nuova occupazione, e può avere impatti importanti anche nel migliorare la qualità stessa del lavoro, consentendo maggiore efficienza e produttività, coniugata ad ambienti e contesti produttivi sempre più a misura di persona. La realizzazione di efficaci programmi di reskilling e upskilling sull'intero territorio è, evidentemente, un presupposto essenziale per questa trasformazione.

Tutto ciò, comunque, non basterà ancora. Affinché le applicazioni derivanti dall'IA producano effetti positivi su tutta la società, riducendo i rischi, sarà necessario allargare ancora di più il concetto di "formazione", puntando in Italia a implementare un processo di alfabetizzazione sull'IA che coinvolga la scuola, i lavoratori e i cittadini tutti, con attenzione alle categorie più deboli. L'obiettivo è quello di evitare che, in una strategia di crescita e di investimenti sull'IA, si alimentino processi di digital divide di conoscenze che, sul lungo periodo, minerebbero la coesione sociale ed economica del Paese. Educare alla cittadinanza digitale al tempo dell'IA è essenziale, peraltro, per colmare il divario di conoscenza e affrontare le preoccupazioni etiche e sociali che può produrre questa tecnologia. Creare percorsi formativi di alfabetizzazione sull'IA nelle scuole, diffondere informazioni attraverso campagne pubblicitarie e promuovere la comprensione delle implicazioni etiche dell'IA rappresentano gli "step" fondamentali che possono consentire il corretto orientamento del tessuto socio-economico, nel suo complesso, sulla comprensione del giusto utilizzo dell'IA, cogliendone appieno i vantaggi e valutandone criticamente le limitazioni e i rischi.

Obiettivi

- **Promuovere una formazione universitaria capillare sull'IA**, in risposta alle sempre più pressanti richieste di nuove competenze nella società e nel mondo del lavoro, in un'ottica trasversale e interdisciplinare; consolidare la formazione specialistica sull'IA nei percorsi orientati verso profili tecnici e di ricercatori, quali il Dottorato Nazionale sull'Intelligenza Artificiale;
- **Realizzare percorsi educativi sull'IA** nelle scuole, per preparare le nuove generazioni a un uso attento e consapevole delle nuove tecnologie; sviluppare iniziative di divulgazione mirate a sensibilizzare e coinvolgere la società italiana nella rivoluzione dell'IA; finanziare e sostenere iniziative di reskilling e upskilling in tutti i contesti produttivi.

Azioni strategiche

F.1 | PERCORSI PER L'AVVICINAMENTO ALL'IA NELLA SCUOLA – STUDENTI E DOCENTI	
Descrizione	La rivoluzione dell'IA impone che l'avvicinamento alla disciplina avvenga con gradualità già dalle scuole primarie e secondarie. Si dovranno pertanto realizzare percorsi formativi per l'alfabetizzazione nell'IA rivolti prioritariamente a docenti e successivamente a discenti. Per quanto attiene agli studenti, un utile orientamento è rappresentato dalla legge 20 agosto 2019, n. 92, "Introduzione dell'insegnamento scolastico dell'educazione civica", che all'art. 5 individua il nucleo tematico dell'Educazione alla cittadinanza digitale. L'attuazione di questa previsione normativa dovrà essere indirizzata verso percorsi che prevedano lo studio dei principi base dell'IA, nonché attività pratiche volte a conseguire abilità nell'utilizzo degli strumenti disponibili, evidenziando il corretto utilizzo degli stessi sul piano del rispetto degli aspetti etici e sociali, nonché della privacy e della sicurezza cibernetica. Per essere concretamente efficaci, i percorsi rivolti agli studenti dovranno essere tenuti da docenti che, a loro volta, dovranno essere stati precedentemente formati sulle basi teoriche e pratiche necessarie per integrare questi concetti nei programmi di studio. A tal fine, dovrà essere dispiegata una larga campagna di realizzazione di percorsi formativi ad-hoc, anche coinvolgendo università, centri di ricerca, associazioni (ad esempio, del terzo settore) e aziende che hanno maturato specifiche competenze in iniziative di formazione, specie su tematiche digitali. I percorsi formativi, erogati su base nazionale sia in presenza sia in modalità online o ibrida, dovranno garantire che il materiale didattico utilizzato sia condiviso in modo ampio e reso disponibile. Ciò potrebbe essere realizzato attraverso repository online appositamente strutturati o altri strumenti digitali che consentano un accesso facile e aperto a risorse educative di qualità. La condivisione del materiale non solo favorirà la trasparenza e la collaborazione tra le istituzioni educative, e dovrà altresì contribuire alla creazione di una base comune di apprendimento della conoscenza nell'ambito della didattica dell'Intelligenza Artificiale. Per definire linee guida chiare e garantire la coerenza dei programmi educativi, sarà infine fondamentale la strutturazione di un coordinamento con tecnici esperti nel campo dell'Intelligenza Artificiale e specialisti di pedagogia e sociologia. La struttura di coordinamento contribuirà a definire gli obiettivi di apprendimento, identificare i concetti e gli argomenti chiave da trattare e sviluppare metodologie didattiche efficaci e personalizzate sulla base delle tipologie di discenti. La collaborazione tra tecnici ed esperti nell'ambito della formazione assicurerà che i percorsi educativi siano curati dal punto di vista tecnico e siano adattati alle esigenze di apprendimento degli studenti.

F.2 | MOBILITÀ QUALE STRUMENTO PER LA FORMAZIONE SULL'IA	
Descrizione	In un contesto così dinamico come quello dell'Intelligenza Artificiale, diventa cruciale saper definire meccanismi che consentano lo scambio di competenze ed esperienze tra diversi attori istituzionali. Specifici programmi di "mobilità" dovranno quindi essere dispiegati su 4 direttrici principali. (1) Tirocini: Esperienze nelle imprese sono spesso determinanti per la formazione dei giovani studenti universitari. Per promuovere questo strumento, dovranno essere finanziate borse di studio per tirocinanti per periodi di 3-6 mesi, da attribuirsi secondo i principi del diritto allo studio. (2) Internship: L'interscambio di competenze tra università e imprese è una buona pratica internazionale che fatica ad essere recepita in Italia. Per promuoverne l'adozione, le imprese/università potranno beneficiare di opportuni incentivi, mentre per le Pubbliche Amministrazioni i percorsi di internship potranno essere assimilatati alla formazione obbligatoria. (3) Mobilità per la ricerca: In questo caso, attraverso borse di ricerca, saranno finanziati periodi di mobilità e visiting tra diverse università italiane e/o centri pubblici e/o della Pubblica Amministrazione, con l'obiettivo di massimizzare il trasferimento delle conoscenze e agendo da leva per favorire uno sviluppo granulare e diffuso. (4) Alto Apprendistato: Una best practice che si dovrà promuovere è il modello dell'Apprendistato Duale di Alta Formazione e Ricerca, utilizzato da varie regioni a valere su fondi FSE e che consente alle imprese di assumere giovani sotto i 30 anni (studenti di ITS, università, master, dottorato) giovando degli sgravi fiscali dell'apprendistato tradizionale, permettendo ai neoassunti un periodo di formazione. Anche in questo caso, specifici finanziamenti per la formazione potranno promuovere questi interessanti percorsi.

F.3 | DIDATTICA DIFFUSA SULL'IA NEI CORSI DI LAUREA UNIVERSITARI	
Descrizione	In considerazione delle crescenti necessità del mondo del lavoro per personale con competenze digitali avanzate e del divario che, invece, oggi esiste con l'attuale qualificazione dei laureati, si dovrà puntare a rafforzare ulteriormente il panorama dei corsi di laurea universitari in Intelligenza Artificiale, promuovendo anche in maniera significativa iniziative di orientamento. D'altra parte, però, uno dei rischi associati al rapido sviluppo delle tecniche e conoscenze in ambito IA risiede nella limitatezza del bacino degli utenti cui è garantito un accesso a percorsi formativi continui e aggiornati in materia, che consentano di costruire le competenze e abilità necessarie per capirne i costi e i benefici, valutarne i processi in maniera critica, e utilizzarne gli strumenti in maniera creativa. Per mitigare questo rischio, sarà dunque essenziale che insegnamenti sulle basi dell'Intelligenza Artificiale vengano integrati in tutti i percorsi universitari, inclusi quelli non-STEM, con contenuti adattati agli obiettivi delle specifiche discipline. Di conseguenza, le università dovranno essere incentivate, ad esempio nell'ambito della quota premiale di funzionamento, sulla base della percentuale di corsi di studio in cui tali percorsi sono attivati.

F.4 | POTENZIAMENTO DEL DOTTORATO NAZIONALE IN IA	
Descrizione	Il Dottorato di Interesse Nazionale in IA (www.PhD-AI.it), attivato nel XXXVII ciclo, è il punto di riferimento della formazione dottorale in IA, con circa 150 iscritti per ciascuno dei tre cicli attivati sino a ora, che hanno creato un ecosistema che ha permesso di superare la frammentazione esistente nella formazione dottorale in IA, mettendo a sistema le iniziative di oltre 60 tra università ed enti di ricerca. I tre cicli sono stati attivati con un finanziamento ad hoc del MUR per i primi due cicli e, principalmente, dal PNRR, per il terzo ciclo. Per garantire la prosecuzione di questa opportunità strategica di formazione dottorale, sarà necessario sostenere con continuità nel tempo i 5 dottorati, oltre i primi tre cicli, attraverso il (co)-finanziamento di un minimo di 40 borse l'anno per ciascuno (anche promuovendo l'allargamento dell'attuale partneriato), in modo da garantire il soddisfacimento del vincolo del DM 226/21 sui Dottorati di Interesse Nazionale e al fine di consentire una pianificazione pluriennale, evitando la competizione con i dottorati locali degli atenei, coerentemente con lo spirito dell'art. 11 del DM 226/21: "Il Ministero favorisce l'attivazione dei dottorati di interesse nazionale e ne prevede le modalità di cofinanziamento". Per quanto attiene, invece, alle attività didattiche, il PhD-AI.it ha usufruito di un budget, limitato, per le attività promosse dal Comitato di Coordinamento solo nei primi due anni, a valere sul finanziamento iniziale MUR/CNR. Sarà, quindi, necessario sostenere a regime le iniziative didattiche coordinate fra i 5 dottorati in termini, ad esempio, di scienziati internazionali invitati a tenere corsi comuni, di organizzazione di doctoral school sia a livello di singolo dottorato sia nazionale, di eventi di promozione e disseminazione dei risultati.

F.5 | PROGRAMMI DI UPSKILLING E RESKILLING PER IMPRESE E PUBBLICA AMMINISTRAZIONE

Descrizione

L'utilizzo sempre più pervasivo dell'Intelligenza Artificiale nei contesti produttivi porterà rapidamente a trasformare le dinamiche del mondo del lavoro. Ben lontani da scenari catastrofistici sulle prospettive occupazionali, è oggi invece sempre più chiaro che le nuove tecnologie si stanno configurando come una grande opportunità.

Le competenze digitali e specifiche conoscenze nel settore dell'Intelligenza Artificiale aprono, infatti, già oggi (e apriranno sempre più nel futuro) le strade del mondo lavorativo. Eppure le prospettive (ad esempio del World Economic Forum) descrivono un crescente fenomeno di disallineamento tra le competenze richieste e quelle possedute da chi cerca lavoro: ci troviamo dunque a vivere in uno scenario paradossale in cui l'Intelligenza Artificiale rischia di ridurre il bacino dei posti di lavoro non in considerazione delle sue capacità di automazione, bensì perché il sistema della formazione non riesce concretamente a colmare la distanza che intercorre tra questi due mondi. Ecco, quindi, che investire in percorsi di upskilling e reskilling diventa a pieno titolo uno degli elementi caratterizzanti la strategia. Si tratta di declinare corsi di formazione e professionalizzazione sull'IA, per la riqualificazione e l'aggiornamento dei lavoratori al fine di favorire il loro (re)inserimento nei nuovi posti di lavoro creati dalle tecnologie dell'IA. Sarà necessaria un'attenzione particolare per i lavoratori dei settori in cui le tecnologie di IA hanno già raggiunto un elevato grado di maturità e offrono prospettive di maggiore impatto, avendo particolare cura di accompagnare – valorizzando gli aspetti motivazionali – coloro che potrebbero incontrare maggiori difficoltà (ad esempio in funzione della propria età) nell'adattamento a nuovi scenari e ad innovazioni tecnologiche. Nella strutturazione dei percorsi formativi, sarà quindi indispensabile articolare i piani di azione in relazione ai diversi ruoli e funzioni dei lavoratori, considerando in primo luogo azioni rivolte agli utilizzatori delle tecnologie, per creare ambienti ricettivi al cambiamento e pronti a valorizzare le competenze esistenti e il supporto che può oggi offrire l'Intelligenza Artificiale. Allo scopo potrà essere utile la condivisione di esperienze di successo maturate in ambito pubblico e privato. Ad esempio, sulla falsariga dell'iniziativa "Elementi di AI" promosso dal Dipartimento di Transizione Digitale e reso disponibile a tutte le realtà economiche del Paese tramite lo sportello digitale dell'imprenditore, sviluppato da InfoCamere, un corso video sull'IA erogato dai maggiori esperti italiani nel settore potrà essere realizzato e reso fruibile con le medesime modalità.

Percorsi di reskilling e upskilling dovranno, inoltre, anche essere rivolti ai quadri dirigenziali. Le nuove tecnologie impattano, infatti, profondamente gli aspetti organizzativi e la gestione dei processi interni; innovare significa non solo adottare nuove tecnologie per rispondere a specifiche esigenze di efficientamento, ma soprattutto – grazie alle enormi potenzialità offerte dall'IA – rivedere complessivamente l'organizzazione interna per creare ambienti più stimolanti e più a misura delle esigenze dei lavoratori.

Infine, percorsi di reskilling e upskilling dovranno essere dedicati ai tecnici, sia delle Imprese sia della Pubblica Amministrazione, per aggiornare il proprio bagaglio di competenze con le nuove tecnologie dell'IA. In tale contesto, oltre all'attivazione di master dedicati e percorsi professionalizzanti, una best practice che andrà dispiegata è quella delle Academy di filiera, implementata da alcune regioni su fondi FSC. L'iniziativa si articolerà con la creazione di appositi consorzi, che includono enti di formazione, associazioni di categoria e imprese medio-grandi che, congiuntamente, siano in grado di erogare corsi di reskilling e upkilling, sia per i propri lavoratori sia per quelli di tutte le PMI coinvolte nell'ambito della propria filiera. I consorziati assumerebbero, quindi, la responsabilità della progettazione e della erogazione dei percorsi formativi, coinvolgendo le proprie strutture e le rispettive risorse umane da impiegare per la formazione ai discenti, per i laboratori didattici e per la pubblicizzazione degli specifici percorsi formativi per attrarre giovani talenti.

F.6 | EDUCAZIONE ALL'UTILIZZO DEGLI STRUMENTI DI IA	
Descrizione	La pervasività dell'IA rende necessaria l'attuazione di un'attività di sensibilizzazione rivolta ai cittadini sul corretto utilizzo delle nuove tecnologie, che promuova l'uso consapevole degli strumenti e delle specifiche applicazioni digitali oggigiorno disponibili. A tal proposito, risulterà essenziale il coinvolgimento di una molteplicità di "attori" nazionali (amministrazioni pubbliche, istituzioni governative, associazioni, fondazioni, media, etc.), al fine di consentire la massima diffusione di una cultura digitale finalizzata ad un utilizzo consapevole delle tecnologie informatiche, non necessariamente solo confinate all'ambito dell'IA. In particolare, risulterà fondamentale la collaborazione con attori (specie del terzo settore) in possesso di specifiche competenze in queste tipologie di iniziative. Le iniziative dovrebbero essere messe in atto su più livelli: (i) contenuti dedicati all'interno di programmi o rubriche televisive o radiofoniche esistenti; (ii) rubriche informative e continuative su riviste e giornali generalisti; (iii) pubblicità progresso, con una campagna dedicata ai rischi e alle opportunità dell'IA; (iv) campagna di affissioni con messaggi emozionali, siti web e social media dedicati, videoclip su social; (v) eventi da realizzare sul territorio, in collaborazione con associazioni di persone o professionali; (vi) dibattiti pubblici e discussione sociale informata che coinvolgono i diversi stakeholder anche con il supporto di piattaforme. Tutte le iniziative saranno coordinate in maniera centralizzata da un comitato tecnico-scientifico, che definirà gli ambiti, i canali e i contenuti.

F.7 | CORSI ITS FOCALIZZATI SULL'IA	
Descrizione	Gli Istituti Tecnologici Superiori (ITS) rappresentano uno straordinario strumento di "eccellenza" italiana sul piano della formazione di qualità e dell'offerta formativa terziaria professionalizzante, che si colloca all'interno di un sistema consolidato da anni anche in altri paesi europei. Gli ITS offrono corsi biennali o triennali per diplomati di circa 900 ore l'anno con attività laboratoriale e stage presso le imprese, con classi di circa 30 studenti. Il loro obiettivo è formare figure con elevate competenze tecnologiche e tecniche professionalizzanti, allo scopo di contribuire in modo sistematico al sostegno delle misure per lo sviluppo economico e la competitività del sistema produttivo, in relazione alle aree tecnologiche considerate strategiche nell'ambito delle politiche di sviluppo industriale e tecnologico e di riconversione ecologica. Anche queste strutture di formazione dovranno strutturarsi per l'erogazione di corsi sull'IA e per introdurre la tematica nei corsi esistenti, prestando particolare attenzione al coinvolgimento delle università e delle aziende del settore ICT specializzate nello sviluppo di soluzioni basate sull'IA.

MONITORAGGIO DELLA STRATEGIA

Architettura del sistema di monitoraggio

La predisposizione di una qualsivoglia iniziativa strategica non può prescindere dalla definizione di un opportuno sistema di monitoraggio, che rappresenta un essenziale ingrediente per garantirne il successo. Monitorare, comprendendo l'effettivo stato di attuazione e le criticità, rappresenta infatti il presupposto per dispiegare azioni correttive ovvero, finanche, per rivedere parzialmente gli obiettivi strategici stessi, qualora fossero state rilevate repentine e significative evoluzioni del contesto. La distinzione principale che si può fare tra i diversi sistemi di misurazione riguarda l'utilizzazione di strumenti quantitativi o l'uso di approcci di natura qualitativa. Non è possibile, tuttavia, stabilire a priori una superiorità dell'uno o dell'altro approccio: la loro efficacia dipende molto dal contesto, dalla natura del piano e naturalmente anche dalla disponibilità di dati.

Ciascuna delle singole azioni strategiche definite nelle aree della Formazione, della Ricerca, della Pubblica Amministrazione e delle Imprese è stata già caratterizzata nel documento da uno specifico valore target associato a una metrica quantitativa, definita attraverso un indicatore chiave di prestazione (o *KPI, Key Performance Indicator*[19]) legato alle principali variabili di interesse. In particolare, si è scelto di utilizzare KPI solo per monitorare l'avanzamento delle azioni strategiche verso i suoi obiettivi (efficacia).

A un livello più ambizioso, si sarebbero potuti traguardare anche i costi (costo/efficacia). A un livello di difficoltà ancora crescente, si sarebbe potuto prendere in considerazione il costo in relazione alle opportunità delle risorse impiegate, arrivando così a stabilire il beneficio differenziale del progetto rispetto ai possibili usi alternativi delle risorse stesse (costi/benefici). Nella strategia si è, tuttavia, fatto riferimento esclusivamente a valutazioni di efficacia, evitando di considerare valutazioni di costo e di opportunità che richiederebbero giudizi di valore non strettamente attinenti alla strategia; ciò nonostante, l'introduzione di criteri di efficacia rappresenta un passo avanti nella diffusione della cultura della autovalutazione.
La valutazione della complessiva efficacia della strategia non può, tuttavia, risolversi con l'analisi del raggiungimento di target (su KPI) riferiti alle singole azioni, ma deve bensì considerare il complessivo impatto che tali azioni hanno generato. Una valutazione più articolata sarà affidata, quindi, alla Fondazione per l'Intelligenza Artificiale che avrà in capo le funzioni di monitoraggio (complessivo e delle singole azioni strategiche), controllo ed early warning. La Fondazione avrà anche la responsabilità di redigere un report annuale, nel quale venga mantenuta aggiornata l'analisi di contesto e venga fornita una valutazione complessiva sull'andamento dell'attuazione della strategia.
Il monitoraggio fornirà, in particolare, una valutazione su ciascuna delle aree strategiche, attraverso la stesura di un report che - in aggiunta alla valutazione circa il raggiungimento dei target per le specifiche azioni strategiche - declini i seguenti approcci:

- l'analisi di KPI riferiti all'intera area strategica;
- l'analisi di *Flagship projects*, identificando un numero molto limitato di specifici progetti, il cui stato di avanzamento possa essere considerato come proxy per l'intero comparto. Ad esempio, per molti anni negli USA, i risultati dei progetti spaziali sono stati presi come indicatore significativo del progresso scientifico e tecnologico dell'intero Paese. Ovviamente, i flagship projects dovranno essere scelti con cura: devono in particolare essere concreti, credibili, avere ampia visibilità, toccare argomenti di interesse per la vita di tutti i cittadini, contribuire a costruire un'immagine del futuro come collettività.

In particolare, per la stesura del report, la Fondazione si avvarrà anche di un panel di esperti che analizzeranno lo stato dei KPI e/o dei flagship projects, per produrre una argomentata relazione di valutazione, adottando il metodo Delphi[20,21]. Sviluppato dalla Rand Corporation ai tempi della guerra fredda (e ripetutamente aggiornato negli anni) il metodo coinvolge esperti anonimi nel rispondere a un questionario in diversi turni, sotto la guida di un facilitatore specializzato. Dopo ogni ciclo, il facilitatore fornisce una sintesi anonima delle valutazioni formulate, nonché le ragioni che gli esperti hanno fornito per i loro giudizi. Alla luce di queste informazioni, gli esperti stessi sono quindi incoraggiati a rivedere le loro risposte precedenti, convergendo gradualmente a una sintesi.

Monitoraggio delle aree strategiche

Per quanto attiene all'area strategica della **FORMAZIONE**, il panel di esperti avrà cura di analizzare alcuni specifici KPI:

- Numero di Corsi di Laurea "interdisciplinari" (non informatici o di ingegneria informatica) con insegnamenti di IA
- Numero di studenti immatricolati a percorsi di dottorato inerenti all'IA
- Competenze e consapevolezza nella cittadinanza sull'IA, da raccogliere tramite survey CATI/CAWI coinvolgendo un campione stratificato della popolazione[22].

[19] *Parmenter D. (2019) Key Performance Indicators: Developing, Implementing, and Using Winning KPIs, John Wiley & Sons Inc.*
[20] *Blokdyk G. (2023) Delphi Method. A Complete Guide, The Art of Service.*
[21] *Niederberger M., Renn O. (Eds, 2023) Delphi Methods in the Social and Health Sciences: Concepts, Applications and Case Studies, Springer Nature.*
[22] *Un campione di 1.000 persone sul totale dei cittadini italiani può fornire risultati con un margine di errore del 3%.*

Per quanto attiene alla **RICERCA**, saranno valutati sia KPI sia flagship projects. In particolare:

- Dati sulla produzione scientifica su Intelligenza Artificiale. In questo settore si può, infatti, far ricorso a consolidati indicatori bibliometrici, tenendo conto che la "scientometria" ha fatto grandi progressi in termini di capacità di analisi, valutazione e previsione[23].

- Lo stato di avanzamento e la qualità delle iniziative sulle azioni strategiche R.1 e R.3. Tali iniziative sono volte a promuovere il rafforzamento dell'ecosistema della ricerca e la realizzazione di LMM italiani, e dovranno essere analizzate valutandone i risultati effettivamente conseguiti e gli effettivi impatti.

Per quanto attiene alla **PUBBLICA AMMINISTRAZIONE**, informazioni interessanti, anche rispetto al confronto tra i paesi dell'Unione Europea, sono fornite dal rapporto DESI; questo però, oltre ad avere un lag di circa anno, offre una vista generale sul processo di digitalizzazione e non è particolarmente focalizzato sull'IA. D'altra parte, una misura specifica per tutti i comparti sarebbe difficile e soprattutto onerosa, per cui si valuterà la crescita del sistema Pubblica Amministrazione monitorando in maniera accurata due importanti flagship projects:

- **L'impatto delle iniziative sull'azione strategica PA.5**. A riguardo, si ritiene importante valutare il miglioramento dell'accesso e della fruizione dei servizi al cittadino, misurandone anche il grado di digitalizzazione. Il monitoraggio potrebbe essere effettuato dando la possibilità al cittadino, che acceda a una piattaforma di servizi, di lasciare il proprio giudizio, come avviene spesso nel caso di servizi offerti dal settore privato; in alternativa, potrebbero essere impiegate survey da somministrare a scadenze prefissate su un campione estratto dall'universo di coloro che hanno effettuato almeno un accesso.

- **L'impatto delle iniziative sull'azione strategica PA.6**. In questo ambito, si ritiene essenziale il coinvolgimento di esperti ben calati nell'ambito della Pubblica Amministrazione che riescano a valutare l'effettivo efficientamento delle procedure amministrative.

Infine, per quanto attiene alle **IMPRESE**, saranno valutati i seguenti KPI e flagship projects:

- Dati relativi all'adozione dell'IA nelle PMI. A riguardo si osserva che alcuni interessanti dati sono forniti dalla rilevazione ISTAT sulle tecnologie dell'informazione e della comunicazione nelle imprese, contenendo una sezione specifica sull'IA. Tale sezione fornisce interessanti indicazioni sullo stato dell'adozione di queste tecnologie; manca però una vista sulle imprese che sviluppano tecnologia e forniscono servizi e/o prodotti con forte contenuto di IA. Si propone dunque una estensione del questionario nella specifica direzione indicata.

- Impatto delle iniziative sull'azione strategica I.2, caratterizzando in particolare le PMI coinvolte nei facilitatori e l'efficacia degli stessi nel promuovere lo sviluppo e l'adozione di soluzioni di IA, nell'ottica di efficientare e trasformare i processi delle imprese.

- Numero di imprese start-up create con focus sull'IA e numero di imprese attive nello sviluppo di tecnologie di IA. Tale indicatore è, infatti, rilevante per monitorare l'impatto della strategia sul contesto produttivo che agisce da abilitatore per l'adozione di soluzioni IA nel settore industriale e nelle PMI.

[23] *Si vedano, ad esempio, le riviste Quantitative Science Studies (ISSN 2641-3337), Scientometrics (ISSN 0138-9130), Journal of Informetrics (ISSN 1751-1577).*

ORGANI REGOLATORI

Contesto di riferimento

Il regolamento europeo sull'intelligenza artificiale (AI Act) istituirà un quadro giuridico uniforme volto a regolare lo sviluppo, la commercializzazione e l'uso dei sistemi di intelligenza artificiale in conformità con i valori e i diritti costituzionali dell'UE. L'AI Act mira a regolare l'intelligenza artificiale attraverso il cosiddetto *risk-based approach* che distingue più o meno elevati obblighi di conformità a seconda del rischio (basso, medio o elevato) che software e applicazioni intelligenti possono causare a danno dei diritti fondamentali. Più alto è il rischio e maggiori sono gli oneri di compliance e le responsabilità degli autori delle applicazioni intelligenti. Escludendo poi che l'intelligenza artificiale possa essere impiegata per alcune finalità individuate dalla stessa normativa considerate contrarie ai valori dell'UE (ad es. il social scoring). Dopo la pubblicazione ufficiale, la disciplina europea necessiterà di circa due anni per essere applicata: così da consentire il complesso adeguamento da parte degli operatori.

Per quanto emerge dalle attuali versioni del regolamento verranno istituite più Autorità chiamate a vigilare e attuare la normativa in materia di IA, distinguendo per competenze e funzioni: il livello europeo (art. 56) e quello nazionale (art. 59). L'Autorità europea avrà anzitutto la finalità di coordinare l'applicazione della disciplina nonché l'attività delle Autorità nazionali. Un ruolo che si tradurrà in un importante redazione di linee guida e best practices a supporto anche di sviluppatori e utilizzatori di questa tecnologia. Una funzione anzitutto coordinatrice, ma inoltre chiarificatrice e di supporto a cui si unisce un ruolo di vigilanza, anche attraverso le eventuali *coordinate joint investigations*. Tuttavia, un ruolo cruciale sarà svolto dalle Autorità nazionali, che secondo l'AI Act "ciascuno Stato membro istituisce o designa".

In particolare, dal regolamento emergono due funzioni principali rimesse al livello nazionale: la funzione di vigilanza e quella di notificazione. Astraendo dagli specifici dettagli, la prima è volta a controllare che l'AI Act sia rispettato da parte dei produttori e distributori di sistemi di IA; la funzione di notificazione invece richiama la verifica di regolarità delle attività di certificazioni rilasciate da soggetti terzi a chi crea sistemi di intelligenza artificiale che rientrano nelle categorie ad alto rischio. Il regolamento prevede che le Autorità nazionali dovranno essere soggetti con una forte specializzazione tecnica, istituite attraverso fonte primaria nazionale coordinata con l'ordinamento europeo.

Agenzia di vigilanza italiana

Alla luce del quadro sopra delineato, l'Autorità definita nell'ambito del quadro regolatorio europeo, potrà essere definita in Italia in termini di una Agenzia, con un ruolo di vigilanza e notificazione. In tal senso si pongono quantomeno due ordini di problemi, dai quali dipenderà lo spazio e la competitività dei sistemi di Intelligenza Artificiale sviluppati in Italia. Anzitutto, il supporto di chi sviluppa, distribuisce o implementa l'IA nella comprensione e attuazione della complessa normativa europea e nazionale. L'Agenzia dovrà porsi grazie alle sue competenze giuridiche e tecnologiche come privilegiato interlocutore affinché l'Italia sostenga l'industria digitale o il sistema produttivo che intenda adottare sistemi di IA, in stretta sinergia con la Fondazione per l'attuazione, il coordinamento e il monitoraggio (di cui all'Azione A.3). Sempre a vantaggio del sistema produttivo, l'Agenzia dovrà operare un'attività di orientamento nell'ambito dell'ordinamento giuridico.

L'AI Act, infatti, interessa numerosi ambiti giuridici già regolati e nei quali già operano altre Autorità con i loro differenti indirizzi per specificità di settori: la data protection e la competenza del Garante privacy; la tutela dei consumatori e la disciplina del mercato dei servizi digitali (inoltre interessato dal recente Digital Market Act) di competenza di AGCM; il contrasto dei con-tenuti digitali dannosi – anche ai sensi del Digital Services Act – di competenza di AGCOM. Inoltre, la materia bancaria e finanziaria che in ambito di intelligenza artificiale l'AI Act lascia alla competenza della BCE e in ambito nazionale di Banca d'Italia e Consob. Insomma, un quadro complesso, una over regulation complicata da sovrapposizioni di discipline e competenze tra Autorità che già rappresenta un problema e che appunto l'Agenzia dovrà aiutare a semplificare consentendo un'applicazione intellegibile, che favorisca il sistema produttivo e l'innovazione.

L'Agenzia dovrà altresì siglare protocolli e mantenere una stretta collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), in considerazione del cruciale ruolo che riveste l'IA nel settore e delle ripercussioni sul piano dell'adeguamento normativo (basti pensare, ad esempio, alle emergenti problematiche dell'attribuzione della responsabilità di attacchi cyber mediante l'utilizzo di strumenti di IA). D'altra parte, l'agenzia di vigilanza e l'ACN dovranno essere necessariamente differenziati e indi-pendenti: anzitutto, perché attuativi di due differenti apparati normativi, ma soprattutto dovranno essere indipendenti per l'alta specializzazione e complessità delle peculiari funzioni distintamente assegnate dal legislatore europeo, definendo precisi e stretti legami di collaborazione affinché i sistemi di IA possano sempre garantire i massimi livelli di affidabilità, integrità, disponibilità e sicurezza della tecnologia nazionale implementata.

AGID Agenzia per l'Italia Digitale