

dossier

XIX Legislatura

14 aprile 2025

Disposizioni e deleghe al Governo in materia di intelligenza artificiale

A.C. 2316



Senato
della Repubblica



Camera
dei deputati



SERVIZIO STUDI

TEL. 06 6706-2451 - ✉ studi1@senato.it – ✕ [@SR_Studi](https://www.instagram.com/SR_Studi)

Dossier n. 289/2



SERVIZIO STUDI

Dipartimento Trasporti

Tel. 06 6760-2614 - ✉ st_trasporti@camera.it – ✕ [@CD_trasporti](https://www.instagram.com/CD_trasporti)

Dipartimento Attività Produttive

Tel. 06 6760-3403 - ✉ st_attprod@camera.it – ✕ [@CD_attprod](https://www.instagram.com/CD_attprod)

Progetti di legge n. 305/2

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

ID0010b.docx

INDICE

PREMESSA	3
-----------------------	----------

SCHEDE DI LETTURA

CAPO I – PRINCIPI E FINALITÀ ’	9
---	----------

- Articolo 1 (*Finalità e ambito di applicazione*).....9
- Articolo 2 (*Definizioni*)11
- Articolo 3 (*Principi generali*).....13
- Articolo 4 (*Principi in materia di informazione e di dati personali*).....15
- Articolo 5 (*Principi in materia di sviluppo economico*)17
- Articolo 6 (*Sicurezza e difesa nazionale*).....19

CAPO II – DISPOSIZIONI DI SETTORE	24
--	-----------

- Articolo 7 (*Uso dell’intelligenza artificiale in ambito sanitario e di disabilità*)24
- Articolo 8 (*Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario*)28
- Articolo 9 (*Trattamento dati personali per finalità di ricerca e sperimentazione*)34
- Articolo 10 (*Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale*).....38
- Articolo 11 (*Disposizioni sull’uso dell’intelligenza artificiale in materia di lavoro*).....43
- Articolo 12 (*Osservatorio sull’adozione di sistemi di intelligenza artificiale nel mondo del lavoro*)46
- Articolo 13 (*Disposizioni in materia di professioni intellettuali*)48
- Articolo 14 (*Uso dell’intelligenza artificiale nella pubblica amministrazione*).....50
- Articolo 15 (*Impiego dei sistemi di intelligenza artificiale nell’attività giudiziaria*)55
- Articolo 16 (*Delega al Governo in materia di dati, algoritmi e metodi matematici per l’addestramento di sistemi di*

<i>intelligenza artificiale)</i>	60
▪ Articolo 17 (<i>Modifiche al codice di procedura civile</i>).....	62
▪ Articolo 18 (<i>Uso dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale</i>).....	64
CAPO III – STRATEGIA NAZIONALE, AUTORITÀ NAZIONALI E AZIONI DI PROMOZIONE.....	66
▪ Articolo 19 (<i>Strategia nazionale per l'intelligenza artificiale</i>)	66
▪ Articolo 20 (<i>Autorità nazionali per l'intelligenza artificiale</i>)	69
▪ Articolo 21 (<i>Applicazione sperimentale dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale</i>).....	74
▪ Articolo 22 (<i>Misure di sostegno per il rientro in Italia dei lavoratori, i giovani e lo sport</i>)	79
▪ Articolo 23 (<i>Investimenti nei settori di intelligenza artificiale, della cybersicurezza e calcolo quantistico</i>)	86
▪ Articolo 24, commi 1, 2 e 6 (<i>Delega al Governo per l'adeguamento della normativa nazionale al regolamento dell'Unione europea in materia di intelligenza artificiale</i>)	92
▪ Articolo 24, commi 3-5 (<i>Delega per la definizione organica della disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite</i>)	120
CAPO IV – DISPOSIZIONI A TUTELA DEGLI UTENTI E IN MATERIA DI DIRITTO D'AUTORE	123
▪ Articolo 25 (<i>Tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale</i>).....	123
CAPO V – DISPOSIZIONI PENALI	126
▪ Articolo 26 (<i>Norme penali</i>)	126
▪ Articolo 26, commi da 2 a 4 (<i>Modifiche alla disciplina dei reati di aggrigotaggio, plagio e manipolazione del mercato</i>)	133
CAPO VI – DISPOSIZIONI FINANZIARIE E FINALI	140
▪ Articolo 27 (<i>Clausola di invarianza finanziaria</i>).....	140
▪ Articolo 28, comma 1 (<i>Funzioni dell'Agenzia per la cybersicurezza nazionale</i>)	141
▪ Articolo 28, comma 2 (<i>Obblighi di notifica di incidenti</i>)	143

PREMESSA

Il disegno di legge di iniziativa governativa recante disposizioni e deleghe al Governo in materia di **intelligenza artificiale** (A.C. 2316) è stato presentato al Senato della Repubblica in data 20 maggio 2024, approvato in prima lettura il 20 marzo 2025 e quindi trasmesso alla Camera dei deputati dove è stato assegnato alle Commissioni riunite IX Trasporti e telecomunicazioni e X Attività produttive.

Il testo è teso a introdurre una normativa nazionale che predisponga un sistema di principi di *governance* e misure specifiche adatte al contesto italiano per mitigare i rischi e cogliere le opportunità dell'intelligenza artificiale.

Difatti, il contesto economico nel quale il provvedimento si inserisce è caratterizzato da una significativa crescita del mercato nazionale. Secondo il [rapporto](#) dell'Osservatorio *Artificial Intelligence* del Politecnico di Milano, aggiornato a febbraio 2025, nel **2024 il mercato dell'intelligenza artificiale** ha raggiunto i **1,2 miliardi di euro** con una crescita del **+58 per cento rispetto al 2023**. Un'analisi più approfondita rivela come l'**intelligenza artificiale generativa**, che include soluzioni innovative tra cui i modelli linguistici avanzati e le tecnologie di creazione automatica, è il principale fattore di traino, in quanto tali soluzioni rappresentano il **43 per cento** del mercato. Il restante **57 per cento** è costituito in prevalenza da soluzioni di **AI tradizionale**, che comprende applicazioni consolidate come *machine learning* e il riconoscimento vocale e visivo.

Tuttavia, persistono difficoltà nel far **crescere realtà imprenditoriali innovative**, nell'adozione delle soluzioni di intelligenza artificiale delle PMI, in quanto solo il **7 per cento** delle piccole e il **15 per cento** delle medie imprese ha avviato progetti, nonché nella lenta integrazione della Pubblica Amministrazione che, nonostante un tasso di crescita anno su anno superiore al **100 per cento**, contribuisce al **6 per cento** del mercato.

In questo contesto, merita citare uno [studio](#) di ottobre 2024, commissionato da Google e condotto da *Implement Consulting Group*, secondo cui l'adozione su larga scala dell'IA generativa potrebbe **incrementare il Prodotto Interno Lordo (PIL)** dell'Italia di 150-170 miliardi di euro l'anno nei prossimi dieci anni, pari quindi ad una **crescita complessiva dell'8 per cento**. Tuttavia, un **ritardo**, di soli cinque anni,

nello sviluppo di queste tecnologie, **ridurrebbe** il potenziale di **crescita economica** in Italia al *2 per cento*.

Il largo utilizzo di soluzioni di intelligenza artificiale, oltre a offrire una serie di opportunità, ha aperto un dibattito sui **rischi** che derivano dal suo impiego e sulle nuove sfide, etiche e giuridiche, che l'IA pone per le libertà delle persone e la stabilità delle democrazie.

In quest'ottica si collocano le numerose iniziative normative avviate a livello internazionale, europeo e nazionale, volte a dar vita ad una **regolamentazione tempestiva e tecnologicamente neutrale**, capace di disciplinare gli usi dell'IA nei vari settori della società, che consenta ai cittadini, alle istituzioni e alle imprese di sfruttare appieno i benefici di questi nuovi strumenti e che garantisca un'adeguata tutela degli interessi nazionali e dei principi fondamentali come la protezione dei diritti umani, la *privacy*, la sicurezza, l'equità e la trasparenza.

Il presente disegno di legge, quale fonte nazionale, si affianca al [Regolamento \(UE\) 2024/1689](#), meglio conosciuto come "*AI Act*", del 13 giugno 2024.

Secondo i principi stabiliti dalla Corte di giustizia del Lussemburgo e dalla stessa Corte costituzionale italiana (a partire dalla sentenza cosiddetta *Granital*, n. 170 del 1984) il Regolamento ha preminenza sulla legge italiana. Questa, pertanto, si intende rivolta agli aspetti tipici della realtà socio-economica nazionale e ai profili non espressamente coperti dalla normativa unionale e a quelli che quest'ultima rimette proprio alla disciplina dei singoli Stati membri.

In particolare, l'*AI Act* mira a promuovere lo sviluppo e l'adozione di sistemi di intelligenza artificiale sicuri e affidabili nel mercato unico dell'UE da parte di soggetti pubblici e privati, attraverso un modello di *governance* armonizzato basato sulla **classificazione dei rischi** di questi sistemi.

A tale riguardo, si ricorda che, in fase ascendente, le Commissioni IX Trasporti e telecomunicazioni e la X Attività produttive, nella scorsa – XVIII - legislatura, hanno esaminato la proposta di regolamento, esprimendo le proprie valutazioni in esito alla seduta del 13 aprile 2022 (qui il [parere approvato](#)), cui la Commissione europea ha dato riscontro il 12 ottobre 2022). Per ulteriori raggugli sulla proposta, si rimanda al relativo [dossier](#).

Il presente disegno di legge, peraltro, si inserisce nel solco di attività (governative e parlamentari) precedenti e contemporanee all'esame dell'*AI Act*.

Il primo filone consiste nell'impegno del governo che, sulla base delle linee del Libro Bianco sull'IA della Commissione europea, a partire dal **2020** ha elaborato una **Strategia Nazionale per l'IA** (Ministero delle imprese e del made in *Italy*), che si inserisce nel quadro del Piano Coordinato Europeo per l'IA, e va collocata nell'ambito di un'azione sinergica tra Stati membri dell'UE e istituzioni comunitarie. A tale riguardo, il 22 luglio 2024, è stato pubblicato il documento completo della [Strategia Italiana per l'Intelligenza Artificiale 2024-2026](#), che identifica **tre macro obiettivi strategici**, quali: i) sostenere la realizzazione e l'adozione di applicazioni di IA per supportare pratiche gestionali, modelli produttivi e progetti di innovazione; ii) promuovere le attività di ricerca scientifica funzionale e applicata; iii) valorizzare il capitale umano attraverso la formazione e la crescita di talenti in possesso delle necessarie competenze.

Il secondo filone è di natura parlamentare, ed è costituito dall'intensa **attività conoscitiva** svolta – in questa legislatura – da vari organi della Camera dei deputati e precisamente:

- il **Comitato di vigilanza sulla documentazione**, costituito all'interno dell'**Ufficio di Presidenza della Camera**, che ha presentato il [proprio Rapporto](#) il 14 febbraio 2024;
- la **Commissione X – Attività produttive**, la quale ha svolto un'indagine conoscitiva, approvando il relativo [documento conclusivo](#) nella seduta del 24 aprile 2024;
- la **Commissione XI – Lavoro**, la quale ha, a sua volta, avviato un'indagine conoscitiva sugli aspetti di propria competenza, approvando il relativo [documento conclusivo](#) nella seduta del 19 marzo 2025.

Il provvedimento, dunque, anche a seguito delle **modifiche introdotte nel corso dell'esame al Senato**, si compone di **28 articoli**, atti a sostenere e promuovere lo sviluppo di sistemi di intelligenza artificiale che, in armonia con l'apposito regolamento europeo, e gli indirizzi governativi e parlamentari nazionali, siano basati su una visione antropocentrica, nonché su principi di trasparenza, responsabilità, equità e rispetto per i diritti fondamentali, che garantiscono un equilibrio tra le opportunità che offrono le nuove tecnologie e i rischi legati al loro uso improprio, al loro impiego dannoso e anche al loro sottoutilizzo.

In particolare, le norme si articolano in cinque capi:

- **Capo I - Principi e Finalità**. Questo capo stabilisce i principi fondamentali per l'uso dell'intelligenza artificiale, anche nei settori

produttivi e di difesa, promuovendo un approccio trasparente e rispettoso dei diritti fondamentali. Reca, inoltre, una serie di definizioni, riprese dall'ordinamento europeo, di termini usati nel testo.

- **Capo II - Disposizioni di Settore.** Il capo disciplina l'applicazione dell'IA in ambiti specifici come il sistema sanitario, la ricerca scientifica, il lavoro, la pubblica amministrazione e l'attività giudiziaria, promuovendo adeguate tutele di trattamento e protezione dei dati personali e regolando l'uso di questi strumenti per garantire che non si verifichino discriminazioni. Inoltre, contiene, all'articolo 16, una delega al governo per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento dei sistemi di IA.
- **Capo III - Strategia Nazionale, Autorità Nazionali e Azioni di Promozione.** Questo capo detta le misure inerenti alla redazione e aggiornamento della Strategia nazionale per l'IA, specificando che essa deve favorire le collaborazioni pubblico-private e promuovere la ricerca e la formazione. Inoltre, l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) sono designate, all'articolo 20, quali autorità nazionali per l'intelligenza artificiale, che sono dunque responsabili di garantire l'applicazione e l'attuazione della normativa nazionale ed unionale. È prevista inoltre una delega al governo per l'adeguamento della normativa nazionale all'*AI Act*.
- **Capo IV - Disposizioni a Tutela degli Utenti e in Materia di Diritto d'Autore.** Il capitolo prevede misure per proteggere gli utenti nell'uso dell'IA, assicurando la tutela della privacy e dei diritti d'autore, inclusa la regolamentazione dell'uso dell'IA per la creazione e manipolazione di contenuti. È inclusa una modifica alla legge sul diritto d'autore per estendere la protezione anche alle opere create con l'ausilio dell'IA.
- **Capo V - Disposizioni Penali.** In questo capo si prevede l'introduzione di modifiche al codice penale per punire l'uso illecito dell'IA. Si introduce la responsabilità penale per chi diffonde contenuti generati con IA in modo ingannevole, e per chi utilizza l'IA in modo da compromettere la sicurezza o l'integrità di persone o sistemi.
- **Capo VI - Disposizioni Finanziarie e Finali.** Il capo finale reca la clausola di invarianza finanziaria, nonché ulteriori disposizioni finali, tra cui la possibilità per l'ACN di concludere accordi di collaborazione con soggetti privati.

Schede di lettura

CAPO I – PRINCIPI E FINALITÀ

Articolo 1 (Finalità e ambito di applicazione)

L'**articolo 1** enuncia finalità ed ambito di applicazione della disciplina prevista dal disegno di legge, con sottolineatura della dimensione antropocentrica dell'utilizzo dell'intelligenza artificiale e della vigilanza sui rischi economici e sociali nonché sull'impatto in ordine ai diritti fondamentali.

Il disegno di legge in esame, dunque, detta, all'inizio del proprio articolato, le disposizioni di natura finalistica che motivano l'adozione del provvedimento, partendo dalla consapevolezza della rivoluzione informatica che, dal secondo Novecento, ha assunto una incidenza sulla vita individuale e collettiva tale da configurare una 'società digitale', in cui la diffusione del *personal computer*, l'avvento di *internet* e degli *smartphone*, hanno dilatato l'impiego di strumenti digitali nella quotidianità. In questo contesto, l'evoluzione tecnologica fa sì che le 'macchine' dispongano ormai di margini di auto-apprendimento, auto-organizzazione, auto-decisione. Ne segue che si pone all'etica, al diritto, al dibattito pubblico il tema della 'intelligenza artificiale' e di una sua regolazione.

In tale direzione muove il regolamento dell'Unione europea sull'intelligenza artificiale, approvato in via definitiva a metà 2024 (regolamento UE 2024/1689 del Parlamento e del Consiglio del 13 giugno 2024, che "stabilisce regole armonizzate sull'intelligenza artificiale" c.d. *AI Act*).

E a livello nazionale si colloca il disegno di legge in esame, volto – specifica il suo **articolo 1** – a disporre norme generali – "principi" – relativamente ai **sistemi e modelli di intelligenza artificiale**, con riguardo alla loro ricerca, sperimentazione, sviluppo, adozione e applicazione.

La disciplina che si viene a profilare persegue una duplice finalità.

Si mira da un lato a un utilizzo "corretto, trasparente e responsabile", in una **dimensione antropocentrica**, di questa strumentazione tecnologica, onde coglierne le opportunità.

Si intende, dall'altro, "garantire" la **vigilanza** sui rischi economici e sociali e sull'impatto sui **diritti fondamentali**.

Le disposizioni così poste si interpretano e si applicano conformemente al diritto dell'Unione europea, e in particolare al ricordato regolamento (UE) n. 1689 del 2024 (c.d. *AI Act*).

L'Unione europea ha approntato strumenti regolatori su più ambiti caratterizzati dalla digitalizzazione, quali la protezione dei dati personali, i diritti sui dati e contenuti digitali, la responsabilità dei fornitori di servizi digitali, la concorrenza dei mercati digitali, il commercio elettronico.

Con specifico riguardo all'intelligenza artificiale, un apposito [regolamento](#) è stato approvato dal Parlamento europeo (il 13 marzo 2024) e dal Consiglio (il 21 maggio 2024).

Per la sua sintesi v. *infra* la scheda di lettura relativa all'articolo 22 del presente disegno di legge, il quale reca delega al Governo per l'adeguamento della normativa interna alle disposizioni appunto di quel regolamento.

Articolo 2 (Definizioni)

L'**articolo 2, modificato nel corso dell'esame al Senato**, reca le definizioni dei vocaboli utilizzati all'interno del provvedimento, quali:

- “**sistemi di intelligenza artificiale**”;
- “**dato**”;
- “**modelli di intelligenza artificiale**”.

Il **comma 2**, specifica che per ulteriori definizioni, non espressamente citate, si rimanda a quanto contenuto nell'*AI Act*.

L'**articolo 2** si compone di **due commi**, di cui il **primo** riporta le seguenti definizioni, riprese dal **diritto dell'Unione europea**, che sono utilizzate nel provvedimento in esame.

In particolare, la **lettera a)**, **modificata nel corso dell'esame al Senato**, indica che la definizione di **sistema di intelligenza artificiale** è la medesima contenuta nell'**articolo 3, comma 1, numero 1) dell'*AI Act***. Pertanto, con tale termine, si intende 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.

La **lettera b)** introduce la definizione di **dato**, considerato come qualsiasi **rappresentazione digitale di atti, fatti o informazioni** e qualsiasi **raccolta** di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva.

Tale definizione è presa dal regolamento (UE) 2022/868, cosiddetto *Data governance Act*.

Infine, la **lettera c)**, **modificata nel corso dell'esame al Senato**, riporta la definizione di **modelli di intelligenza artificiale**, di cui all'**articolo 3, comma 1, numero 63) dell'*AI Act***. In particolare, il dettato europeo definisce un “**modello di IA per finalità generali**”; come un “modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'auto-supervisione su larga scala, che sia caratterizzato da

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 che sono utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato”.

Il comma **2, introdotto nel corso dell’esame al Senato**, specifica che per quanto non espressamente previsto si rimanda alle definizioni contenute nel [AI Act](#).

Articolo 3 (Principi generali)

L'**articolo 3** definisce i principi generali della disciplina posta dal disegno di legge.

Vi è ricompreso il rispetto dei diritti fondamentali, delle libertà, dello svolgimento con metodo democratico della vita istituzionale e politica.

La disciplina prevista dal disegno di legge ha quale ambito di applicazione – si è ricordato trattando dell'articolo 1 – la ricerca, sperimentazione, sviluppo, adozione, applicazione ed utilizzo di sistemi e di modelli di intelligenza artificiale.

Sono modelli di intelligenza artificiale “per finalità generali”.

Si ricorda che nella definizione resa dall'*AI Act* sull'intelligenza artificiale, essi sono quei modelli di intelligenza artificiale che, anche là dove addestrati con grandi quantità di dati utilizzando l'auto-supervisione su larga scala, presentino una generalità significativa e siano in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello sia immesso sul mercato, e che possano essere integrati in una varietà di sistemi o applicazioni a valle (ad eccezione dei modelli utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato).

L'**articolo 3** prescrive loro alcuni obblighi. Sono:

- ✓ il rispetto dei **diritti fondamentali** e delle **libertà** previsti dall'ordinamento italiano ed europeo;
- ✓ il rispetto dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità (**comma 1**);
- ✓ la correttezza, attendibilità, sicurezza, qualità, appropriatezza e trasparenza, secondo il principio di proporzionalità, dei dati e processi su cui si sviluppa l'intelligenza artificiale (**comma 2**);
- ✓ il rispetto dell'autonomia e del potere decisionale umani;
- ✓ la prevenzione del danno;
- ✓ la conoscibilità e spiegabilità (**comma 3**).

Si prescrivono altresì:

- ✓ la trasparenza;
- ✓ l'assicurazione della sorveglianza e del controllo umani;
- ✓ l'esercizio delle funzioni e competenze delle “istituzioni territoriali”, sulla base dei principi di autonomia e sussidiarietà.

L'utilizzo di sistemi di intelligenza artificiale non deve recare pregiudizio allo svolgimento con metodo democratico della vita istituzionale e politica (**comma 4**).

Le disposizioni della presente legge si intendono 'ricettive' del dispositivo *dell'AI Act*. Dunque non si hanno obblighi altri rispetto a quelli posti da quella fonte (specifica il **comma 5**).

Il **comma 6** prescrive la cybersicurezza (protezione dagli attacchi informatici) lungo l'intero ciclo di vita dei sistemi e modelli di intelligenza artificiale, sulla base del rischio e con specifici controlli di sicurezza, con riguardo tra l'altro ai tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.

Infine il **comma 7** dispone che l'accesso delle persone con disabilità avvenga su base di uguaglianza e senza alcuna forma di discriminazione e di pregiudizio (in conformità alle disposizioni della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, fatta a New York il 13 dicembre 2006, ratificata e resa esecutiva in Italia con la legge n. 18 del 2009).

Articolo 4 *(Principi in materia di informazione e di dati personali)*

L'**articolo 4** reca principi specifici, in materia di informazione e di riservatezza dei dati personali.

Inoltre reca previsione relativa all'accesso dei minori alle tecnologie di intelligenza artificiale (differenziando a seconda che abbiano o meno compiuto quattordici anni).

L'**articolo 4** reca taluni specifici principi, per un duplice riguardo: l'informazione; i dati personali.

Per quanto concerne l'**informazione**, l'utilizzo di sistemi di intelligenza artificiale non deve pregiudicare:

- ✓ la libertà e il pluralismo dei mezzi di comunicazione;
- ✓ la libertà di espressione;
- ✓ l'obiettività, completezza, imparzialità e lealtà dell'informazione (**comma 1**).

Per quanto riguarda i **dati personali**, deve esserne garantito:

- ✓ il trattamento lecito, corretto e trasparente dei dati personali;
- ✓ la compatibilità con le finalità per le quali sono stati raccolti, in conformità con il diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza (**comma 2**).

Si estendono pertanto all'ambito dell'intelligenza artificiale i principi vigenti in materia di riservatezza dei dati personali.

Ancora, le informazioni e le comunicazioni connesse all'utilizzo di sistemi di intelligenza artificiale, se relative al trattamento dei dati, debbono essere rese con linguaggio "chiaro e semplice", in modo da garantire all'utente la conoscibilità dei correlativi rischi nonché il diritto di opporsi ai "trattamenti autorizzati" dei propri dati personali (**comma 3**).

Specifica disposizione detta il **comma 4** per l'accesso dei **minori** alle tecnologie di intelligenza artificiale.

In particolare, per i minori **infra-quattordicenni**, si prescrive il **consenso** di chi eserciti la responsabilità genitoriale.

Per i minori che abbiano **compiuto quattordici anni**, è prevista la **facoltà** di esprimere il proprio consenso al trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili.

Siffatta disciplina ‘ricalca’ quella vigente circa il consenso del minore al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione (cfr. l'articolo 2-*quinqües* del decreto legislativo n. 196 del 2003 recante il Codice in materia di protezione dei dati personali, come novellato dal decreto legislativo n. 101 del 2018).

Articolo 5 *(Principi in materia di sviluppo economico)*

L'**articolo 5** prevede che lo Stato e le altre autorità pubbliche **promuovano l'utilizzo dell'intelligenza artificiale (IA) per migliorare la produttività e la competitività** del sistema economico nazionale, favoriscano un mercato dell'IA innovativo, equo, aperto e concorrenziale, facilitino la **disponibilità di dati di alta qualità** per le imprese che sviluppano o utilizzano sistemi di IA, indirizzino le piattaforme di *e-procurement* delle pubbliche amministrazioni a scegliere fornitori di sistemi e modelli di IA che garantiscono una **localizzazione ed elaborazione dei dati critici presso data center sul territorio nazionale ed elevati standard di trasparenza**.

L'**articolo 5** stabilisce una serie di linee strategiche che lo Stato e le altre autorità pubbliche sono tenute a porre in essere. In particolare, viene disposto che essi:

a) **promuovano lo sviluppo e l'utilizzo dell'intelligenza artificiale** come strumento per **migliorare** l'interazione uomo-macchina nei settori produttivi, la **produttività** in tutte le catene del valore e le funzioni organizzative, nonché quale strumento utile all'avvio di **nuove attività economiche**, al fine di accrescere la **competitività** del sistema economico nazionale e la sovranità tecnologica della Nazione nel quadro della strategia europea;

b) **favoriscano la creazione di un mercato dell'intelligenza artificiale innovativo, equo, aperto e concorrenziale** e di ecosistemi innovativi;

c) **facilitino la disponibilità e l'accesso a dati di alta qualità** per le imprese che sviluppano o utilizzano sistemi di intelligenza artificiale e per la comunità scientifica e dell'innovazione;

d) **indirizzino le piattaforme di e-procurement delle amministrazioni pubbliche** di cui all'articolo 1, comma 2, del decreto legislativo n. 165 del 2001, in modo che, nella scelta dei fornitori di sistemi e di modelli di intelligenza artificiale, possano essere privilegiate quelle soluzioni che **garantiscono la localizzazione e l'elaborazione dei dati strategici presso data center posti sul territorio nazionale**, le cui procedure di *disaster recovery* e *business continuity* siano implementate in *data center* posti sul territorio nazionale, nonché modelli in grado di assicurare elevati standard in termini sicurezza e di trasparenza nelle modalità di addestramento e di sviluppo di applicazioni basate sull'intelligenza artificiale generativa, nel

rispetto della normativa sulla concorrenza e dei principi di non discriminazione e proporzionalità.

A seguito delle modifiche introdotte dal Senato, è stata inserita una ulteriore **lettera e)** in base alla quale deve essere favorita la ricerca collaborativa tra imprese, organismi di ricerca e criteri di trasferimento tecnologico in materia di intelligenza artificiale al fine di incoraggiare la valorizzazione economica e commerciale dei risultati della ricerca.

Ai sensi dell'articolo 1, comma 2, del decreto legislativo n. 165 del 2001, per **amministrazioni pubbliche** si intendono **tutte le amministrazioni dello Stato**, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le **aziende e amministrazioni dello Stato ad ordinamento autonomo**, le **Regioni**, le **Province**, i **Comuni**, le **Comunità montane**, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le Agenzie di cui al decreto legislativo n. 300 del 1999 e il CONI.

Articolo 6 *(Sicurezza e difesa nazionale)*

L'**articolo 6** esclude, al comma 1, dall'ambito applicativo della disciplina prevista dal presente disegno di legge, le attività connesse ai sistemi e modelli di intelligenza artificiale, condotte dagli organismi preposti alla sicurezza nazionale, alla cybersicurezza, alla difesa nazionale. Rimangono fermi peraltro alcuni loro obblighi, anche in materia di trattamento dei dati personali. Una più analitica disciplina di rango applicativo è demandata a successivi D.P.C.M. Il comma 2 – introdotto nel corso dell'esame al Senato – dispone che i sistemi di intelligenza artificiale destinati all'uso in ambito pubblico debbano essere installati su *server* ubicati nel territorio nazionale. È fatta eccezione per i sistemi di intelligenza artificiale che siano impiegati all'estero nell'ambito di operazioni militari. Ciò al fine di tutelare la “sovranità e la sicurezza dei dati sensibili dei cittadini”.

L'articolo 6 esclude dall'ambito applicativo della disciplina posta dal disegno di legge le attività connesse ai sistemi e modelli di intelligenza artificiale, se condotte a fini di **sicurezza nazionale**, di **cybersicurezza**, di **difesa nazionale**.

Il **comma 1** specifica il novero di soggetto per i quali vale l'esclusione sopra ricordata.

Sono:

- il Dipartimento delle informazioni per la sicurezza (DIS), l'Agenzia informazioni e sicurezza esterna (AISE), l'Agenzia informazioni e sicurezza interna (AISI): vale a dire gli organismi oggetto rispettivamente degli articoli 4, 6 e 7 della legge 3 agosto n. 104 del 2007, la quale disciplina il Sistema di informazione per la sicurezza della Repubblica (oltre che il segreto);
- l'Agenzia per la cybersicurezza nazionale, istituita dal decreto-legge n. 82 del 2021. Di questo, l'articolo 1, comma 1, lettere *a*) e *b*) forniscono una definizione di cybersicurezza (“l'insieme delle attività - fermi restando le attribuzioni di cui alla legge n. 124 del 2007 e gli obblighi derivanti da trattati internazionali - necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello

spazio cibernetico”) nonché di resilienza nazionale nello spazio cibernetico (“le attività volte a prevenire un pregiudizio per la sicurezza nazionale”);

- le Forze armate, per scopi di difesa nazionale;
- le Forze di polizia (ed è, questa, previsione introdotta in sede referente) “dirette a prevenire e contrastare, ai fini della sicurezza nazionale, i reati di cui all’articolo 9, comma 1, lettera *b*) e lettera *b-ter*) della legge n. 146 del 2006” (la quale ha ratificato e dato esecuzione a Convenzione e Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

Della citata legge n. 146 del 2006, l’articolo 9 dispone la non punibilità degli autori delle operazioni sotto copertura lì enumerate al comma 1.

Di quest’ultimo, la lettera *b*) menziona “gli ufficiali di polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato e dell’Arma dei carabinieri specializzati nell’attività di contrasto al terrorismo e all’eversione e del Corpo della guardia di finanza competenti nelle attività di contrasto al finanziamento del terrorismo, i quali, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo o di eversione, anche per interposta persona, compiono le attività di cui alla lettera *a*) ovvero si introducono all’interno di un sistema informatico o telematico, danneggiano, deteriorano, cancellano, alterano o comunque intervengono su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attivano identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assumono il controllo o comunque si avvalgono dell’altrui dominio e spazio informatico comunque denominato o compiono attività prodromiche o strumentali”.

La lettera *b-ter*) menziona gli ufficiali di polizia giudiziaria dell’organo del Ministero dell’interno per la sicurezza e la regolarità dei servizi di telecomunicazione (cfr. art. *7-bis*) del decreto-legge n. 144 del 2005) i quali compiano le attività sopra ricordate, nel corso di specifiche operazioni di polizia finalizzate al contrasto dei reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale.

A fronte dell’esclusione dall’ambito applicativo della disciplina che si viene a porre, rimane fermo l’obbligo del rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione nonché dello svolgimento con metodo democratico della vita istituzionale e politica.

Il comma 2 – introdotto dal Senato – dispone che i sistemi di intelligenza artificiale **destinati all’uso in ambito pubblico** debbano essere installati su **server ubicati nel territorio nazionale**. È fatta eccezione per i sistemi di intelligenza artificiale che siano impiegati all’estero nell’ambito

di operazioni militari. Ciò al fine di tutelare la “**sovranità e la sicurezza dei dati sensibili dei cittadini**”.

Al riguardo, merita rilevare che:

- l'utilizzo dell'espressione “uso in ambito pubblico” sembrerebbe fare riferimento all'”utilizzo dei sistemi di IA da parte delle **pubbliche amministrazioni** e dei soggetti che forniscono pubblici servizi”; l'espressione appare comunque suscettibile di maggiore specificazione;
- la direttiva n. 2006/123/CE (c.d. Direttiva Servizi) prescrive agli Stati membri di non restringere la libera circolazione dei servizi **imponendo requisiti relativi all'uso di attrezzature** e di materiali che costituiscono parte integrante della prestazione del servizio (articolo 16, paragrafo 2, lettera f); al tempo stesso il combinato disposto dell'articolo 16, paragrafi 1 e 3, dispone che possano essere imposti requisiti al prestatore qualora giustificati da motivi di **ordine pubblico**, di **pubblica sicurezza**, di sanità pubblica o tutela dell'ambiente, nel rispetto dei principi di non discriminazione, necessità e proporzionalità;
- il Regolamento Generale sulla Protezione dei Dati (GDPR, Regolamento n. 2016/679/UE) stabilisce che gli Stati membri non possano limitare o vietare la **libera circolazione dei dati personali** all'interno dell'Unione Europea per motivi attinenti alla protezione delle persone fisiche riguardo al trattamento dei dati personali; anche questa disposizione però prevede eccezioni ai sensi dell'articolo 23 del GDPR, il quale consente agli Stati o all'UE di imporre restrizioni ai diritti e agli obblighi previsti dal regolamento, inclusa la libera circolazione dei dati personali, attraverso misure legislative. Tali restrizioni sono ammesse per salvaguardare, tra le altre: a) la **sicurezza nazionale**; b) la **difesa**; c) la **sicurezza pubblica**;
- la formulazione della disposizione appare suscettibile di coordinamento con l'articolo 5, comma 1, lett. d), del provvedimento in esame, il quale, in luogo dell'obbligo di localizzazione dei “*server*” in territorio nazionale, pone in capo allo Stato e alle altre autorità pubbliche competenti il compito di **indirizzare** le piattaforme di *e-procurement* delle pubbliche amministrazioni a scegliere fornitori di sistemi e modelli di IA che garantiscono una localizzazione e elaborazione dei dati critici presso “*data center*” sul territorio nazionale;

I *data center* o centri di elaborazione dati (CED) sono infrastrutture fisiche in cui vengono localizzate le apparecchiature (*server*, sistemi di *storage*, etc) ed i servizi di gestione delle

risorse informatiche, ovvero l'infrastruttura IT, funzionali a uno o più fruitori (Ministero dell'ambiente e della sicurezza energetica, [Linee guida per le procedure di valutazione ambientale dei data center](#), 2024). Il *server* è un elaboratore che svolge, all'interno di una rete di calcolatori elettronici, funzioni di servizio per ogni terminale collegato (definito per questo *client*).

- la disposizione appare suscettibile di coordinamento anche con l'articolo 3, comma 5, del provvedimento in esame che esclude l'introduzione di nuovi obblighi rispetto a quelli previsti dall'*AI Act*; detto regolamento, che stabilisce requisiti specifici per i sistemi di IA ad alto rischio, non appare contemplare obblighi relativi alla localizzazione dei server utilizzati dai fornitori di l'intelligenza artificiale.

Si valuti quindi l'opportunità di un approfondimento sugli aspetti richiamati.

Il **comma 3** dispone che lo sviluppo di sistemi e modelli di intelligenza artificiale è tenuto alla correttezza, attendibilità, sicurezza, qualità, appropriatezza e trasparenza dei dati e processi, secondo il principio di proporzionalità (come prescritto dall'articolo 3, comma 2, del disegno di legge).

Specificazione del comma 3 riguarda il **trattamento dei dati personali**.

Se l'intelligenza artificiale sia utilizzata dagli organismi del sistema di sicurezza nazionale, il trattamento dei dati personali deve uniformarsi a puntuali previsioni del Codice in materia di protezione dei dati personali (decreto legislativo n. 196 del 2003), enumerate dal suo articolo 58, comma 1 (tra queste, figura il divieto (ai sensi dell'articolo 8 del decreto legislativo n. 51 del 2018, di decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge; nonché le sanzioni previste per le violazioni).

Se l'intelligenza artificiale sia utilizzata dall'Agenzia per la cybersicurezza nazionale, vale la disposizione sopra detta, nonché, in caso di elevato rischio per i diritti e le libertà delle persone fisiche, l'effettuazione di una valutazione d'impatto sulla protezione dei dati e la consultazione preventiva del Garante (secondo quanto dispongono gli articoli 23 e 24 del decreto legislativo n. 51 del 2018, cui fa rinvio l'articolo 58, comma 2, del Codice in materia di protezione dei dati personali, cui fa a

sua volta rinvio l'articolo 13 del decreto-legge n. 82 del 2021, richiamato dalla disposizione in esame).

Infine il **comma 4** demanda a **regolamento** adottato con DPCM (anche in deroga a quanto previsto dalla legge n. 400 del 1988) previo parere del Comitato parlamentare per la sicurezza della Repubblica e sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), la definizione delle modalità di svolgimento della attività connesse all'intelligenza artificiale, svolte dagli organismi sopra ricordati componenti il Sistema di informazione per la sicurezza della Repubblica, o delle attività loro funzionali, svolte da altri soggetti pubblici e privati esclusivamente per scopi di sicurezza nazionale.

Per le attività svolte dall'Agenzia per la cybersicurezza nazionale è previsto analogo regolamento, adottato con DPCM, su proposta del direttore generale dell'Agenzia (anche in deroga alla legge n. 400 del 1988 ed alle norme in materia di contratti pubblici), previo parere del Comitato parlamentare per la sicurezza della Repubblica e sentito il Comitato interministeriale per la cybersicurezza (CIC).

CAPO II – DISPOSIZIONI DI SETTORE**Articolo 7**

(Uso dell'intelligenza artificiale in ambito sanitario e di disabilità)

L'articolo 7, modificato dal Senato, enuncia alcuni principi volti a regolare l'uso dei sistemi di intelligenza artificiale in ambito sanitario, con particolare riguardo al **miglioramento delle condizioni di vita delle persone con disabilità**.

In particolare, il **comma 1 prevede** che l'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione, alla diagnosi (quest'ultima espressione aggiunta **dal Senato**) e alla cura delle malattie, nel **rispetto dei diritti, delle libertà e degli interessi della persona**, anche in materia di protezione dei dati personali.

Il **comma 2 pone il divieto di condizionare l'accesso alle prestazioni sanitarie a criteri discriminatori**, tramite l'impiego di strumenti di intelligenza artificiale.

Il **comma 3, modificato dal Senato, prevede** che l'interessato ha diritto di essere informato sull'impiego di tecnologie di intelligenza artificiale.

Il **comma 4 promuove** lo sviluppo, lo studio e la diffusione di sistemi di intelligenza artificiale anche con il fine di realizzare il progetto di vita previsto dalla riforma sulla disabilità.

Il **comma 5 prevede** che i sistemi di intelligenza artificiale nell'ambito sanitario fungano da supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che deve sempre essere rimessa agli esercenti la professione medica.

Il **comma 6 stabilisce** che i sistemi di intelligenza artificiale in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati, nell'ottica di minimizzare il rischio di errori e migliorare la sicurezza dei pazienti (quest'ultima finalità è stata aggiunta **dal Senato**).

L'articolo 7, nell'evidenziare il contributo fornito dall'utilizzo di sistemi di intelligenza artificiale al potenziamento del sistema sanitario e alla prevenzione e cura delle malattie, enuncia alcuni limiti e principi in quest'ambito.

Il **comma 1 prevede** che l'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione, alla **diagnosi** (quest'ultimo riferimento è stato aggiunto in sede referente) e alla

cura delle malattie, nel **rispetto dei diritti, delle libertà e degli interessi della persona**.

Inoltre, lo stesso comma richiama tra i principi **la necessaria garanzia della protezione dei dati personali**, a cui fa riferimento più nel dettaglio l'articolo 8 del presente disegno di legge (v. *infra*).

Il **comma 2** pone il **divieto di condizionare l'accesso alle prestazioni sanitarie a criteri discriminatori**, tramite l'impiego di strumenti di intelligenza artificiale.

Il **comma 3**, modificato in sede referente, prevede che l'interessato ha diritto di essere informato sull'impiego di tecnologie di intelligenza artificiale.

A tal proposito, si ricorda che il [regolamento del Parlamento europeo e del Consiglio UE del 2024](#), cd. "*AI Act*", qualifica i sistemi di intelligenza artificiale nell'ambito dell'assistenza sanitaria come "ad alto rischio", ponendo in capo ai soggetti fornitori maggiori obblighi di informazione al fine di garantire la trasparenza nell'impiego di tali strumenti.

In specie, il regolamento europeo considera ad alto rischio un numero limitato di sistemi di intelligenza artificiale che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali, tutelati dalla Carta dei diritti fondamentali dell'Unione europea.

Prima di immettere un sistema di intelligenza artificiale ad alto rischio sul mercato dell'Unione europea, o di farlo entrare in servizio, i fornitori dovranno sottoporlo a una valutazione della conformità. Dovranno, quindi, dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersecurity e robustezza).

I sistemi di IA ad alto rischio dovranno essere tecnicamente robusti per garantire che la tecnologia sia adatta allo scopo e che i risultati falsi positivi/negativi non incidano in modo sproporzionato sui gruppi protetti (ad esempio, per origine razziale o etnica, sesso, età, ecc.).

Dovranno, inoltre, essere addestrati e testati con set di dati sufficientemente rappresentativi per ridurre al minimo il rischio di integrare distorsioni inique nel modello e garantire che, se presenti, queste possano essere risolte mediante opportune misure di rilevazione, correzione e attenuazione. Dovranno anche essere tracciabili e verificabili, garantendo la conservazione dell'opportuna documentazione, compresi i dati utilizzati per addestrare l'algoritmo, fondamentali per le indagini *ex post*.

Si impone inoltre agli operatori che siano organismi di diritto pubblico o operatori privati che forniscono servizi pubblici, nonché agli operatori che forniscono sistemi ad alto rischio di effettuare una valutazione d'impatto sui diritti fondamentali prima di mettere in uso i sistemi di intelligenza artificiale.

Con riguardo specifico all'utilizzo dei sistemi di intelligenza artificiale nell'ambito della disabilità, il **comma 4** promuove lo studio, lo sviluppo e la diffusione di sistemi di intelligenza artificiale che migliorano le condizioni di vita delle persone con disabilità, agevolano l'accessibilità, la mobilità indipendente (**questa specifica è stata introdotta dal Senato**) e l'autonomia, la sicurezza e i processi di inclusione sociale delle medesime persone anche con il fine di realizzare il progetto di vita di cui **all'articolo 2, comma 1, lett. n) del decreto legislativo n. 62 del 2024**¹ (**quest'ultimo riferimento normativo è stato introdotto dal Senato**- il testo originario del disegno di legge faceva riferimento all'articolo 2, comma 2, lettera c), della legge n. 227/2021, la legge delega in materia di riforma della disabilità).

Più nel dettaglio, tale comma individua nei sistemi di intelligenza artificiale uno strumento diretto a contribuire all'accessibilità, la mobilità indipendente e all'autonomia, alla sicurezza e ai processi di inclusione sociale delle persone con disabilità, tenuto altresì conto della finalità di elaborare un progetto di vita individuale, personalizzato e partecipato. Si intende, pertanto, prevedere forme di applicazione dei sistemi di intelligenza artificiale tra i contenuti ricompresi nel progetto di vita.

Si ricorda che la **legge n. 227/2021**, recante delega al Governo per il riassetto delle disposizioni vigenti in materia di disabilità, adottata in attuazione della **riforma 1.1**, prevista dalla **Missione 5 "Inclusione e Coesione" Componente 2 "Infrastrutture sociali, famiglie, comunità e Terzo settore" del PNRR**, ha il proprio fulcro nel progetto di vita personalizzato e partecipato diretto a consentire alle persone con disabilità di essere protagoniste della propria vita e di realizzare una effettiva inclusione nella società.

In attuazione della citata legge, è stato adottato il **decreto legislativo del 3 maggio 2024, n. 62** (per un approfondimento v. *dossier* su **A.G. n. 122**). In particolare, l'**articolo 2, comma 1, lett. n) del decreto legislativo n. 62 del 2024** fornisce la definizione di "progetto di vita", quale "progetto individuale, personalizzato e partecipato della persona con disabilità che, partendo dai suoi desideri e dalle sue aspettative e preferenze, è diretto ad individuare, in una visione esistenziale unitaria, i sostegni, formali e informali, per consentire alla persona stessa di migliorare la qualità della propria vita, di sviluppare tutte le sue potenzialità, di poter scegliere i contesti di vita e partecipare in condizioni di pari opportunità rispetto agli altri".

Più in generale, il **comma 5** prevede che i sistemi di intelligenza artificiale nell'ambito sanitario fungano da supporto nei processi di prevenzione,

¹ *Definizione della condizione di disabilità, della valutazione di base, di accomodamento ragionevole, della valutazione multidimensionale per l'elaborazione e attuazione del progetto di vita individuale personalizzato e partecipato.*

diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che deve sempre essere rimessa agli esercenti la professione medica.

Sinteticamente può qui ricordarsi che anche **l'AI Act** ha evidenziato l'importanza degli strumenti di intelligenza artificiale nell'ambito della **sicurezza e della salute pubblica**, con particolare riguardo all'individuazione delle malattie, alla diagnosi, alla prevenzione, al controllo e al trattamento e miglioramento dei sistemi di assistenza sanitaria.

Infine, il **comma 6** stabilisce che i sistemi di intelligenza artificiale in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati, nell'ottica di minimizzare il rischio di errori e **migliorare la sicurezza dei pazienti (quest'ultima finalità è stata aggiunta dal Senato)**.

Articolo 8

(Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario)

In base al **comma 1** dell'articolo in titolo, i **trattamenti di dati, anche personali**, eseguiti da determinati soggetti pubblici e privati per la **ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità terapeutica e farmacologica**, in quanto necessari ai fini della realizzazione e dell'utilizzazione di **banche dati e modelli di base**, sono **dichiarati di rilevante interesse pubblico**.

Ai fini predetti e da parte dei soggetti summenzionati, in base al successivo **comma 2**, è **consentito l'uso secondario dei dati personali privi degli elementi identificativi diretti**, anche se appartenenti alle particolari categorie indicate all'articolo 9 del regolamento (UE) 2016/679², **senza necessità di ulteriore consenso** dell'interessato e fermo restando l'**obbligo di informativa** di quest'ultimo, assolvibile con modalità semplificate. Sono fatti **salvi i casi** nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute.

In base al **comma 3** è sempre consentito, in determinati ambiti o per determinate finalità e previa informativa all'interessato, il **trattamento per finalità di anonimizzazione, pseudonimizzazione o sintetizzazione** dei dati personali, anche appartenenti alle succitate categorie particolari. E' consentito altresì il predetto trattamento finalizzato allo studio e alla ricerca **su determinati aspetti concernenti l'ambito sportivo**, nel rispetto di alcuni principi e diritti espressamente indicati.

Il **comma 4** prevede la possibile adozione di **linee guida** per le procedure di anonimizzazione di dati personali e per la creazione di dati sintetici, anche per categorie di dati e finalità di trattamento.

Ai sensi del **comma 5**, i trattamenti e usi di dati di cui ai commi 1 e 2 devono essere oggetto di **approvazione da parte dei comitati etici** interessati, nonché di **comunicazione al Garante** per la protezione dei dati personali, insieme ad una serie di informazioni; inoltre, possono essere iniziati **decorsi trenta giorni** dalla predetta comunicazione, **se non sono stati oggetto di blocco** disposto dal medesimo Garante.

Il **comma 6** precisa che **restano fermi i poteri** ispettivi, interdittivi e sanzionatori del Garante per la protezione dei dati personali.

² Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, c.d. regolamento generale sulla protezione dei dati.

Più in particolare, il **comma 1** dell'articolo in esame elenca le seguenti **finalità** di ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale, in relazione alle quali i predetti trattamenti di dati sono dichiarati di rilevante interesse pubblico: prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria e, infine, studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario.

Come sopra evidenziato, il comma in esame riconosce il **rilevante interesse pubblico** in quanto i trattamenti di dati in questione siano necessari **ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base**. Inoltre, tali trattamenti devono essere eseguiti da soggetti pubblici e privati senza scopo di lucro oppure dagli Istituti di ricovero e cura a carattere scientifico (IRCCS), nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro ovvero IRCCS.

Si ricorda che l'articolo 2 del disegno di legge in esame reca le definizioni di "sistema di intelligenza artificiale", "dato" e "modelli di intelligenza artificiale" (v. sopra la relativa scheda di lettura), ma non anche quella di "modello di base", né quella di "banca dati". Il predetto articolo 2, come modificato in sede referente, rinvia, per quanto non espressamente previsto, alle definizioni di cui al Regolamento (UE) 2024/1689 del 13 giugno 2024³. Neppure quest'ultimo Regolamento reca le definizioni di "modello di base" e di "banca dati"; reca però la definizione – per quanto qui rileva – di "modello di IA per finalità generali" (art. 3, comma 1, numero 63).

La **dichiarazione di interesse pubblico** di cui al comma in disamina è asseritamente disposta in attuazione dell'articolo 32 e **dell'articolo 33** della Costituzione, nonché in conformità a quanto previsto dall'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679.

Si ricorda che l'articolo 32 della Costituzione, tra l'altro, stabilisce che la Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività. Il successivo articolo 33 Cost. concerne, *in primis*, la libertà dell'arte e della scienza e dell'insegnamento delle stesse.

La richiamata disposizione del regolamento (UE) 2016/679 (art. 9, par. 2, lett. g)) consente il trattamento di determinate categorie di dati "sensibili" (v. *infra*), tra cui quelli relativi alla salute, se il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

³ Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale.

La disposizione richiamata precisa che il trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Il **comma 2** dell'articolo in esame tratta dell'**uso secondario dei dati personali privi degli elementi identificativi diretti**, sempre da parte dei soggetti e per le finalità di cui al precedente comma 1. Tale uso è autorizzato **anche con riferimento ai dati appartenenti alle particolari categorie indicate all'articolo 9 del regolamento (UE) 2016/679** (si tratta dei dati già individuati come "sensibili")⁴, vale a dire: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Viene precisato che: **resta fermo l'obbligo di informativa** all'interessato, che può essere assolto anche mediante messa a disposizione di un'informativa generale sul sito *web* del titolare del trattamento; **non è richiesto ulteriore consenso** dell'interessato ove inizialmente previsto dalla legge. La disposizione fa salvi, in riferimento alla prevista mancanza di elementi identificativi diretti, i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute.

La disposizione sopra descritta sull'uso secondario, secondo la relazione illustrativa del testo iniziale del provvedimento in esame, "si rende necessaria per chiarire che la finalità di ricerca medico scientifica di pubblico interesse non richiede di replicare il consenso dell'interessato (ove richiesto) se cambia l'ambito della ricerca stessa. In altri termini, se è stato prestato un consenso al trattamento di dati per la ricerca di una cura di una determinata patologia, gli stessi dati devono poter essere utilizzati senza ulteriori adempimenti salva la comunicazione al Garante per la protezione dei dati personali".

Si ricorda che, per uso secondario dei dati, si intende il trattamento di dati personali per scopi diversi da quelli per i quali i dati stessi sono stati inizialmente raccolti.

⁴ Per "dati sensibili", in base alla previgente disciplina recata dal Codice in materia di protezione dei dati personali, si intendevano i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. Ai sensi di quanto disposto dall'art. 22, comma 2, del d.lgs. 10 agosto 2018, n. 101, a decorrere dal 25 maggio 2018, l'espressione "dati sensibili" si intende riferita alle categorie particolari di dati di cui all'art. 9 del succitato Regolamento (UE) n. 2016/679.

L'articolo 14 del citato regolamento (UE) 2016/679 richiede un'informativa all'interessato, tra l'altro, qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti.

Il d.lgs.196/2003, all'articolo 110-*bis*, disciplina il trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, prevedendo che il Garante per la protezione dei dati personali possa autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del regolamento (UE) 2016/679, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, comprese forme preventive di minimizzazione e di anonimizzazione dei dati. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza. Il trattamento ulteriore di dati personali da parte di terzi per le finalità anzidette può essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati.

L'articolo 110 del d.lgs.196/2003 prevede alcuni casi nei quali il consenso dell'interessato - per il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico - non è necessario. In tali casi: il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato; il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale; il Garante per la protezione dei dati personali individua le garanzie da osservare.

Il **comma 3** stabilisce che è sempre consentito, previa informativa all'interessato, il trattamento per finalità di **anonimizzazione, pseudonimizzazione o sintetizzazione** dei dati personali, anche appartenenti alle categorie particolari di cui all'articolo 9, paragrafo 1 del Regolamento UE n.679/2016 (al riguardo v. sopra); ciò **negli ambiti di cui al comma 1** del presente articolo, **oppure** per finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale (ossia per le finalità di cui al richiamato articolo 2-

sexies, comma 2, lettera v) del decreto legislativo 196/2003). L'ultimo periodo del comma in esame, introdotto durante l'*iter* in Senato, consente il predetto trattamento finalizzato allo studio e alla ricerca **sui gesti atletici, sui movimenti e sulle prestazioni nell'attività sportiva** in tutte le sue forme, nel rispetto dei principi generali di cui al presente provvedimento e dei diritti di sfruttamento economico dei dati relativi alle attività agonistiche che spettano a chi le organizza.

Il **comma 4** prevede la **possibile adozione di linee guida** per le procedure di anonimizzazione di dati personali e per la creazione di dati sintetici, anche per categorie di dati e finalità di trattamento. Tali linee guida possono essere adottate (e aggiornate) dall'Agenzia nazionale per i servizi sanitari regionali, previo parere del Garante per la protezione dei dati personali, tenendo conto di standard internazionali e dello stato dell'arte e della tecnica.

Il **comma 5** stabilisce, in primo luogo, che i trattamenti di dati di cui ai precedenti commi 1 e 2 devono essere oggetto di approvazione da parte dei **comitati etici** interessati⁵.

In secondo luogo, prevede che detti trattamenti debbano essere **comunicati al Garante** per la protezione dei dati personali **insieme con informazioni sulle misure per assicurare la sicurezza** del trattamento e sulla **valutazione dell'impatto del trattamento** medesimo (questo, in sintesi, il senso del richiamo degli articoli 24, 25, 32 e 35 del regolamento (UE) 2016/679, operato dal comma in esame), nonché con l'indicazione espressa dei soggetti individuati quali **responsabili del trattamento**, ove presenti (v. richiamo dell'articolo 28 del medesimo regolamento (UE) 2016/679).

In terzo luogo, il comma in esame pone un **termine dilatorio per l'inizio dei trattamenti** in questione: essi possono essere iniziati **decorsi trenta giorni** dalla predetta comunicazione al Garante, **se non sono stati oggetto di blocco** disposto dal Garante medesimo.

Il **comma 6** precisa che **restano fermi i poteri** ispettivi, interdittivi e sanzionatori del Garante per la protezione dei dati personali.

Si ricorda che i poteri di indagine del Garante, quale autorità di controllo, sono previsti dall'articolo 58, co. 1, del regolamento (UE) 2016/679. Tra l'altro, spetta al Garante: di ingiungere al titolare del trattamento e al responsabile del

⁵ Si ricorda che i comitati etici sono organismi indipendenti la cui principale funzione è la valutazione degli aspetti etici e scientifici delle ricerche biomediche al fine di tutelare i diritti, la sicurezza e il benessere delle persone coinvolte. Per un approfondimento in materia si veda <https://www.issalute.it/index.php/la-salute-dalla-a-alla-z-menu/c/comitato-etico>

trattamento (e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento) di fornirgli ogni informazione di cui necessita per l'esecuzione dei suoi compiti; di ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; di ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Il predetto articolo 58, al co. 2, prevede alcuni poteri correttivi, tra i quali quello di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento, e quello di infliggere una sanzione amministrativa pecuniaria.

Il successivo co. 3 tratta invece dei poteri autorizzativi e consultivi.

L'articolo 157 del d.lgs. 196/2003, al co. 1, stabilisce che il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.

Il Garante, in base al successivo articolo 158, può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

Si ricorda, in conclusione, che nell'ambito della missione 6 (Salute) del PNRR, l'investimento M6C1 I1.2 - Casa come primo luogo di cura e telemedicina prevede anche un subinvestimento concernente le Centrali operative territoriali (COT), all'interno del quale 50 milioni di euro sono da destinare alla implementazione di un progetto pilota per i servizi di Intelligenza artificiale a supporto dell'assistenza primaria, per verificare le opportunità e i rischi relativi all'implementazione di tali strumenti all'interno del SSN.

Articolo 9 *(Trattamento dati personali per finalità di ricerca e sperimentazione)*

L'**articolo 9**, inserito nel corso dell'esame al Senato, rimette ad un decreto del Ministro della salute da emanarsi entro centoventi giorni dall'entrata in vigore della legge, sentiti il Garante per la protezione dei dati personali, gli enti di ricerca, i presidi sanitari, le autorità e gli operatori del settore, **la disciplina del trattamento dei dati personali**, anche particolari, di cui all'articolo 9 del [Regolamento \(UE\) 2016/679](#)⁶ del Parlamento europeo e del Consiglio, del 27 aprile 2016, con il massimo delle modalità semplificate consentite dal citato Regolamento, **per finalità di ricerca e sperimentazione** anche tramite sistemi di intelligenza artificiale e machine learning, inclusi la costituzione e l'utilizzo di spazi speciali di sperimentazione a fini di ricerca, anche mediante l'uso secondario dei dati personali.

L'**articolo 9**, inserito nel corso dell'esame al Senato, rimette ad un **decreto del Ministro della salute** da emanarsi entro centoventi giorni dall'entrata in vigore della legge, sentiti il Garante per la protezione dei dati personali, gli enti di ricerca, i presidi sanitari, le autorità e gli operatori del settore, la disciplina **del trattamento dei dati personali**, anche particolari, di cui all'articolo 9 del [Regolamento \(UE\) 2016/679](#)⁷ del Parlamento europeo e del Consiglio, del 27 aprile 2016, con il massimo delle modalità semplificate consentite dal citato Regolamento, **per finalità di ricerca e sperimentazione** anche tramite sistemi di intelligenza artificiale e machine learning, inclusi la costituzione e l'utilizzo di spazi speciali di sperimentazione a fini di ricerca, anche mediante l'uso secondario dei dati personali.

In proposito va ricordato che la nuova normativa sulla protezione dei dati personali risulta dalle disposizioni del [regolamento \(UE\) 2016/679](#) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione

⁶ *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)*

⁷ *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)*

delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. GDPR), nonché dalle disposizioni del Codice della privacy ([decreto legislativo n. 196 del 2003](#)), così come riformato dal [decreto legislativo n. 101 del 2018](#), recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR. Ulteriori modifiche al Codice sono state successivamente apportate attraverso il [decreto-legge n. 139 del 2021](#).

Il decreto legislativo n. 101 del 2018 è andato ad aggiungersi al [decreto legislativo n. 51 del 2018](#), con il quale l'ordinamento italiano ha attuato la [direttiva 2016/680](#), 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, completando il recepimento del c.d. pacchetto protezione dati dell'Unione europea.

Lo sviluppo dell'intelligenza artificiale e dei big data ha inoltre stimolato ulteriori interventi normativi a livello sovranazionale, al fine di assicurare il diritto alla protezione dei dati personali (e non).

Con riguardo alle **principali novità introdotte dal [Regolamento 2016/679 UE](#)** volte a dare vita ad un quadro più solido e coerente in materia di privacy si segnalano:

- l'ambito di applicazione territoriale: le norme regolamentari si applicano **anche** al trattamento di dati personali di soggetti stabiliti nell'Unione Europea da parte di un **sogetto stabilito al di fuori** della stessa;
- **la liceità del trattamento** è ancorata a due requisiti alternativi: la necessità del trattamento, o il consenso dell'interessato. Il **consenso dei minori**, in relazione ai servizi della società dell'informazione, può essere validamente espresso a partire dai 16 anni (gli Stati possono abbassare tale limite fino a 13 anni); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;
- il trattamento di "**particolari categorie di dati**" (cfr. *infra*), corrispondenti sostanzialmente a quelli che nel nostro ordinamento sono definiti come "sensibili e giudiziari". Con particolare riferimento al trattamento di dati genetici, biometrici e relativi alla salute, è consentito agli Stati membri di introdurre disposizioni più stringenti;
- l'espressa previsione sia del **diritto all'oblio** (ossia alla cancellazione definitiva dei dati trattati e conservati dal titolare del trattamento), che del diritto alla **portabilità dei dati** da un titolare del trattamento ad un altro, su richiesta degli interessati;
- la disciplina relativa al **titolare del trattamento e al responsabile del trattamento** basata sulla "**responsabilizzazione**" (*accountability*) dei suddetti soggetti – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento; viene affidato ai titolari il compito di **decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali**;
- l'introduzione del concetto di **protezione dei dati personali "by design"** e "**by default**", ossia la necessità per i titolari di adottare adeguate misure

a protezione dei dati, sia al momento della loro raccolta, che per tutta la durata del trattamento, e di usarli secondo le finalità per cui gli interessati hanno prestato il loro consenso;

- la previsione, in capo al titolare, di un obbligo di notifica all'autorità di controllo e di comunicazione all'interessato in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati (c.d. **data breach**);
- la necessità di un'analisi e una preventiva valutazione del **rischio inerente al trattamento** all'esito della quale il titolare potrà decidere, in autonomia, se iniziare il trattamento ovvero consultare l'autorità di controllo competente che non avrà il compito di autorizzare il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare;
- l'introduzione della **figura del Data protection officer** con riguardo agli enti pubblici e agli enti privati che trattino dati di natura delicata o monitorino su larga scala e in maniera sistematica gli individui;
- il nuovo sistema sanzionatorio che si fonda principalmente sulla previsione di **sanzioni amministrative pecuniarie** per molte violazioni, espressamente indicate dal Regolamento UE; si tratta di sanzioni particolarmente elevate (fino ad un massimo di € 20.000.000 o, nel caso di imprese, fino al 4% del fatturato annuo complessivo) ma definite solo nella misura massima, che dunque lasciano **ampi spazi di discrezionalità alle autorità di controllo**.

Soffermandosi più specificamente sulla ridefinizione della disciplina dei c.d. "dati sensibili", con l'entrata in vigore del Regolamento UE, tale categoria di dati sensibili, è stata assorbita nella definizione di «**categorie particolari di dati personali**», di cui al **citato articolo 9 del Regolamento medesimo**. In generale, il trattamento di questi dati - che sostanzialmente sono gli stessi già definiti "sensibili" con l'aggiunta dei dati genetici e biometrici e relativi all'orientamento sessuale - è vietato, a meno che non trovi fondamento nel consenso esplicito dell'interessato ovvero nella necessità del trattamento stesso per una serie di motivi tassativamente elencati. Per dare attuazione a questa disposizione il nuovo articolo 2-*sexies* del Codice, disciplina il trattamento delle categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante, consentendolo solo in presenza di un fondamento legislativo o regolamentare che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante. Tra i dati particolari si colloca anche la categoria dei **dati genetici, biometrici e relativi alla salute**, per il cui trattamento il regolamento UE consente agli Stati membri di introdurre garanzie supplementari, e dunque di mantenere o introdurre ulteriori condizioni, comprese limitazioni. A tal fine, il nuovo articolo 2-*septies* prevede che il trattamento di questi dati sia subordinato all'osservanza di misure di garanzia, stabilite dal Garante con provvedimento adottato con cadenza almeno biennale, a seguito di consultazione pubblica. Inoltre, l'articolo 2-*septies*, in relazione esclusiva ai dati genetici e a quelli relativi

ad ambito sanitario, diagnostico e alle prescrizioni di medicinali, prevede che nell'ambito delle misure di garanzia sia possibile anche, in caso di particolare ed elevato livello di rischio, introdurre il consenso come ulteriore misura di protezione dei diritti dell'interessato.

Articolo 10

(Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale)

L'articolo 10, modificato dal Senato, apporta modifiche al D.L. n. 179 del 2012, il cui articolo 12 detta disposizioni riguardanti il **Fascicolo sanitario elettronico**, i sistemi di sorveglianza del settore sanitario e il governo della sanità digitale, aggiungendo il nuovo articolo **12-bis in tema di intelligenza artificiale nel settore sanitario** per garantire strumenti e tecnologie avanzate in campo sanitario.

L'articolo 10 (comma 1) inserisce l'articolo 12-bis nel [D.L. n. 179 del 2012](#)⁸ (conv. con mod. dalla [L. n. 221 del 2012](#)), in tema di *Intelligenza artificiale nel settore sanitario*. Viene previsto (comma 1, art. 12-bis) che le **soluzioni di intelligenza artificiale** aventi funzione di supporto alle finalità di cui all'articolo 12, comma 2, del citato D.L. (v. *infra*), devono essere disciplinate con uno o più decreti del Ministro della salute, di concerto con l'Autorità politica delegata in materia di innovazione tecnologica e transizione digitale e con l'Autorità delegata per la sicurezza della Repubblica e cybersicurezza, sentita la Conferenza Permanente Stato-Regioni. Ciò al fine di **garantire strumenti e tecnologie avanzate nel settore sanitario**.

Si ricorda che il comma 2 dell'articolo 12 del D.L. n. 179 del 2012 prevede che il Fascicolo sanitario elettronico (FSE) è istituito con le seguenti finalità:

- a) diagnosi, cura e riabilitazione;
- a-bis) prevenzione;
- a-ter) profilassi internazionale;
- b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
- c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

Il FSE deve inoltre consentire l'accesso da parte del cittadino ai servizi sanitari *on line* secondo predeterminate modalità ovvero tramite il Portale nazionale sul Fascicolo sanitario.

Il Portale è costituito da una [pagina web](#) che consente l'accesso al cittadino mediante l'inserimento dei propri dati certificati e rispettando specifiche procedure di sicurezza. Il Governo offre inoltre una [specifica pagina web](#) in cui sono spiegate le modalità per accedere al FSE.

⁸ *Ulteriori misure urgenti per la crescita del Paese.*

Tramite i decreti approvati con la procedura indicata dalla norma, si dispone che devono essere individuati i **soggetti** che, nell'esercizio delle proprie funzioni, accedono alle **soluzioni di intelligenza artificiale** secondo le modalità definite dai medesimi decreti.

Si dispone inoltre (comma 2, art. 12-*bis*) che per il supporto alle finalità di cura, e in particolare per l'**assistenza territoriale** (v. *box*) deve essere istituita una **piattaforma di intelligenza artificiale**.

Al riguardo, la progettazione, la realizzazione, la messa in servizio e la titolarità della piattaforma vengono attribuite all'**Agenzia nazionale per i servizi sanitari regionali** (AGENAS) in qualità di **Agenzia nazionale per la sanità digitale**.

Più in dettaglio, tale piattaforma dovrà erogare i seguenti servizi di supporto:

- a) ai **professionisti sanitari** per la presa in carico della popolazione assistita **con suggerimenti non vincolanti** (quest'ultima specificazione è stata **aggiunta nel corso dell'esame al Senato**);
- b) ai **medici** nella pratica clinica quotidiana con suggerimenti non vincolanti;
- c) agli **utenti** per l'accesso ai servizi sanitari delle Case di Comunità.

Il **comma 3** dell'articolo 12-*bis*, **inserito dal Senato**, prevede che l'**AGENAS**, previa **intesa in sede di Conferenza Permanente Stato-Regioni, espliciti**, con proprio provvedimento, **i servizi di supporto** elencati al precedente comma 2 (v. *supra*).

La citata piattaforma (comma 4, art. 12-*bis*) deve essere alimentata con i **dati strettamente necessari** per l'erogazione dei servizi di cui al medesimo comma 2, che saranno trasmessi dai relativi titolari del trattamento. In proposito, si precisa che l'**AGENAS** è il soggetto **titolare del trattamento dei dati raccolti** e generati all'interno della piattaforma.

L'Agenzia, con proprio provvedimento, dopo aver acquisito i previ pareri del Ministero della salute e del Garante per la protezione dei dati personali, oltre che dell'[Agenzia per la Cybersicurezza nazionale](#), e valutato l'impatto del trattamento, **specifica i tipi di dati trattati e le operazioni eseguite all'interno della piattaforma, nonché le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e per tutelare i diritti fondamentali e gli interessi dell'interessato**, in coerenza con le disposizioni del [Regolamento UE 2016/679](#), vale a dire il **Regolamento generale sulla protezione dei dati** (comma 5, art. 12-*bis*).

Il **comma 2** dell'articolo 10 in commento prevede poi **la clausola di invarianza degli oneri finanziari**, stabilendo che dall'attuazione del

presente articolo non devono derivare nuovi o maggiori oneri per la finanza pubblica. Inoltre, si specifica che l’Agenzia nazionale per i servizi sanitari regionali (AGENAS) è chiamata a provvedere alle attività di cui al presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

• *Il Fascicolo sanitario elettronico e gli investimenti PNRR*

Il **Fascicolo Sanitario Elettronico (FSE)**, introdotto dall’art. 12 del D.L. n. 179 del 2012, costituisce l’insieme dei **dati e documenti digitali di tipo sanitario e sociosanitario** generati da eventi clinici presenti e trascorsi riguardanti l’assistito ed è alimentato in maniera continuativa dai soggetti che prendono in cura l’assistito nell’ambito del Servizio sanitario nazionale. Il FSE, istituito dalle regioni e dalle province autonome, mira al raggiungimento di diverse finalità:

- a) prevenzione, diagnosi, cura e riabilitazione;
- b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
- c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell’assistenza sanitaria.

Il [DPCM 29 settembre 2015, n. 178](#), il **regolamento di attuazione del FSE**, ha definito i contenuti del FSE, tra cui: il profilo sanitario sintetico che riassume la storia clinica dell’assistito (redatto dal medico di medicina generale o dal pediatra di libera scelta); il taccuino personale dell’assistito, sezione riservata del FSE in cui si consente all’assistito di inserire documenti relativi ai propri percorsi di cura, effettuati anche al di fuori del SSN; tutti gli elementi in materia di riservatezza dei dati come da normativa del Codice in materia di protezione dei dati personali. Le Regioni hanno assunto il compito di rendere operativo l’accesso alle informazioni per tutte le finalità sopra previste, garantendo l’interoperabilità su tutto il territorio nazionale mediante le specifiche tecniche in continuo aggiornamento (per la consultazione delle linee guida di riferimento, dei manuali e dei documenti tecnici per lo sviluppo e la gestione del Fascicolo Sanitario Elettronico si rimanda a questo [link](#)). Sulla interoperabilità del FSE è intervenuta, attraverso un apposito stanziamento, la legge di bilancio per il 2017 (art. 1, co. 382, [L. 232 del 2016](#)) disponendo, mediante l’infrastruttura del Sistema Tessera Sanitaria (v. art. 50 del [D.L. 269 del 2003](#)⁹, conv. con mod. dalla [L. 326 del 2003](#)), l’identificazione dell’assistito registrato all’Anagrafe Nazionale degli Assistiti (ANA), oltre ad una serie di servizi idonei ad interrogare il Sistema. Ulteriori disposizioni attuative sono previste dal [decreto del Ministero della salute del 7 settembre 2023](#), come da ultimo modificato dal [decreto 30 dicembre 2024](#) (G.U. n. 33 del 10/02/2025).

⁹ *Disposizioni urgenti per favorire lo sviluppo e per la correzione dell’andamento dei conti pubblici.*

L'AGID (Agenzia per l'Italia Digitale), in proposito, ha elaborato un documento per definire nel dettaglio funzionalità e obiettivi della citata Infrastruttura nazionale di interoperabilità (v. [circolare n. 4 del 1° agosto 2017](#)). Al fine di favorire l'interoperabilità tra i modelli realizzati in completa autonomia dalle regioni, la [circolare AgID n. 3 del 2 settembre 2019](#) ha introdotto il portale nazionale FSE, che costituisce un punto di accesso unico per l'intero territorio nazionale.

Più recentemente, il [decreto MEF dell'11 aprile 2024](#) e il [decreto MEF del 22 ottobre 2024](#) sono intervenuti modificando la disciplina prevista dal [decreto MEF del 4 agosto 2017](#), circa le modalità di **esercizio della facoltà di opposizione all'alimentazione automatica del Fascicolo sanitario elettronico** con i dati e documenti digitali sanitari generati da eventi clinici riferiti alle prestazioni erogate dal Servizio sanitario nazionale fino al 18 maggio 2020. Ulteriori disposizioni sulle modalità di messa a disposizione ai Fascicoli sanitari elettronici, tramite l'Infrastruttura nazionale per l'interoperabilità, dei dati del Sistema tessera sanitaria e del consenso o diniego del Sistema informativo trapianti, sono previste nel [decreto del MEF del 17 ottobre 2024](#).

L'articolo 42 del [D.L. n. 19 del 2024](#)¹⁰ (conv. con mod. dalla [L. n. 56 del 2024](#)) ha poi previsto alcune norme per il **potenziamento delle competenze** dell'Agenzia nazionale per i servizi sanitari regionali (AGENAS), in materia di Fascicolo sanitario elettronico e senza nuovi o maggiori oneri per la finanza pubblica, prevedendo che l'AGENAS **estenda l'esercizio delle proprie competenze** attualmente previste per i soli livelli centrali (Ministero del lavoro e politiche sociali e Ministero della salute) e regionali di governo, anche con riferimento allo studio e alla **ricerca scientifica** in campo medico, biomedico ed epidemiologico e relativamente alla **programmazione sanitaria**, alla verifica delle qualità delle cure ed alla valutazione dell'assistenza sanitaria che rientrano nel FSE. Tra i compiti dell'AGENAS vi rientra quello della **gestione dell'Intelligenza Artificiale** e della valutazione delle tecnologie sanitarie (*Health Technology Assessment – HTA*) relative ai dispositivi medici, nell'ambito della gestione della **piattaforma nazionale di telemedicina**. All'Agenzia si attribuiscono inoltre le attività relative alla raccolta e alla gestione dei **dati utili anche pseudonimizzati**, garantendo che gli interessati non siano direttamente identificabili, nell'ambito dell'attività di monitoraggio dell'erogazione dei servizi di telemedicina necessario per il raggiungimento degli obiettivi riconducibili al sub-intervento di investimento M6C1 1.2.3.2 “Servizi di telemedicina”, tra cui il target comunitario M6C1-9, nonché per garantire la tempestiva attuazione del sub intervento M6C1 1.2.2.4 “COT-Progetto pilota di intelligenza artificiale”.

Successivamente, i commi 317 e 318 dell'articolo 1 della legge di bilancio per il 2025 ([L. n. 207 del 2024](#)) hanno stabilito che, al fine di potenziare il **monitoraggio dell'appropriatezza prescrittiva** e di garantire la **completa alimentazione del fascicolo sanitario elettronico**, tutte le **prescrizioni** a carico del Servizio sanitario nazionale, dei Servizi territoriali per l'assistenza sanitaria al personale navigante, marittimo e dell'Aviazione civile (SASN) oltre che a carico

¹⁰ *Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza.*

del cittadino, siano effettuate nel **formato elettronico** di cui ai decreti ministeriali del MEF in materia di **dematerializzazione delle ricette mediche**. Le Regioni, nell'esercizio delle proprie funzioni di vigilanza e controllo, devono assicurare, per mezzo delle autorità competenti per territorio, l'attuazione della **completa alimentazione del FSE in formato elettronico**.

Lo sviluppo e l'utilizzo del FSE su tutto il territorio nazionale è stato considerato uno degli obiettivi da raggiungere nel nuovo disegno programmatico del PNRR (M6C2, I 1.3.1), che ha previsto una spesa di 1.379,99 milioni per il completamento dell'infrastruttura e la diffusione del Fascicolo sanitario elettronico (FSE) esistente. Il FSE espletterà tre funzioni principali: in primo luogo, conferirà maggiore autonomia ai professionisti sanitari, che potranno avvalersi di una stessa fonte di informazioni cliniche per ottenere il dettaglio dell'anamnesi del paziente; in secondo luogo, diventerà per i cittadini e i pazienti il punto di accesso ai servizi fondamentali erogati dai sistemi sanitari nazionale e regionali; in terzo luogo, le amministrazioni sanitarie avranno la possibilità di utilizzare i dati clinici per effettuare analisi cliniche e migliorare l'erogazione dell'assistenza sanitaria.

Articolo 11 *(Disposizioni sull'uso dell'intelligenza artificiale in materia di lavoro)*

L'**articolo 11** disciplina l'utilizzo dell'**intelligenza artificiale** all'interno del **mondo del lavoro**. In particolare, la norma esamina gli **obiettivi** che si intendono perseguire mediante l'impiego della nuova tecnologia - quali il **miglioramento delle condizioni di lavoro**, la **salvaguardia dell'integrità psico-fisica dei lavoratori**, l'**incremento delle prestazioni lavorative e della produttività delle persone** – prevedendo, allo stesso tempo, il **rispetto della dignità umana**, la **riservatezza dei dati personali** e la **tutela dei diritti inviolabili** dei prestatori, in conformità a quanto prescritto dal diritto europeo.

Il **comma 1** individua le finalità che deve perseguire l'utilizzo dell'intelligenza artificiale all'interno del mondo del lavoro.

In particolare, gli obiettivi richiamati riguardano:

- il miglioramento delle condizioni di lavoro;
- la salvaguardia dell'integrità psico-fisica dei lavoratori;
- l'incremento delle prestazioni lavorative e della produttività delle persone.

Si può osservare come le predette finalità valorizzino un approccio cd. **antropocentrico**, come sottolineato anche dalla Relazione Illustrativa, in conformità con quanto prescritto dalla normativa sovranazionale, in particolare dal Considerando n. 8 dell'"*AI Act*".

A tal riguardo, si ricorda che il predetto Regolamento europeo ha dettato una normativa dettagliata in materia di IA, disciplinando anche gli aspetti concernenti l'impatto della nuova tecnologia sul mercato del lavoro (per approfondimento cfr. scheda su **articolo 24, commi 2 e 6**).

Nello specifico l'allegato III del Regolamento (a cui fa espresso rinvio l'articolo 6, paragrafo 7 del medesimo atto), analizza, tra gli altri, i sistemi di IA¹¹

¹¹ In base alla definizione fornita dal Regolamento, per "sistema di IA" si intende "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" (articolo 3 Regolamento UE sull'IA).

ad alto rischio¹² nell'ambito dell'"occupazione, gestione dei lavoratori e accesso al lavoro autonomo".

In questa categoria sono, pertanto, ricompresi:

- "i sistemi di IA destinati ad 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";
- "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".

Il **comma 2** specifica che il ricorso a sistemi di IA non può ledere i diritti inviolabili¹³ della dignità umana e della riservatezza dei dati personali.

A tal riguardo l'impiego della nuova tecnologia in ambito lavorativo deve possedere i caratteri della sicurezza, dell'affidabilità e della trasparenza¹⁴.

Inoltre, con specifico riferimento a quest'ultimo elemento, la norma prevede che il datore sia tenuto a fornire al lavoratore un'informativa trasparente sugli ambiti di impiego di sistemi di IA.

La disposizione rinvia all'articolo 1-*bis* del D.Lgs. 26 maggio 1997, n. 152 per l'individuazione dei casi e delle modalità con cui il datore deve adempiere ai predetti obblighi di informazione.

Si ricorda che l'articolo 1-*bis*, appena richiamato, prevede che il datore sia tenuto ad informare il prestatore dell'utilizzo di sistemi decisionali o di monitoraggio, integralmente automatizzati, che siano in grado di fornire indicazioni in materia di: assunzione, conferimento dell'incarico, gestione e cessazione del rapporto di lavoro, assegnazione di compiti o mansioni, sorveglianza, valutazione, adempimento degli obblighi contrattuali da parte dei prestatori (comma1).

¹² Il Regolamento, in questo contesto, definisce il "rischio" come "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso" (articolo 3 Regolamento "AI Act").

¹³ Secondo quanto riportato al Considerando n. 9 del Regolamento UE: "(...) 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 (...)"

¹⁴ Sempre al Considerando n. 9 il Regolamento UE, afferma che "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".

L'articolo prescrive, inoltre, che il datore (o il committente) debba fornire le suddette informazioni "in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico". Le informazioni devono essere comunicate anche alle RSA o RSU competenti, ovvero, in mancanza, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale (comma 6).

Il **comma 3** prende in esame l'ipotesi specifica di utilizzo dell'intelligenza artificiale negli ambiti dell'organizzazione e della gestione del rapporto di lavoro.

A tal riguardo, la disposizione prescrive che, durante i suddetti impieghi dell'IA, occorre garantire i diritti inviolabili degli individui, evitando forme di discriminazione fondate sul sesso, sull'età, delle origini etniche, del credo religioso, dell'orientamento sessuale, delle opinioni politiche e sulle condizioni personali, sociali ed economiche, in conformità con il diritto dell'Unione europea¹⁵.

Attraverso tale disposizione, inoltre, vengono applicati anche al mondo del lavoro principi già espressi in via generale dall'articolo 3, comma 1, di questo stesso disegno di legge (per approfondimento cfr. scheda di lettura **articolo 3**).

¹⁵ Il Considerando n. 57 del Regolamento UE esamina puntualmente l'applicazione dei sistemi di IA sulla gestione e sull'organizzazione del mondo del lavoro. A tal riguardo si asserisce che "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 (...). 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".

Articolo 12 *(Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro)*

L'articolo 12 istituisce, presso il Ministero del lavoro e delle politiche sociali, l'Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro, al fine di contenere i rischi derivanti dall'impiego dei sistemi di IA in ambito lavorativo, massimizzando i benefici.

Per la suddetta finalità, all'Osservatorio viene attribuito il compito di **(comma 1)**:

- definire una strategia sull'utilizzo dell'intelligenza artificiale in ambito lavorativo;
- monitorare l'impatto sul mercato del lavoro;
- identificare i settori lavorativi maggiormente interessati dall'avvento dell'intelligenza artificiale;
- promuovere la formazione dei lavoratori e dei datori di lavoro in materia di intelligenza artificiale.

Si ricorda che l'*AI Act* (per una sintesi del quale si rinvia alla scheda di lettura relativa al successivo articolo 24, c. 2 e 6), annovera tra i **sistemi definiti ad alto rischio (di cui all'Allegato III, punto 4)** - ossia potenzialmente in grado di violare diritti fondamentali - anche **quelli utilizzati per l'occupazione, la gestione dei lavoratori e l'accesso al lavoro** (in particolare per l'assunzione e la selezione delle persone), dal momento che tali sistemi possono influire sensibilmente sulle prospettive di carriera future e sui mezzi di sussistenza di tali persone e sui diritti dei lavoratori. Per tale ragione, il Regolamento prevede che, prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul posto di lavoro, i datori di lavoro devono **informare i** rappresentanti dei lavoratori e **i lavoratori** interessati che saranno soggetti al sistema (**articolo 26, paragrafo 7**). Inoltre, in base al fatto che, come chiarito nei considerando del regolamento in questione, lo stesso non deve incidere sul diritto dell'Unione in materia di politica sociale e sul diritto del lavoro nazionale, si dispone che il regolamento medesimo non osta a che gli Stati membri o l'Unione mantengano o introducano disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori per quanto riguarda la tutela dei loro diritti relativi all'uso dei sistemi di IA da parte dei datori di lavoro, o per incoraggiare o consentire l'applicazione di contratti collettivi più favorevoli ai lavoratori.

L'Osservatorio è **presieduto dal Ministro del lavoro** e delle politiche sociali o da un suo rappresentante e, con decreto del medesimo Ministro, da adottare entro novanta giorni dalla data di entrata in vigore della presente legge, sono stabiliti i suoi componenti, ai quali non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati. A tale decreto è demandata altresì la definizione delle modalità di funzionamento, nonché degli ulteriori compiti e funzioni dell'Osservatorio (**comma 2**).

Con riferimento a tali disposizioni, potrebbe risultare opportuno precisare – mediante apposita specificazione normativa – quali possano essere gli ambiti nei quali il decreto è legittimato ad attribuire, con fonte di rango secondario, ulteriori compiti e funzioni all'Osservatorio e, al contempo, indicare nei confronti di quali soggetti, pubblici e/o privati, sia rivolta la relativa attività di carattere istruttorio, programmatorio e formativo.

Si dispone, infine, che l'istituzione e il funzionamento dell'Osservatorio **non comportano nuovi o maggiori oneri** a carico della finanza pubblica e sono assicurati con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente (**comma 3**).

Articolo 13 *(Disposizioni in materia di professioni intellettuali)*

L'**articolo 13**, la cui formulazione letterale è stata **modificata dal Senato**, **limita alle attività strumentali e di supporto** la possibile finalità di utilizzo **dei sistemi di intelligenza artificiale nelle professioni intellettuali** e richiede che l'eventuale utilizzo dei medesimi sistemi **sia oggetto di informativa ai clienti** da parte dei professionisti in esame.

L'**articolo 13** concerne l'utilizzo dei sistemi di intelligenza artificiale – come definiti nel precedente **articolo 2, comma 1, lettera a)** – nelle professioni intellettuali.

Riguardo all'ambito e alla disciplina generale di queste ultime, la **relazione illustrativa** del presente disegno di legge¹⁶ fa riferimento agli articoli [da 2229 a 2238 del codice civile](#). Tali articoli concernono il contratto di prestazione d'opera intellettuale (in tale ambito, l'[articolo 2230](#) fa rinvio, in quanto compatibili con le suddette disposizioni e con la natura del rapporto, alle norme di cui agli [articoli da 2222 a 2228 del citato codice](#), relative al contratto d'opera in generale).

La disciplina di cui al presente **articolo 13** è, dunque, inerente ai contratti di prestazione d'opera intellettuale e non anche a contratti (quali, per esempio, i contratti di edizione) di cessione o utilizzo di opere intellettuali precedentemente realizzate senza un incarico sottostante, opere che restano quindi al di fuori della disciplina limitativa in oggetto.

Il **comma 1** dell'**articolo 13**, la cui formulazione letterale è stata **modificata dal Senato**, limita alle attività strumentali e di supporto la possibile finalità di utilizzo dei sistemi di intelligenza artificiale nelle professioni intellettuali e specifica che, nell'ambito di queste ultime, l'attività professionale deve restare contraddistinta dalla prevalenza del lavoro intellettuale oggetto della prestazione d'opera. La suddetta **relazione illustrativa** osserva che, in base al **comma in esame**, il pensiero critico umano deve sempre risultare prevalente rispetto all'uso degli strumenti di intelligenza artificiale. Il requisito di prevalenza appare, dunque, posto dal **comma** con riferimento al profilo della qualità della prestazione (e non implica una prevalenza anche di tipo quantitativo).

Il successivo **comma 2** dispone che le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista siano comunicate al

¹⁶ Si ricorda che la suddetta **relazione** è reperibile nell'[A.S. n. 1146](#).

soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo (nel rispetto del rapporto fiduciario tra professionista e cliente).

Riguardo all'uso dei sistemi di intelligenza artificiale da parte dei professionisti, cfr. anche la disciplina di delega di cui all'**articolo 24, comma 2, lettera f)**, del presente disegno di legge (si rinvia alla relativa scheda).

Articolo 14 *(Uso dell'intelligenza artificiale nella pubblica amministrazione)*

L'**articolo 14** pone talune previsioni di ordine generale circa l'utilizzo dell'intelligenza artificiale nei procedimenti della pubblica amministrazione, alla stregua di principi quali la conoscibilità, tracciabilità, strumentalità rispetto alla decisione spettante comunque alla persona responsabile dell'agire amministrativo.

Il **comma 1** pone le finalità dell'utilizzo dell'intelligenza artificiale da parte delle pubbliche amministrazioni.

Sono:

- ✓ l'incremento della propria efficienza;
- ✓ la riduzione dei tempi di definizione dei procedimenti;
- ✓ l'incremento della qualità e quantità dei servizi erogati.

Al contempo, si prescrive di assicurare agli interessati la **conoscibilità** del suo funzionamento e la **tracciabilità** del suo utilizzo.

L'utilizzo dell'intelligenza artificiale ha da essere in **funzione strumentale** e di supporto all'attività provvedimentale.

Ed è tenuto al rispetto dell'autonomia e del **potere decisionale della persona** che resta l'unica responsabile dei provvedimenti e dei procedimenti (così il **comma 2**).

Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative, volte a garantire un utilizzo dell'intelligenza artificiale "**responsabile**" e a sviluppare le capacità trasversali degli utilizzatori (**comma 3**).

Infine è posta una clausola di invarianza finanziaria (**comma 4**).

I principi così formulati concernono un ambito di utilizzo dell'intelligenza artificiale – da parte delle pubbliche amministrazioni – sul quale, se allo stato non sono intervenute pronunzie della Corte costituzionale, si è profilata ormai una prima giurisprudenza amministrativa.

Vale rammentare, per questo riguardo, la **sentenza del Consiglio di Stato, Sezione VI, 8-4-2019, n. 2270**, entro un giudizio in cui gli appellanti erano docenti della scuola secondaria di secondo grado già inseriti nelle relative graduatorie ad esaurimento, individuati come destinatari di proposta di assunzione a tempo indeterminato, in conseguenza del piano straordinario nazionale (di cui alla legge n. 107 del 2015, art. 1, commi 95-104) nella fase "B". Essi lamentavano di essersi ritrovati - per effetto di un meccanismo algoritmico - destinatari di una nomina su classi di concorso ed ordine di scuola in cui non avevano mai lavorato,

e scuola superiore di primo grado benché avessero espresso preferenza per quella di secondo grado, ed in province lontane rispetto a quella di provenienza, quando poi in seguito, durante la fase “C”, i docenti collocati in graduatoria in posizione deteriore rispetto agli appellanti, hanno beneficiato dell’assunzione a tempo indeterminato nella classe di concorso prescelta e nella provincia di residenza.

Il Consiglio di Stato rilevava preliminarmente “gli indiscutibili vantaggi derivanti dalla automazione del processo decisionale dell’amministrazione mediante l’utilizzo di una procedura digitale ed attraverso un ‘algoritmo’ - ovvero di una sequenza ordinata di operazioni di calcolo - che in via informatica sia in grado di valutare e graduare una moltitudine di domande. L’utilità di tale modalità operativa di gestione dell’interesse pubblico è particolarmente evidente con riferimento a procedure seriali o standardizzate, implicanti l’elaborazione di ingenti quantità di istanze e caratterizzate dall’acquisizione di dati certi ed oggettivamente comprovabili e dall’assenza di ogni apprezzamento discrezionale”.

Dunque la strumentazione digitale può concorrere ai canoni di efficienza ed economicità dell’azione amministrativa, secondo il principio costituzionale di buon andamento dell’azione amministrativa (art. 97 Cost.); non solo, “l’assenza di intervento umano in un’attività di mera classificazione automatica di istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall’uomo), e l’affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell’art. 97 Cost. coerenti con l’attuale evoluzione tecnologica”.

Tuttavia, soggiungeva il Consiglio di Stato, l’utilizzo di procedure ‘robotizzate’ non può essere motivo di elusione dei principi che conformano il nostro ordinamento e che regolano lo svolgersi dell’attività amministrativa. “Difatti, la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall’uomo e non dalla macchina, per essere poi (solo) applicata da quest’ultima, anche se ciò avviene in via esclusiva. Questa regola algoritmica, quindi:

- possiede una piena valenza giuridica e amministrativa, anche se viene declinata in forma matematica, e come tale, come si è detto, deve soggiacere ai principi generali dell’attività amministrativa, quali quelli di pubblicità e trasparenza (art. 1 l. 241/90), di ragionevolezza, di proporzionalità, etc.;

- non può lasciare spazi applicativi discrezionali (di cui l’elaboratore elettronico è privo), ma deve prevedere con ragionevolezza una soluzione definita per tutti i casi possibili, anche i più improbabili (e ciò la rende in parte diversa da molte regole amministrative generali); la discrezionalità amministrativa, se senz’altro non può essere demandata al *software*, è quindi da rintracciarsi al momento dell’elaborazione dello strumento digitale;

- vede sempre la necessità che sia l’amministrazione a compiere un ruolo *ex ante* di mediazione e composizione di interessi, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell’algoritmo (soprattutto nel caso di apprendimento progressivo e di *deep learning*);

- deve contemplare la possibilità che – come è stato autorevolmente affermato – sia il giudice a “dover svolgere, per la prima volta sul piano ‘umano’,

valutazioni e accertamenti fatti direttamente in via automatica”, con la conseguenza che la decisione robotizzata “impone al giudice di valutare la correttezza del processo automatizzato in tutte le sue componenti”. **In definitiva, dunque, l’algoritmo, ossia il *software*, deve essere considerato a tutti gli effetti come un “atto amministrativo informatico”.**

Ciò comporta un duplice ordine di conseguenze. “In primo luogo, come già messo in luce dalla dottrina più autorevole, il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l’algoritmo) deve essere “**conoscibile**”, secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico. Tale conoscibilità dell’algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare - e conseguentemente sindacabili - le modalità e le regole in base alle quali esso è stato impostato. In altri termini, la “caratterizzazione multidisciplinare” dell’algoritmo (costruzione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la “formula tecnica”, che di fatto rappresenta l’algoritmo, sia corredata da spiegazioni che la traducano nella “regola giuridica” ad essa sottesa e che la rendano leggibile e comprensibile, sia per i cittadini che per il giudice”

“In secondo luogo, **la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo.** La suddetta esigenza risponde infatti all’irrinunciabile necessità di poter sindacare come il potere sia stato concretamente esercitato, ponendosi in ultima analisi come declinazione diretta del diritto di difesa del cittadino, al quale non può essere precluso di conoscere le modalità (anche se automatizzate) con le quali è stata in concreto assunta una decisione destinata a ripercuotersi sulla sua sfera giuridica. Solo in questo modo è possibile svolgere, anche in sede giurisdizionale, una valutazione piena della legittimità della decisione; valutazione che, anche se si è al cospetto di una scelta assunta attraverso una procedura informatica, non può che essere effettiva e di portata analoga a quella che il giudice esercita sull’esercizio del potere con modalità tradizionali. In questo senso, la decisione amministrativa automatizzata impone al giudice di valutare in primo luogo la correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all’inserimento dei dati, alla loro validità, alla loro gestione. Da qui, come si è detto, si conferma la necessità di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell’algoritmo medesimo. In secondo luogo, conseguente al primo, il giudice deve poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della “regola” che governa l’algoritmo, di cui si è ampiamente detto”

Sulla scorta di tali considerazioni, il Consiglio di Stato accoglieva l'appello dei ricorrenti, ravvisando la violazione dei principi di imparzialità, pubblicità e trasparenza, poiché non era dato comprendere per quale ragione le legittime aspettative di soggetti collocati in una determinata posizione in graduatoria fossero andate deluse. “Infatti, l'impossibilità di comprendere le modalità con le quali, attraverso il citato algoritmo, siano stati assegnati i posti disponibili, costituisce di per sé un vizio tale da inficiare la procedura. Non solo, gli esiti della stessa paiono effettivamente connotati dall'illogicità ed irrazionalità denunciate dalle appellanti”.

Ancora in un giudizio relativo al procedimento di assegnazioni di sedi scolastiche, interveniva la **sentenza del Consiglio di Stato, Sezione VI, 13 dicembre 2019, n. 8472**. Essa rimarcava il rilievo fondamentale assunto, anche alla luce della disciplina di origine sovranazionale, da “due aspetti preminenti, quali elementi di minima garanzia per ogni ipotesi di utilizzo di algoritmi in sede decisoria pubblica: a) la piena **conoscibilità** a monte del modulo utilizzato e dei criteri applicati; b) l'**imputabilità** della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo”.

Per quanto riguarda la conoscibilità dell'algoritmo, essa “deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che i criteri, i presupposti e gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare - e conseguentemente sindacabili - le modalità e le regole in base alle quali esso è stato impostato”.

Per quanto concerne l'imputabilità, “deve essere garantita la verifica a valle, in termini di logicità e di correttezza degli esiti. Ciò a garanzia dell'imputabilità della scelta al titolare del potere autoritativo, individuato in base al principio di legalità, nonché della verifica circa la conseguente individuazione del soggetto responsabile, sia nell'interesse della stessa p.a. che dei soggetti coinvolti ed incisi dall'azione amministrativa affidata all'algoritmo”.

Sulla scorta del diritto sovranazionale europeo, il Consiglio di Stato rilevava inoltre la rilevanza del “**principio di non esclusività della decisione algoritmica**. Nel caso in cui una decisione automatizzata «produca effetti giuridici che riguardano o che incidano significativamente su una persona», questa ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato (art. 22 Reg. 2016/679). In proposito, deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. In ambito matematico ed informativo il modello viene definito come HITL (*human in the loop*), in cui, per produrre il suo risultato è necessario che la macchina interagisca con l'essere umano”.

Così come sottolineava “un ulteriore principio fondamentale, di **non discriminazione algoritmica**, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la

profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti”.

Le due sentenze ‘apripista’ del 2019 sopra ricordate – la prima concernente l’attività amministrativa vincolata, la seconda con ‘apertura’ a quella discrezionale – hanno avuto successivi ribadimenti (cfr. ancora della Sezione VI, la sentenza 4-2-2020, n. 881) e possono dirsi recare salienti indirizzi giurisprudenziali in ordine all’utilizzo, allo stato, di strumenti della ‘rivoluzione digitale’ da parte delle pubbliche amministrazioni.

Articolo 15 *(Impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria)*

L'**articolo 15**, integralmente sostituito nel corso dell'esame in Senato, detta norme generali per l'utilizzo dei sistemi di intelligenza artificiale **in ambito giudiziario**.

La formulazione dell'articolo 15 è volta a delimitare in maniera precisa gli ambiti nei quali l'impiego di sistemi di intelligenza artificiale è consentito nello svolgimento dell'attività giudiziaria propriamente detta e delle attività ad essa collaterali.

Innanzitutto, il **comma 1** stabilisce che in caso di utilizzo dei sistemi di intelligenza artificiale sono sempre riservate al magistrato le decisioni concernenti:

- l'**interpretazione** e l'**applicazione** della legge;
- la **valutazione** dei fatti e delle prove;
- l'adozione dei **provvedimenti**.

Per le decisioni sopra elencate, che costituiscono il nucleo fondamentale e più sensibile nell'esercizio della giurisdizione, viene esclusa pertanto qualsiasi possibilità di fare ricorso all'intelligenza artificiale.

La disposizione, dunque, non consentirebbe l'impiego dei sistemi di AI riconducibili alla c.d. "**giustizia predittiva**", ovvero di sistemi che, sulla base di un modello statistico elaborato in maniera autonoma dal sistema stesso a seguito dell'analisi di una mole significativa di atti giuridici, sono in grado di formulare una previsione che può giungere fino al possibile esito di un giudizio.

Rispetto all'originaria formulazione del testo dell'articolo 15, non è più presente il riferimento all'utilizzo dei sistemi di intelligenza artificiale per le attività di ricerca giurisprudenziale e dottrinale, per le quali dovrebbe ritenersi applicabile la disciplina di cui al successivo comma 2. Sul punto, la Commissione giustizia del Senato con riferimento alla disposizione in commento ha reso parere rilevando la necessità del ripristino della formulazione originale del primo periodo del comma 1 dell'articolo in commento, che consentiva l'utilizzo di sistemi di intelligenza artificiale per l'attività giudiziaria finalizzato alle sole attività strumentali e di supporto, ovvero «per l'organizzazione e la semplificazione del lavoro giudiziario nonché per la ricerca giurisprudenziale e dottrinale».

Ai sensi del **comma 2**, è invece consentito il ricorso a sistemi di intelligenza artificiale per ciò che riguarda:

- l'**organizzazione** dei servizi relativi alla giustizia;
- la **semplificazione** del lavoro giudiziario;
- le **attività amministrative accessorie**.

In tali ambiti, la **disciplina** puntuale per l'impiego dei sistemi di intelligenza artificiale è **demandata al Ministro della giustizia**.

La formulazione precedente demandava al Ministro della giustizia la disciplina per l'impiego dei sistemi di intelligenza artificiale da parte degli uffici giudiziari relativamente alla giustizia ordinaria, mentre per le altre giurisdizioni erano chiamati a provvedere **gli organi di governo competenti** sulla base dei rispettivi ordinamenti (ovvero il Consiglio di Presidenza della Giustizia amministrativa e le Sezioni riunite della Corte dei conti).

Il **comma 3** prevede che, fino alla compiuta attuazione del regolamento europeo sull'intelligenza artificiale ([Reg. \(UE\) 2024/1689](#)), l'**autorizzazione alla sperimentazione e l'impiego dei sistemi di intelligenza artificiale negli uffici giudiziari ordinari** è concessa dal **Ministero della giustizia**, che provvede sentite le autorità nazionali cui sono demandate le attività di controllo e sorveglianza ai sensi dell'**articolo 20** (su cui si veda la relativa scheda di lettura), ovvero l'Agencia per l'Italia digitale (AgId) e l'Agencia per la cybersicurezza (ACN).

Si valuti l'opportunità di specificare se, come sembrerebbe dal tenore letterale della disposizione, l'autorizzazione del Ministro della giustizia sia di carattere generale e si riferisca all'utilizzo di specifici sistemi di intelligenza artificiale da parte di tutti gli uffici giudiziari ordinari.

Si ricorda sul punto che il regolamento (UE) 2024/1689 prevede la creazione di appositi spazi di sperimentazione normativa per l'intelligenza artificiale (artt. 57 e ss.), operativi fino al 2 agosto 2026 (data a partire dalla quale, ad esclusione di specifiche previsioni, si applica il regolamento).

Infine, il **comma 4** è volto alla **promozione di attività didattiche sul tema dell'intelligenza artificiale** e sugli impieghi dei sistemi di intelligenza artificiale nell'attività giudiziaria, attraverso la loro inclusione nelle linee programmatiche sulla **formazione dei magistrati** formulate dal Ministro della giustizia ai sensi dell'articolo 12, comma 1, lettera *a*), del d.lgs. 26/2006.

La citata lettera *a*) prevede che il comitato direttivo della Scuola superiore della magistratura ha il compito di predisporre la bozza di programma annuale delle

attività didattiche, da sottoporre al comitato direttivo per la sua adozione, tenendo conto delle linee programmatiche sulla formazione pervenute dal Consiglio superiore della magistratura e dal Ministro della giustizia, nonché delle proposte pervenute dal Consiglio nazionale forense e dal Consiglio universitario nazionale.

Le attività formative sono volte:

- alla formazione digitale di base e avanzata,
- all'acquisizione e condivisione di competenze digitali,
- alla sensibilizzazione sui benefici e sui rischi connessi all'utilizzo dell'intelligenza artificiale.

Il Ministro deve altresì curare lo svolgimento di analoghe **attività formative** a favore del **personale amministrativo** della giustizia.

• ***Regolamentazione e applicazione dell'IA nell'amministrazione della giustizia***

Il [regolamento del Parlamento europeo e del Consiglio UE n. 1689 del 2024](#), cd. "AI Act", si caratterizza per un approccio basato sulla definizione di diversi **livelli di rischio** delle applicazioni di IA. In tale contesto, i **sistemi di intelligenza artificiale destinati all'amministrazione della giustizia** sono riconosciuti come "ad alto rischio" giacché incidono sugli ambiti più sensibili del diritto, nei quali occorre minimizzare i "rischi di potenziali distorsioni, errori e opacità", tenendone distinte le "attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi o l'assegnazione delle risorse", alle quali non si ritiene opportuno estendere la classificazione di rischio elevato (Considerando 61).

Particolarmente sensibili sono i profili attinenti all'utilizzo dell'IA nell'ambito del **diritto penale**. Sul tema è intervenuta una specifica [risoluzione del Parlamento europeo](#) (6 ottobre 2021), nella quale si ribadisce che "la decisione che produce effetti giuridici o analoghi deve sempre essere presa da un essere umano, il quale possa essere ritenuto responsabile per le decisioni adottate".

La disposizione in commento risulta altresì in linea con la [Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi](#), adottata dalla Commissione europea per l'efficienza della giustizia (CEPEJ) nel dicembre del 2018, dove, in particolare, si stabilisce che il giudice dovrebbe poter controllare in qualsiasi momento le decisioni giudiziarie e i dati utilizzati per produrre una decisione, mantenendo la possibilità di discostarsi dalle soluzioni proposte dall'IA, tenendo conto delle specificità del caso in questione.

Si segnala, infine, che la **Commissione Giustizia del Senato** sta svolgendo un'[indagine conoscitiva](#) sull'impatto dell'intelligenza artificiale nel settore della

giustizia, nell'ambito della quale hanno già avuto luogo alcune audizioni di esperti in materia.

Per maggiori dettagli circa l'utilizzo dei sistemi di intelligenza artificiale nel settore della giustizia si rinvia all'apposito [dossier](#).

Dal punto di vista operativo, il Ministro della giustizia, nell'ultima relazione sull'amministrazione della giustizia riferita all'anno 2024 ([Vol. I](#) e [Vol II](#)), ha dato conto di una serie di **applicazioni dell'intelligenza artificiale** negli ambiti di competenza del **Ministero**, tra i quali si segnalano in particolare:

- il programma "Nemesis", attivo presso l'Ispettorato generale del Ministero, con compiti di registrazione e gestione delle ispezioni ordinarie e delle attività di natura straordinaria e/o riservata;

- la Piattaforma per le indagini, che facilita il lavoro della polizia giudiziaria e del pubblico ministero durante le indagini preliminari, migliorando l'analisi e il trattamento dei dati;

- il progetto DataLake Giustizia, realizzato nell'ambito del PNRR, in cui sono ricompresi sei diversi sistemi concernenti la gestione di dati e statistiche relativi a processi civili e penali, le attività di anonimizzazione e pseudonimizzazione delle sentenze civili e penali e l'identificazione del rapporto vittima- autore del reato. All'interno del progetto, è in fase avanzata lo sviluppo di una piattaforma di *Business Intelligence* per *dashboard* interattive e report, utili per l'elaborazione di statistiche nazionali e distrettuali, nonché la realizzazione di un *data mart* dedicato all'analisi del fenomeno della violenza di genere.

Un altro importante progetto allo studio è BIGOSINT, in cui l'intelligenza artificiale è utilizzata per contrastare crimini transfrontalieri come il traffico di migranti.

Più in generale, nella relazione si sottolinea come l'intelligenza artificiale sia «utilizzata per ottimizzare i carichi di lavoro e prevedere criticità, trasformando il dato grezzo in conoscenza utile». Tra gli esempi l'anonimizzazione automatica delle sentenze civili e penali; la possibilità di eseguire ricerche avanzate all'interno dei testi delle sentenze civili di merito e dei procedimenti collegati, con collegamenti alla normativa citata nelle sentenze e la capacità di generare delle sintesi dei testi. Inoltre è stata prevista la possibilità di utilizzare *dashboard* interattive per monitorare, in tempo reale, la durata dei procedimenti (cd. *Disposition time*) ed i valori del carico arretrato e sono stati predisposti modelli di analisi predittiva per stimare i carichi di lavoro e anticipare problematiche organizzative.

Il Ministero della giustizia è inoltre parte attiva in **numerosi progetti europei** che promuovono l'innovazione e l'adozione di tecnologie avanzate, come i progetti e-EDES (per la creazione di un'infrastruttura digitale sicura per la cooperazione giudiziaria penale a livello europeo), AI – TSI (per lo sviluppo di standard etici comuni per l'uso dell'intelligenza artificiale nei sistemi giudiziari europei), ViSAR (per l'implementazione di una piattaforma per supportare le vittime di crimini con strumenti basati sull'intelligenza artificiale).

Infine, sotto il coordinamento del Ministero della giustizia, sono state implementate delle "UPP *task force*", in cui le università operano in stretto

raccordo con gli uffici giudiziari dei singoli territori per migliorarne l'efficienza e le prestazioni attraverso la sperimentazione di modelli di intelligenza artificiale.

Articolo 16

(Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale)

L'articolo 16, reca delega al Governo, indicandone i **principi e criteri direttivi**, per la definizione organica della disciplina relativa all'**utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale**, affidando le controversie in materia alle sezioni specializzate in materia d'impresa.

L'articolo 16 al **comma 1** delega il Governo ad adottare, entro 12 mesi dalla entrata in vigore della legge, uno o più decreti legislativi per definire organicamente la disciplina organica relativa all'**utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale**.

Con riguardo alla **procedura di adozione** dei suddetti decreti, il **comma 2** prevede che siano adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia. Di ciascuno schema di decreto è prevista la successiva trasmissione alle Camere per l'espressione dei **pareri delle Commissioni parlamentari competenti**, che si pronunciano entro il termine di 60 giorni dalla data di trasmissione, decorso il quale i decreti legislativi possono essere comunque emanati. La disposizione prevede inoltre il principio dello "**scorrimento**" in base al quale se il termine previsto per il parere cade nei trenta giorni che precedono la scadenza del termine previsto o successivamente, la scadenza medesima è prorogata di sessanta giorni.

Il **comma 3** dell'articolo 16 reca i **principi e criteri direttivi** ai quali il Governo è tenuto ad attenersi nell'esercizio della delega di cui ai commi precedenti.

Nel dettaglio, il legislatore delegato è chiamato, in primo luogo, a individuare le ipotesi per le quali appare necessario dettare il **regime giuridico dell'utilizzo di dati, algoritmi e metodi matematici** per l'addestramento di sistemi di intelligenza artificiale, nonché i **diritti e gli obblighi** gravanti sulla parte che intenda procedere al suddetto utilizzo (**lett. a**).

Si ricorda che l'articolo 4 del disegno di legge in esame (su v. *supra*) prevede che con riferimento ai **dati personali**, deve esserne garantito: il trattamento lecito, corretto e trasparente, nonché la compatibilità con le finalità per le quali sono stati raccolti, in conformità con il diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza. Si estendono pertanto all'ambito dell'intelligenza artificiale i principi vigenti in materia di riservatezza dei dati personali.

Conseguentemente, in caso di violazione delle prescrizioni che saranno dettate ai sensi della precedente lett. *a*), il legislatore delegato dovrà individuare **strumenti di tutela**, a carattere risarcitorio o inibitorio, nonché delineare un apposito **apparato sanzionatorio (lett. b)**.

Infine, si prevede che le controversie relative alla disciplina che sarà introdotta nell'esercizio della delega dovranno essere attribuite alle **sezioni specializzate in materia di impresa (lett. c)**.

Le sezioni specializzate in materia di impresa sono articolazioni dei tribunali ordinari e delle corti d'appello istituite per trattare in via esclusiva determinate controversie relative al diritto commerciale e societario disciplinate dal **D. Lgs. 27 giugno 2003, n. 168**. L'art. 3 del **citato decreto legislativo** definisce le controversie attribuite alla competenza delle sezioni specializzate, che comprendono, in particolare:

- proprietà industriale;
- diritto d'autore e diritti connessi;
- concorrenza sleale e pratiche anticoncorrenziali;
- normativa *antitrust* dell'UE;
- tutela collettiva dei consumatori

Articolo 17 (*Modifiche al codice di procedura civile*)

L'**articolo 17** affida al **tribunale la competenza in materia** di procedimenti riguardanti il funzionamento di un sistema **di intelligenza artificiale**.

Più nel dettaglio, l'articolo in commento modifica l'articolo 9, secondo comma, del codice di procedura civile al fine di introdurre, tra le materie di **esclusiva competenza del tribunale**, quelle hanno ad oggetto il funzionamento di un **sistema di intelligenza artificiale**, escludendo pertanto la competenza del giudice di pace in tali materie.

Si ricorda che il primo comma dell'art. 9 c.p.c., nella sua formulazione vigente, attribuisce al tribunale la competenza per tutte quelle cause che non sono di competenza di un altro giudice, mentre il secondo comma del medesimo articolo individua alcune specifiche materie per le quali il tribunale è competente in via esclusiva ovvero:

- ✓ imposte e tasse;
- ✓ stato e capacità delle persone e diritti onorifici;
- ✓ querela di falso;
- ✓ esecuzione forzata;
- ✓ cause di valore indeterminabile.

Codice di procedura civile

Testo previgente	Modificazioni apportate dall'art. 17
Art. 9 <i>(Competenza del tribunale)</i>	Art. 9 <i>(Competenza del tribunale)</i>
Il tribunale è competente per tutte le cause che non sono di competenza di altro giudice.	<i>Identico.</i>
Il tribunale è altresì esclusivamente competente per le cause in materia di imposte e tasse, per quelle relative allo stato e alla capacità delle persone e ai diritti onorifici, per la querela di falso, per l'esecuzione forzata e, in generale, per ogni causa di valore indeterminabile.	Il tribunale è altresì esclusivamente competente per le cause in materia di imposte e tasse, per quelle relative allo stato e alla capacità delle persone e ai diritti onorifici, per la querela di falso, per l'esecuzione forzata, per le cause che hanno ad oggetto il funzionamento di un

Codice di procedura civile

Testo previgente

Modificazioni apportate dall'art. 17

sistema di intelligenza artificiale e, in generale, per ogni causa di valore indeterminabile.

Articolo 18 *(Uso dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale)*

L'articolo 18 reca modifiche all'art. 7, comma 1, del decreto-legge n. 82 del 2021, in materia di *cybersicurezza*, attribuendo ulteriori funzioni all'Agenzia per la *cybersicurezza nazionale* in materia di intelligenza artificiale.

L'articolo 18 si compone di un unico comma e reca modifiche all'articolo 7, comma 1, del decreto-legge n. [82 del 2021](#) (convertito con la legge n. 109 del 2021) finalizzate a favorire l'utilizzo dell'intelligenza artificiale a supporto della *cybersicurezza nazionale*.

Il **decreto-legge n. 82 del 2021**, recante disposizioni urgenti in materia di *cybersicurezza*, definizione dell'architettura nazionale di *cybersicurezza* e istituzione dell'Agenzia per la *cybersicurezza nazionale*, è stato convertito dalla legge n. 109 del 2021. Tale atto normativo definisce il **sistema nazionale di sicurezza cibernetica** e istituisce una nuova "**Agenzia per la cybersicurezza nazionale**" (ACN), a tutela degli interessi nazionali nel campo della *cybersicurezza*, definendone organizzazione e compiti.

L'articolo 7, comma 1, individua le funzioni dell'Agenzia che viene qualificata quale **Autorità nazionale** per la *cybersicurezza* (ACN). Tra le sue attribuzioni rientrano: il coordinamento tra soggetti pubblici coinvolti nella *cybersicurezza* a livello nazionale; la predisposizione della strategia nazionale di *cybersicurezza*; la promozione di azioni comuni dirette ad assicurare la sicurezza cibernetica.

Per approfondimenti si veda il relativo [dossier](#).

In particolare, l'articolo 18, comma 1, introduce una nuova lettera **m-quater**) al suddetto articolo del decreto-legge n. 82 del 2021, attribuendo all'Agenzia per la *cybersicurezza nazionale* (ACN) il **compito** di promuovere e sviluppare ogni iniziativa finalizzata a **valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale**. In precedenza il testo attribuiva all'Autorità la facoltà di promuovere a tal fine iniziative di solo partenariato pubblico-privato. Tuttavia, nel corso dell'esame in sede referente è stato modificato quest'ultimo inciso al fine di precisare che la stessa può concludere accordi di collaborazione con i privati, comunque denominati, nonché di partenariato pubblico-privato.

Dalla relazione illustrativa che ha accompagnato la proposta emendativa si evince che la stessa è volta evitare il sorgere di incertezze analoghe a quelle riscontrate in sede applicativa rispetto a quanto previsto dall'articolo 7, comma 1, lett. z), del decreto-legge

n. 82/2021 nel quale si attribuisce all’Autorità la competenza a costituire e partecipare esclusivamente a partenariati pubblico-privato (terminologia che riconduce, impropriamente, ai modelli adottati dal Codice dei contratti pubblici).

In questo modo, come si evince dalla Relazione illustrativa che accompagna il disegno di legge, anche nell’ambito del settore strategico della *cybersicurezza*, viene affermata la **visione antropocentrica** quale fattore di prevenzione e di contenimento del rischio, come anche evidenziato nel **Considerando 6** dell’*AI Act*.

Inoltre, l’assegnazione di questo compito all’ACN appare in linea con l’osservazione, rinvenibile nel **Considerando 76** dell’*AI Act*, secondo cui la *cybersicurezza* svolge un “ruolo cruciale nel garantire che i sistemi di intelligenza artificiale siano resilienti ai tentativi” di terzi animati da intenzioni malevole e agli attacchi informatici.

Circa la puntualizzazione, contenuta nella novella, in ordine al **partenariato pubblico-privato**, appare conferente menzionare:

- sia l’**art. 67** dell’*AI Act*, il quale istituisce il **Forum consultivo** volto a fornire consulenze e competenze agli organi delle istituzioni europee, il quale è composto da una “selezione equilibrata” di portatori d’interessi, tra cui imprese, *start-up*, società civile e mondo accademico;
- sia il **consenso internazionale** maturato sulla circostanza che gli **investimenti** e la **sperimentazione** sull’intelligenza artificiale debbano contare sullo **sforzo congiunto tra soggetti e regolatori pubblici e impresa privata**. Vedi in proposito, da ultimo, la [dichiarazione di Seul del 21 maggio 2024](#), nella quale si fa riferimento all’“*active multi-stakeholder collaboration, including governments, the private sector, academia, and civil society*”.

CAPO III – STRATEGIA NAZIONALE, AUTORITÀ NAZIONALI E AZIONI DI PROMOZIONE

Articolo 19 (*Strategia nazionale per l'intelligenza artificiale*)

L'articolo 19 definisce la **governance italiana** sull'intelligenza artificiale, dettando disposizioni in materia di **Strategia nazionale per l'intelligenza artificiale**.

L'articolo 19 apre il **Capo III** del disegno di legge, relativo alla "**Strategia nazionale, Autorità nazionali e azioni di promozione**", recante norme che, come evidenziato dalla Relazione illustrativa "disegnano la *governance* italiana e le azioni di promozione sull'intelligenza artificiale".

L'articolo in commento appare in linea con il *Considerando 148* dell'*AI Act*, che raccomanda a livello nazionale l'istituzione di un **adeguato livello** di *governance* e con il (conseguente) art. **70** del medesimo regolamento europeo sull'intelligenza artificiale.

La norma si compone di **5 commi** e detta disposizioni relative alla Strategia nazionale per l'intelligenza artificiale.

Il **comma 1** individua i **oggetti** chiamati a **predisporre** e ad **aggiornare** la suddetta Strategia. Nello specifico, la norma affida tale incarico al **Dipartimento per la trasformazione digitale** della Presidenza del Consiglio dei ministri, **d'intesa** con le **Autorità nazionali per l'intelligenza artificiale** di cui all'articolo 18. Prevede, inoltre, che per la sua predisposizione debbano essere **sentiti**:

- il Ministro delle **imprese e del *made in Italy*** per i profili di politica industriale e di incentivazione;
- il **Ministro dell'università e della ricerca** per i profili relativi alla formazione superiore e alla ricerca (modifica introdotta nel corso dell'esame in sede referente);
- il Ministro della **difesa** per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale.

Infine, è previsto che la Strategia debba essere approvata con cadenza almeno **biennale** dal **Comitato interministeriale per la transizione**

digitale (CITD) di cui all'articolo 8, comma 2, del decreto-legge n. 22 del 2021, convertito, con modificazioni, dalla legge n. 55 del 2021.

Si ricorda che il 22 luglio 2024, è stato pubblicato il documento [Strategia Italiana per l'Intelligenza Artificiale 2024-2026](#)

A norma dell'**art. 18** del disegno di legge in commento, sono Autorità nazionali per l'intelligenza artificiale l'**Agenzia per l'Italia digitale** (AgID) e l'**Agenzia per la cybersicurezza nazionale** (ACN).

L'art. 8, comma 2, del decreto-legge n. 22 del 2021, convertito dalla legge n. 55 del 2021, istituisce presso la Presidenza del Consiglio dei Ministri il **Comitato interministeriale per la transizione digitale (CITD)**, e gli attribuisce tra gli altri, il compito di assicurare il coordinamento e monitoraggio dell'attuazione delle iniziative relative allo sviluppo e alla diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'*internet* delle cose (IoT) e della *blockchain*.

Con riferimento alla sua composizione, il comma 3 del medesimo articolo stabilisce che esso è presieduto dal Presidente del Consiglio dei Ministri o dalla Autorità delegata per l'innovazione tecnologica e la transizione digitale, ove nominata, ed è formato dai Ministri per la pubblica amministrazione, ove nominato, dell'economia e delle finanze, della giustizia, delle imprese e del *made in italy* e della salute. Vi partecipano altresì gli altri Ministri o loro delegati aventi competenza nelle materie oggetto dei provvedimenti e delle tematiche poste all'ordine del giorno.

Per approfondimenti si rimanda a relativo [dossier](#).

Il **comma 2** individua le **finalità** della Strategia nazionale per l'intelligenza artificiale, prevedendo che essa debba mirare a favorire la **collaborazione** tra le amministrazioni pubbliche e i soggetti privati relativamente allo sviluppo e all'adozione di sistemi di intelligenza artificiale, **coordinare** l'attività della pubblica amministrazione in materia, **promuovere** la ricerca e la diffusione della conoscenza in materia di intelligenza artificiale, **indirizzare** le misure e gli incentivi finalizzati allo sviluppo imprenditoriale e industriale dell'intelligenza artificiale.

Pertanto, come si evince anche dalla Relazione illustrativa, il documento garantisce la collaborazione tra pubblico e privato, coordinando le azioni della PA in materia e le misure e gli incentivi economici rivolti allo sviluppo imprenditoriale e industriale.

Il nuovo **comma 3, introdotto nel corso dell'esame al Senato**, dà rilievo, nell'ambito della Strategia nazionale per l'intelligenza artificiale, ai principi del diritto internazionale umanitario, al fine di garantire lo sviluppo e la promozione di sistemi di intelligenza artificiale che tutelino i diritti umani.

Il **comma 4** attribuisce al **Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri** il compito di coordinare e monitorare l'attuazione della strategia. Nello svolgimento di tale incarico il

Dipartimento si avvale dell'Agencia per l'Italia digitale, d'intesa, per gli aspetti di competenza, con l'Agencia per la *cybersicurezza* nazionale.

Tale comma è stato oggetto di modifica nel corso dell'esame in sede referente. In particolare, secondo la nuova formulazione il Dipartimento, in sede di attuazione della strategia, è tenuto altresì a sentire la Banca d'Italia, la Consob e l'IVASS in qualità di autorità di vigilanza del mercato.

È previsto, infine, che i **risultati** del monitoraggio vengano trasmessi **annualmente** alle **Camere**.

Il **comma 5** reca modifiche **all'articolo 8, comma 3, primo periodo**, del citato **decreto-legge n. 22 del 2021**. Nello specifico, ai componenti, su indicati, del Comitato interministeriale per la transizione digitale (CITD) viene aggiunto il Ministero dell'università e della ricerca. Con emendamento approvato in sede referente, viene inserita altresì, tra i componenti del Comitato, l'Autorità delegata per la sicurezza della Repubblica e per la cybersicurezza, ove istituita.

Dalla relazione illustrativa che ha accompagnato la proposta emendativa si evince che la *ratio* della modifica si basa sulla considerazione delle attribuzioni del CITD in materia di Strategia sull'intelligenza artificiale e della competenza che spetta in tale ambito all'Autorità per la Cybersicurezza Nazionale. Conseguentemente si è ritenuto opportuno garantire alla citata Autorità una rappresentanza permanente e con poteri decisionali all'interno del Comitato, al di là della generale previsione contenuta all'articolo 8, comma 4, del decreto-legge n. 22/2021 che consente di integrare la partecipazione al Comitato *ratione materiae*.

Articolo 20 *(Autorità nazionali per l'intelligenza artificiale)*

L'**articolo 20** qualifica Autorità nazionali per l'intelligenza artificiale due soggetti: l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN).

In particolare, qualifica rispettivamente l'AgID come autorità di notifica, e l'Agenzia per la cybersicurezza nazionale come autorità di vigilanza del mercato e punto di contatto unico con le istituzioni dell'Unione europea.

In entrambi i casi, tiene ferma l'attribuzione a Banca d'Italia, CONSOB e IVASS del ruolo di autorità di vigilanza del mercato secondo quanto previsto, in materia di operatori finanziari, dall'articolo 74, paragrafo 6, del Regolamento europeo sull'intelligenza artificiale.

Istituisce inoltre un Comitato di coordinamento presso la Presidenza del Consiglio, per agevolare la collaborazione delle due Agenzie tra loro e con le pubbliche amministrazioni.

Infine, prevede che il Nucleo per la Cybersicurezza sia composto anche da un rappresentante dell'AgID.

L'articolo 20 attribuisce la **qualifica di Autorità nazionale per l'intelligenza artificiale** a due soggetti:

- ✓ l'**Agenzia per l'Italia digitale (AgID)**;
- ✓ l'**Agenzia per la cybersicurezza nazionale (ACN)**.

Prima di definirne le rispettive competenze, specifica (secondo aggiunta inserita nel corso dell'esame in prima lettura presso il Senato) che resta ferma l'attribuzione a **Banca d'Italia, Consob e IVASS** (Istituto per la vigilanza delle assicurazioni) del ruolo di **autorità di vigilanza del mercato** secondo quanto previsto, in materia di operatori finanziari, dall'**articolo 74, paragrafo 6, del Regolamento (UE) 2024/1689** (c.d. *AI Act*).

La richiamata disposizione del Regolamento europeo stabilisce che 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 medesimo regolamento si identifichi nella pertinente **autorità nazionale responsabile della vigilanza finanziaria di tali enti** ai sensi del diritto nazionale di ciascuno Stato membro, 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.

In qualità di Autorità nazionale per l'intelligenza artificiale, all'**Agenzia per l'Italia digitale** sono attribuiti:

- ✓ la responsabilità di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale;
- ✓ le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale.

Nella medesima qualità, all'**Agenzia per la cybersicurezza nazionale** sono attribuiti:

- ✓ la responsabilità per la vigilanza - ivi incluse le attività ispettive e sanzionatorie - dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea;
- ✓ la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza.

Peraltro, è previsto che le due Agenzie (ciascuna secondo la rispettiva competenza) assicurino l'istituzione e la gestione **congiunta** di spazi di **sperimentazione**, sentito il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave 'duale', nonché (è stato introdotto nel corso dell'esame presso il Senato) il Ministero della giustizia per i modelli e i sistemi di intelligenza artificiale applicabili all'attività giudiziaria.

La disposizione tuttavia fa **salva** (secondo modifica introdotta in Senato) la disciplina prevista dall'[articolo 36, commi da 2-bis a 2-novies, del decreto-legge 30 aprile 2019, n. 34](#), convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58, per quanto concerne la **sperimentazione di sistemi di intelligenza artificiale** destinati ad essere immessi sul mercato, messi in servizio o usati da **istituti finanziari**.

Si ricorda che le citate disposizioni hanno previsto che il Ministro dell'Economia e delle Finanze, sentiti la Banca d'Italia, la CONSOB e l'IVASS, adottasse, entro il 31 gennaio 2021, uno o più **regolamenti** per definire le **condizioni** e le **modalità di svolgimento** di una **sperimentazione relativa alle attività di tecno-finanza** (Fin.Tech) volte al **perseguimento**, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, **dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati**. Le disposizioni prevedono che la disciplina regolamentare sia orientata a promuovere e a sostenere l'imprenditoria, a stimolare la competizione nel mercato e, al contempo, ad assicurare una protezione adeguata dei consumatori, degli investitori e del mercato dei capitali, nonché a favorire il raccordo tra le istituzioni, le autorità e gli operatori del settore. Esse stabiliscono altresì i principi e i criteri direttivi ai fini dell'esercizio del potere normativo in questione.

In attuazione delle richiamate disposizioni, a seguito di una consultazione pubblica conclusa il 30 marzo 2020 per l'adozione di un regolamento finalizzato

all'introduzione della sperimentazione Fintech in Italia (c.d. *regulatory sandbox*) è stato adottato il [Decreto del Ministero dell'Economia e delle Finanze 30 aprile 2021, n. 100](#). Il regolamento, oltre a recare la disciplina di dettaglio della suddetta sperimentazione, ivi compresi i requisiti di accesso alla medesima, istituisce il **Comitato FinTech**. Tale ente è investito del compito di individuare gli obiettivi, definire i programmi e porre in essere le azioni per **favorire lo sviluppo della tecno-finanza**, anche in cooperazione con soggetti esteri, nonché di formulare proposte di carattere normativo e agevolare il contatto degli operatori del settore con le istituzioni e con le autorità. Il Comitato è composto, in qualità di membri permanenti, dal Ministro dell'Economia e delle Finanze, dal Ministro dello Sviluppo Economico, dal Ministro per gli Affari Europei, dalla Banca d'Italia, dalla CONSOB, dall'IVASS, dall'Autorità garante della concorrenza e del mercato, dal Garante per la protezione dei dati personali, dall'AgID e dall'Agenzia delle entrate.

Altra disposizione (introdotta in Senato) provvede all'attuazione dell'articolo 70 del Regolamento (UE) 2024/1689, rispettivamente attribuendo:

- ✓ all'AgID la qualifica di **autorità di notifica**;
- ✓ all'ACN la qualifica di **autorità di vigilanza del mercato e punto di contatto unico** con le istituzioni dell'Unione europea.

Ed anche in tal caso, tiene ferma l'attribuzione a **Banca d'Italia, CONSOB e IVASS** del ruolo di **Autorità di vigilanza del mercato** secondo quanto previsto, in materia di operatori finanziari, dal già richiamato articolo 74, paragrafo 6, del Regolamento sull'intelligenza artificiale.

Tale disciplina persegue lo scopo di 'anticipare' l'**individuazione delle Autorità nazionali competenti** ai sensi del citato Regolamento europeo sull'intelligenza artificiale, senza che sia necessario attendere il decorso del termine previsto dal provvedimento in esame ai fini dell'adozione del decreto legislativo di adeguamento (stabilito in 12 mesi dalla data di entrata in vigore della presente legge, ai sensi dell'articolo 22, comma 1: per un approfondimento, si rinvia alla relativa scheda di lettura).

L'**articolo 70** del citato Regolamento europeo sull'intelligenza artificiale impone a ciascuno **Stato membro** di **istituire** o di **designare**, in qualità di autorità nazionali competenti ai fini del presente regolamento, **almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato**. La disposizione prescrive che tali autorità nazionali esercitino i loro poteri in modo indipendente, imparziale e senza pregiudizi, garantendo l'applicazione e l'attuazione della disciplina recata dal Regolamento. Essa, inoltre, vincola gli Stati membri a comunicare alla Commissione europea l'identità delle autorità di notifica e delle autorità di vigilanza del mercato e i compiti di tali autorità, nonché a designare un'autorità di vigilanza del mercato che funga da punto di contatto unico per il regolamento, notificandone l'identità alla Commissione. La

disposizione, infine, impone agli Stati membri di garantire che tali autorità nazionali dispongano di risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti. Per quanto attiene alle risorse umane, specifica inoltre che le stesse siano dotate di sufficiente personale disponibile in via permanente, che disponga di una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cybersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza e di una conoscenza delle norme e dei requisiti giuridici esistenti.

È prevista altresì la istituzione di un **Comitato di coordinamento** presso la Presidenza del Consiglio, composto dai direttori generali delle due Agenzie e dal Capo del Dipartimento per la trasformazione digitale della medesima Presidenza del Consiglio.

Tale Comitato è volto a prestare ausilio al coordinamento e alla collaborazione delle due Agenzie tra loro e con le altre pubbliche amministrazioni e autorità indipendenti.

Si prevede (ed è, questa, aggiunta introdotta nel corso dell'esame presso il Senato) che al Comitato partecipino **rappresentanti** di vertice della **Banca d'Italia**, della **CONSOB** e dell'**IVASS**, quando siano trattate questione ricadenti nella rispettiva competenza di tali enti.

Ai componenti del Comitato non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

Si valuti l'opportunità che la norma definisca, sia pure nelle linee generali, le modalità di funzionamento del Comitato e gli eventuali principi cui improntare la collaborazione con le altre amministrazioni pubbliche e autorità indipendenti.

La disposizione, inoltre, tiene **ferme le attribuzioni del Garante per la protezione dei dati personali**.

Infine è posta una **modifica** all'[articolo 8, comma 2, primo periodo, del decreto-legge 14 giugno 2021, n. 82](#).

La norma dispone l'**inserimento** delle parole: “**e dell’Agenzia per l’Italia digitale**” dopo le parole: “Presidenza del Consiglio dei Ministri”.

La novella (introdotta in Senato) pertanto determina che il **Nucleo per la cybersicurezza**, costituito ai sensi dell'articolo medesimo, sia **composto** anche da un **rappresentante dell’AgID**.

Il citato decreto-legge n. 42 del 2021 reca disposizioni urgenti in materia di cybersicurezza, definisce l'architettura nazionale di cybersicurezza e istituisce l'Agenzia per la cybersicurezza nazionale.

Il richiamato **articolo 8** costituisce presso l'Agenzia, in via permanente, il **Nucleo per la cybersicurezza**, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla

prevenzione e alla **preparazione ad eventuali situazioni di crisi** e per l'attivazione delle procedure di allertamento.

Il Nucleo è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, nonché da un rappresentante, rispettivamente: del DIS; dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'[articolo 6 della legge 3 agosto 2007, n. 124](#); dell'Agenzia informazioni e sicurezza interna (AIS), di cui all'[articolo 7 della legge n. 124 del 2007](#); di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Inoltre, per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'[articolo 9 della legge n. 124 del 2007](#).

Articolo 21
***(Applicazione sperimentale dell'intelligenza artificiale ai servizi
forniti dal Ministero degli affari esteri e della cooperazione
internazionale)***

L'**articolo 21** autorizza la spesa di 300.000 euro, per ciascuno degli anni 2025 e 2026, per la realizzazione di **progetti sperimentali volti all'applicazione dell'intelligenza artificiale** relativamente ai servizi forniti dal MAECI.

L'**articolo 21, comma 1** autorizza la spesa di 300.000 € annui per ciascuno degli anni 2025 e 2026 per la realizzazione di progetti sperimentali volti all'applicazione dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale a cittadini e a imprese.

A tal riguardo si fa presente che i servizi in questione sono principalmente rivolti agli **italiani residenti all'estero** e ai **cittadini o residenti del Paese di accreditamento** (ad es. visti), ma, nei casi previsti dalla legge, anche agli **italiani temporaneamente all'estero**. Inoltre, ai sensi dell'art. 23 del [Trattato sul funzionamento dell'Unione europea](#), **l'Ufficio consolare può prestare assistenza anche ai cittadini dell'Unione europea** nel caso in cui lo Stato membro di cittadinanza non disponga nel Paese in cui si opera di alcuna Ambasciata, Consolato o Console onorario. Allo stesso modo, nei Paesi in cui l'Italia non è rappresentata, ma vi è un'Ambasciata o un Consolato di un altro Stato membro dell'UE, il connazionale ha il diritto di essere tutelato alle stesse condizioni dei cittadini di tale Stato.

Il **comma 2** specifica che agli oneri derivanti dal comma 1 (300.000€ annui per il biennio 2025-26) si provvede mediante corrispondente **riduzione dello stanziamento del fondo speciale** di parte corrente iscritto, ai fini del bilancio triennale 2025-2027, nell'ambito del programma «Fondi di riserva e speciali» della missione «Fondi da ripartire» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2025, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero degli affari esteri e della cooperazione internazionale.

Come **esposto dal Governo nella relazione tecnica allegata al disegno di legge**, per la quantificazione dello stanziamento, in assenza di una serie

storica di dati derivante dalla novità del settore dell'intelligenza artificiale, **si è tenuto conto di progetti sperimentali per l'uso dell'intelligenza artificiale già avviati dal MAECI** e di altre organizzazioni pubbliche e private anche simili con esigenze analoghe a quelle del predetto Ministero, il cui valore medio è stato di circa 75.000€ per un anno. **Nel biennio considerato si è pertanto considerata la possibilità di avviare quattro iniziative** (di durata biennale) di valore medio comparabile a quello del progetto sperimentale già avviato. La disposizione è espressamente redatta come un **tetto di spesa** e non è quindi suscettibile di comportare nuovi o maggiori oneri per la finanza pubblica superiori a quelli espressamente quantificati nel testo normativo. Agli oneri si provvede mediante corrispondente riduzione delle disponibilità della Tabella A, voce Ministero degli affari esteri e della cooperazione internazionale, che presenta le necessarie disponibilità. Si precisa che la riduzione non compromette l'attività di ratifica dei trattati internazionali e il connesso adempimento degli obblighi internazionali.

Si segnala inoltre che, rispetto al testo originario del ddl, **la copertura è stata aggiornata** al bilancio 2025-2027 durante l'esame in sede referente.

Giova rammentare l'[Audizione del Sottosegretario di Stato per gli affari esteri e la cooperazione internazionale Giorgio Silli](#) sui servizi consolari e le principali questioni riguardanti i cittadini italiani residenti all'estero, tenutasi nella III Commissione della Camera Affari esteri e comunitari il 22 novembre 2023. Il Sottosegretario Silli ha evidenziato l'**ampiezza della nostra diaspora**, considerato che “i cittadini italiani residenti all'estero sono attualmente 7 milioni, un numero enorme che richiede un'attenta gestione dei servizi loro dedicati”. Inoltre, “a questi 7 milioni **si aggiungono gli italo-discendenti**, cioè il numero di persone che, ai sensi della [legge italiana sulla cittadinanza](#) n. 91 del 1992, possono vantare il diritto ad acquisire la cittadinanza italiana”. Nello specifico nel corso dell'audizione è stata preannunciata l'intenzione del Governo di **migliorare i servizi consolari**, anche nell'ottica di una loro **digitalizzazione** ove possibile, e di **ampliare la partecipazione della Comunità italiana all'estero alla vita democratica del nostro Paese**, attraverso i **COMITES**, le **scuole** e le **associazioni italiane** o con nuovi strumenti mutuabili, con i dovuti aggiustamenti, da altri ordinamenti (ad esempio il voto elettronico utilizzato dalla Francia per far votare i propri cittadini all'estero). Il Sottosegretario Silli ha inoltre citato nel suo intervento la **proposta di legge [A.C. 994 On. Onori](#)**, in corso di esame presso la III Commissione, relativa alla **creazione di un Portale unico telematico per gli italiani all'estero**, volto all'unificazione ed omogeneizzazione di tutte le informazioni disponibili sui servizi consolari che possono essere erogati *on line*. Il Portale potrebbe rispondere alle esigenze di tre

macro-gruppi di cittadini italiani: coloro che sono in procinto di andare all'estero, coloro che sono già residenti all'estero e coloro i quali desiderano legittimamente ritornare nel nostro Paese.

Si ricorda, inoltre, che il 21 novembre 2024 è stata definitivamente approvata dal Senato la proposta di legge [A.C. 960](#) dei deputati Toni Ricciardi ed altri concernente la "Destinazione agli uffici diplomatici e consolari di quota dei proventi derivanti dal rilascio dei passaporti all'estero". La conseguente [Legge 28 novembre 2024 n. 188](#) prevede, all'articolo 1, l'istituzione di un fondo, con una dotazione pari a 4 milioni di euro annui a decorrere dall'anno 2025, per il finanziamento di interventi destinati al rafforzamento dei servizi consolari in favore dei cittadini italiani residenti o presenti all'estero, con priorità per i servizi maggiormente richiesti. Le risorse del fondo sono ripartite annualmente tra gli uffici diplomatico-consolari in proporzione al numero dei passaporti ordinari rilasciati da ciascun ufficio nell'anno precedente.

• Principali servizi consolari

Fra i principali servizi consolari si annoverano:

- **L'assistenza ai detenuti: visite periodiche** in carcere; suggerimento di **nominativi di legali** di riferimento *in loco*; cura dei **contatti con i familiari**, previo consenso espresso del detenuto; fornitura, quando necessario e consentito dalle norme locali, di **generi di conforto** al detenuto; piccoli aiuti economici sotto forma di **sussidi occasionali**; mediazione per favorire il **trasferimento in Italia** del detenuto, qualora stia scontando la pena in Paesi aderenti alla [Convenzione di Strasburgo sul trasferimento dei detenuti del 1983](#) o con cui siano in vigore accordi bilaterali con l'Italia; mediazione per sostenere le **domande di grazia** presentate dal detenuto o dal suo legale.
- **L'assistenza economica**: l'Ufficio consolare, compatibilmente con i fondi disponibili, può eccezionalmente erogare al cittadino italiano che risiede stabilmente residente nella propria circoscrizione consolare e che si trovi in situazione di comprovata indigenza un **sussidio**. Può altresì erogare al cittadino italiano temporaneamente all'estero e residente in Italia o in altra circoscrizione consolare che non possa avvalersi dell'aiuto dei familiari a ciò tenuti per legge (art. 433 c.c.) o di terze persone un **prestito con promessa di restituzione** all'Erario entro 90 giorni.
- **L'assistenza in caso di furto o smarrimento dei documenti**: qualora il cittadino italiano si trovi in una situazione di emergenza (ad esempio un turista in transito che deve ripartire ed ha smarrito o è stato derubato del proprio passaporto) e non si faccia in tempo ad esperire la necessaria istruttoria per l'emissione di un nuovo passaporto, la Rappresentanza consolare rilascia un **documento provvisorio di viaggio** (E.T.D, *Emergency Travel Document*) **con validità per il solo viaggio di rientro** in Italia, nel Paese di stabile residenza all'estero o, in casi eccezionali, per una diversa destinazione.

- La collaborazione con le competenti Autorità italiane (Questure, Agenzia delle Entrate) per il **rilascio di passaporti e codici fiscali**.
- La collaborazione con i Comuni italiani per la tenuta dell'**Anagrafe degli Italiani residenti all'estero (AIRE)** e la gestione dei registri di **stato civile** (cittadinanza, nascita, matrimonio e morte), che includono gli atti di stato civile formati dalla Rappresentanza diplomatico-consolare e quelli emessi dalle Autorità straniere nonché altri provvedimenti stranieri (ad es. sentenze di divorzio, adozione) trasmessi ai Comuni italiani per la trascrizione.
- La **celebrazione del matrimonio consolare e della costituzione di unioni civili**, se non vi si oppongono le leggi locali.
- La gestione del processo di **voto all'estero** dei cittadini italiani iscritti AIRE **per le elezioni politiche, i referendum abrogativi e costituzionali** di cui agli artt. 75 e 138 della Costituzione, le **elezioni dei membri del Parlamento europeo** spettanti all'Italia e, ove costituiti nelle circoscrizioni consolari in cui risiedono almeno 3.000 italiani, l'elezione dei **Comitati degli italiani residenti all'estero (COMITES)**.

Il voto all'estero per le elezioni politiche e i referendum nazionali è regolato dalla [Legge 27 dicembre 2001, n. 459](#) e dal relativo regolamento attuativo [D.P.R. 2 aprile 2003, n. 104](#). Il voto all'estero per l'elezione dei rappresentanti dell'Italia al Parlamento europeo è invece regolato dalla [Legge 24 gennaio 1979, n. 18](#) e dal [Decreto-legge 24 giugno 1994, n. 408](#) convertito in Legge 3 agosto 1994, n. 483. Il voto per i COMITES è regolato dalla [Legge 23 ottobre 2003, n. 286](#).

Possono essere ammessi al voto per le elezioni politiche, del Parlamento europeo e per i referendum nazionali anche i cittadini temporaneamente domiciliati all'estero per un periodo di almeno 3 mesi per motivi di lavoro, studio o cure mediche, previa apposita istanza da presentare alla Rappresentanza diplomatico-consolare competente in base al temporaneo domicilio.

- La collaborazione con il Ministero dell'Interno nella gestione delle **domande di cittadinanza italiana** presentate all'estero, inclusi l'identificazione del richiedente, l'acquisizione in originale della documentazione pertinente e gli altri adempimenti necessari al perfezionamento dell'istanza.
- La **notifica all'estero** degli atti giudiziari ed extragiudiziari italiani in materia civile e commerciale.
- Il rilascio a favore di cittadini italiani che si trovano all'estero in via permanente o temporanea di alcuni **atti notarili** (procure, testamenti, atti notori, autenticazioni di sottoscrizioni apposte a scritture private).
- La **legalizzazione e traduzione di atti e documenti** stranieri emessi dalle Autorità di Paesi che non hanno sottoscritto la [Convenzione de L'Aia del 5 ottobre 1961 relativa all'abolizione della legalizzazione di atti pubblici stranieri](#).
- Il **rimpatrio consolare**, in collaborazione con gli enti italiani territorialmente competenti (Prefetture, Questure, Comuni, Aziende Sanitarie Locali, Servizi Sociali), di cittadini italiani residenti all'estero che versino in **gravi condizioni di indigenza** e di **minori italiani in stato di abbandono**, subordinatamente alla verifica della disponibilità dei congiunti ad assumersi in Italia le responsabilità connesse con il mantenimento e l'assistenza del rimpatriando.

In assenza di tale disponibilità, il rimpatrio è coordinato con i Servizi Sociali del Comune di ultima residenza o di origine in Italia, ovvero attraverso il ricorso a fondi regionali mentre il rimpatrio di minori in stato di abbandono è effettuato a carico dell'Erario, di concerto con il Tribunale dei Minori competente e i Servizi Sociali del Comune di residenza.

- Il **rimpatrio di salme** di cittadini italiani deceduti all'estero, in collaborazione con il Comune italiano competente per la tumulazione della salma o delle ceneri.
- La collaborazione con la Commissione **Adozioni Internazionali** (CAI), Autorità centrale per l'Italia per l'applicazione della [Convenzione de L'Aja del 29 maggio 1993 sulla tutela dei minori e la cooperazione in materia di adozione internazionale](#), per il buon esito delle procedure di adozione.
- La collaborazione con l'INPS per il pagamento delle **pensioni** all'estero.

Occorre inoltre sottolineare che le Rappresentanze diplomatico-consolare svolgono un significativo lavoro relativamente alla concessione dei **visti di ingresso in Italia** nei casi previsti dalla normativa vigente.

Per un approfondimento della normativa concernente i servizi consolari cfr. https://www.esteri.it/it/servizi-consolari-e-visti/normativa_consolare/serviziconsolari/ Per un approfondimento della normativa concernente il rilascio dei visti di ingresso cfr. https://www.esteri.it/it/servizi-consolari-e-visti/normativa_consolare/visti/.

Articolo 22

(Misure di sostegno per il rientro in Italia dei lavoratori, i giovani e lo sport)

L'**articolo 22** introduce modifiche e iniziative in ambiti specifici riguardanti il **rientro in Italia dei lavoratori**, i **giovani** e lo **sport**. In particolare, il **comma 1** annovera lo svolgimento di attività di **ricerca applicata** nel campo delle **tecnologie di intelligenza artificiale** tra i requisiti in presenza dei quali è possibile accedere al **regime fiscale agevolativo** in favore dei **lavoratori** cosiddetti **impatriati**. Il **comma 2** dispone poi che, per gli studenti delle scuole superiori con **alto potenziale cognitivo**, il **piano didattico personalizzato (PDP)** può includere attività volte a sviluppare competenze aggiuntive, tramite **esperienze di apprendimento** presso **istituzioni di istruzione superiore**, con la possibilità che i **crediti formativi** acquisiti attraverso queste attività vengano riconosciuti e valutati nei percorsi di formazione superiore che lo studente intraprenderà dopo aver ottenuto il diploma di maturità. Il **comma 3** promuove l'intervento dello Stato per favorire l'accesso ai **sistemi di intelligenza artificiale** per migliorare il **benessere psicofisico** delle persone tramite **l'attività sportiva**. Questo include lo sviluppo di soluzioni innovative per una maggiore inclusione delle persone con disabilità nel settore sportivo. Inoltre, si prevede che i sistemi di intelligenza artificiale possono essere utilizzati anche per organizzare attività sportive.

Nello specifico, il **comma 1**, mediante una integrazione alla lettera *d*) del comma 1 dell'articolo 5 del [decreto legislativo 27 dicembre 2023, n. 209](#), aggiunge un riferimento allo svolgimento di **attività di ricerca, anche applicata**, nell'ambito delle **tecnologie di intelligenza artificiale** nell'elenco dei **requisiti** in presenza dei quali è possibile accedere al **regime fiscale agevolativo** a favore dei **lavoratori cosiddetti impatriati**.

Si ricorda che [l'articolo 5, comma 1 del decreto legislativo n. 209 del 2023](#) disciplina un **regime temporaneo di tassazione agevolata** riconosciuto, a determinate condizioni, ai lavoratori che trasferiscono la residenza fiscale in Italia a partire dal periodo d'imposta 2024 e nei quattro periodi d'imposta successivi a quello in cui è avvenuto il trasferimento.

Più nel dettaglio, il regime stabilisce che i **redditi di lavoro dipendente** e **assimilati**, e i **redditi di lavoro autonomo**, derivanti dall'esercizio di arti e professioni, prodotti in Italia entro il limite annuo di 600.000 euro da

lavoratori che trasferiscono la residenza fiscale nel territorio dello Stato, **concorrono alla formazione del reddito complessivo**, ai fini IRPEF, limitatamente al **50 per cento** del loro ammontare.

Il suddetto regime è applicabile, a legislazione vigente, quando ricorrono (tutte) le seguenti condizioni:

a) i lavoratori si impegnano a risiedere fiscalmente in Italia per almeno quattro anni;

b) i lavoratori non sono stati fiscalmente residenti in Italia nei tre periodi d'imposta precedenti il loro trasferimento;

c) l'attività lavorativa è prestata per la maggior parte del periodo d'imposta nel territorio dello Stato;

d) i lavoratori sono in possesso dei requisiti di elevata qualificazione o specializzazione indicati dal [decreto legislativo n. 108/2012](#) e dal [decreto legislativo n. 206/2007](#).

Per un **ulteriore approfondimento** sul **regime agevolativo** a favore dei lavoratori impatriati, si rinvia [all'apposita scheda di lettura](#) del relativo [dossier](#) presente nel *Portale della documentazione*.

Ora, con l'entrata in vigore del comma in commento, la lettera *d*) dell'art. 5, comma 1, appena citata, assumerebbe la **seguente nuova formulazione**:

d) i lavoratori sono in possesso dei requisiti di elevata qualificazione o specializzazione indicati dal [decreto legislativo n. 108/2012](#) e dal [decreto legislativo n. 206/2007](#) **oppure hanno svolto un'attività di ricerca anche applicata nell'ambito delle tecnologie di intelligenza artificiale**.

In proposito, si evidenzia che, secondo la **relazione tecnica** allegata al disegno di legge in commento, la **novella** di cui al comma 1 in esame avrebbe una **valenza puramente specificativa**.

Essa cioè sarebbe volta a chiarire “che anche **i soggetti che hanno svolto un'attività di ricerca nell'ambito delle tecnologie di intelligenza artificiale sono tra coloro che possono rientrare nel già vigente regime agevolativo a favore dei lavoratori impatriati**, di cui all'art. 5 del d.lgs. 27 dicembre 2023, n. 209, senza pertanto comportare nuovi o maggiori oneri a carico della finanza pubblica, **poiché sicuramente in possesso dei requisiti di elevata qualificazione o specializzazione** come definiti dal d.lgs. 108/2012, richiesto dall'art.5, comma 1, lettera *d*), del d.lgs. 209/2023”.

In proposito, si ricorda **che l'articolo 1 del decreto legislativo n. 108 del 2012** ha introdotto, nel testo unico sull'immigrazione di cui al decreto legislativo n. 286 del 1998, **l'art. 27-quater** (rubricato “Ingresso e soggiorno per lavoratori altamente qualificati. Rilascio della Carta blu UE”), che, nel testo attualmente

vigente (e cioè, come **modificato** dall'[articolo 1 del decreto legislativo n. 152 del 2023](#)) fa riferimento alla necessità, per poter accedere e soggiornare in Italia per periodi superiori a tre mesi quali lavoratori stranieri altamente qualificati, di essere **alternativamente** in possesso dei seguenti **requisiti**:

a) del **titolo di istruzione superiore di livello terziario** rilasciato dall'autorità competente nel paese dove è stato conseguito che attesti il completamento di un **percorso di istruzione superiore di durata almeno triennale o di una qualificazione professionale di livello post secondario di durata almeno triennale** o corrispondente almeno al **livello 6 del Quadro nazionale delle qualificazioni** allegato al [decreto del Ministero del lavoro e delle politiche sociali dell'8 gennaio 2018](#) (laurea triennale, diploma accademico di primo livello, diploma ITS);

b) dei **requisiti** previsti dal [decreto legislativo n. 206 del 2007](#), limitatamente all'**esercizio di professioni regolamentate**;

c) di una **qualifica professionale superiore attestata da almeno cinque anni di esperienza professionale di livello paragonabile** ai titoli d'istruzione superiori di livello terziario, pertinenti alla professione o al settore specificato nel contratto di lavoro o all'offerta vincolante;

d) di una **qualifica professionale superiore attestata da almeno tre anni di esperienza professionale pertinente acquisita nei sette anni precedenti** la presentazione della domanda di Carta blu UE, per quanto riguarda dirigenti e specialisti nel settore delle tecnologie dell'informazione e della comunicazione di cui alla [classificazione ISCO-08](#), rispettivamente designati con il codice [n. 133](#) (dirigenti nei servizi delle tecnologie dell'informazione e della comunicazione) e [n. 25](#) (Specialisti delle tecnologie dell'informazione e della comunicazione).

Per quanto riguarda, invece, il **decreto legislativo n. 206 del 2007**, esso disciplina il **riconoscimento delle qualifiche professionali** già acquisite in uno o più Stati membri dell'Unione europea che permettono al titolare l'accesso e l'esercizio alle **professioni regolamentate**. Tali professioni, all'[articolo 4](#), sono definite come:

1) l'attività, o l'insieme delle attività, il cui esercizio è consentito solo a seguito di **iscrizione in ordini o collegi o in albi, registri ed elenchi** tenuti da amministrazioni o enti pubblici, se la iscrizione è **subordinata al possesso di qualifiche professionali o all'accertamento delle specifiche professionalità**;

2) i **rapporti di lavoro subordinato**, se l'accesso ai medesimi è subordinato, da disposizioni legislative o regolamentari, al possesso di **qualifiche professionali**;

3) l'attività esercitata con **l'impiego di un titolo professionale** il cui uso è **riservato** a chi possiede una qualifica professionale;

4) le attività attinenti **al settore sanitario** nei casi in cui il possesso di una **qualifica professionale** è condizione determinante ai fini della retribuzione delle relative prestazioni o della ammissione al rimborso;

5) le professioni esercitate dai membri di **specifici organismi o associazioni britanniche o irlandesi** (riportate all'[Allegato I](#) del decreto legislativo).

Il **comma 2** dell'articolo in esame dispone che nel **piano didattico personalizzato (PDP)** adottato dall'istituzione scolastica secondaria di secondo grado, nell'ambito della propria autonomia, per le **studentesse** e gli **studenti ad alto potenziale cognitivo**, possano essere inserite attività volte all'acquisizione di ulteriori competenze attraverso **esperienze di apprendimento** presso le **istituzioni della formazione superiore** (università e istituzioni dell'alta formazione artistica, musicale e coreutica – AFAM).

La disposizione prosegue precisando che le citate esperienze di apprendimento avvengono in **deroga** a quanto previsto dall'articolo 6 del regolamento di cui al [decreto del Ministro dell'istruzione, dell'università e della ricerca 22 ottobre 2004, n. 270](#), in materia di previo possesso del titolo, in coerenza con il profilo in uscita dell'indirizzo di studio. La previsione è stata **modificata in sede referente**, al solo fine di individuare la corretta norma cui derogare.

Il medesimo comma prevede, infine, che i **crediti formativi acquisiti** nell'ambito delle attività di cui sopra sono **valutati** nell'ambito dei **percorsi formativi della formazione superiore** intrapresi dopo il conseguimento del titolo summenzionato.

Si ricorda che l'articolo 6, comma 1, del regolamento di cui al decreto dell'allora Ministro dell'istruzione, dell'università e della ricerca 22 ottobre 2004, n. 270, stabilisce, in via generale, che “**per essere ammessi ad un corso di laurea occorre essere in possesso di un diploma di scuola secondaria superiore o di altro titolo di studio conseguito all'estero, riconosciuto idoneo**”.

In relazione a quanto disposto dal comma 2 dell'articolo in commento, si rileva che il citato **piano didattico personalizzato (PDP)**, a **livello legislativo**, risulta richiamato in tale specifica denominazione solo **dagli articoli 11 e 20 del decreto legislativo n. 62 del 2017**, peraltro in relazione ai **solli alunni con disabilità o con disturbi specifici di apprendimento**. Tali richiami **non forniscono una definizione di piano didattico personalizzato (PDP)**, né rinviano a tal fine a ulteriori disposizioni normative, anche di rango secondario. Per una ricostruzione del percorso che ha portato alla diffusione dei **piani didattici personalizzati** all'interno del sistema scolastico italiano, e per l'individuazione più precisa degli studenti per cui tali piani sono adottati, si rinvia all'approfondimento che segue.

• *Il Piano didattico personalizzato e i bisogni educativi speciali*

In materia di personalizzazione dei percorsi didattici, è opportuno ricordare preliminarmente che all'interno dell'ordinamento scolastico italiano vige, e riveste fondamentale importanza, il principio **dell'autonomia scolastica**.

Esso è espressamente riconosciuto **dall'articolo 117, terzo comma, della Costituzione**, e si desume implicitamente dagli altri articoli dedicati alla cultura e all'istruzione (artt. 9, 33 e 34). A livello legislativo, l'autonomia scolastica è riconosciuta **dall'articolo 21 della [legge 15 marzo 1997, n. 59](#)**, ed è disciplinata nel dettaglio dal relativo regolamento di attuazione, **il [decreto del Presidente della Repubblica 8 marzo 1999, n. 275](#)**.

Ai sensi del comma 9 dell'articolo 21 della citata legge n. 59 del 1997, **l'autonomia didattica** delle istituzioni scolastiche “si sostanzia nella scelta libera e programmata di metodologie, strumenti, organizzazione e tempi di insegnamento, da adottare nel rispetto della possibile pluralità di opzioni metodologiche, e in ogni iniziativa che sia espressione di **libertà progettuale**, compresa l'eventuale offerta di **insegnamenti opzionali, facoltativi o aggiuntivi** e nel rispetto delle **esigenze formative degli studenti**.”

L'articolo 4, comma 2, lettera c) del [DPR n. 275 del 1999](#) dispone poi che, nell'esercizio dell'autonomia scolastica, le scuole possono adottare tutte **le forme di flessibilità** che ritengono opportune, tra cui, l'attivazione di **percorsi didattici individualizzati**, nel rispetto del principio generale dell'integrazione degli alunni nella classe e nel gruppo, anche in relazione agli alunni “in situazione di handicap”, secondo quanto già previsto dalla [legge n. 104 del 1992](#).

La [legge 8 ottobre 2010, n. 170](#), ha successivamente introdotto nuove norme in materia di **disturbi specifici di apprendimento (DSA)** in ambito scolastico. Ai sensi dell'articolo 5 della legge appena citata, **agli studenti con DSA diagnosticato** le istituzioni scolastiche garantiscono, tra l'altro, l'uso di una **didattica individualizzata e personalizzata**, con forme efficaci e flessibili di lavoro scolastico che tengano conto anche di caratteristiche peculiari dei soggetti. Il [decreto ministeriale n. 5669 del 12 luglio 2011](#), attuativo della legge n. 170 del 2010, fa esplicito riferimento, all'articolo 5, all'adozione di un **piano didattico personalizzato** per gli **alunni e studenti con DSA**, in particolare specificando che la sua redazione può costituire lo strumento attraverso il quale la scuola garantisce ed esplicita, nei confronti di alunni e studenti con DSA, interventi didattici individualizzati e personalizzati.

Nel 2012 è quindi intervenuta la [direttiva ministeriale del 27 dicembre 2012](#) volta a definire strumenti di intervento per **gli alunni con bisogni educativi speciali – BES**. La direttiva parte dall'assunto che “**l'area dello svantaggio scolastico è molto più ampia** di quella riferibile esplicitamente alla presenza di deficit”, che “**le problematiche ricomprese nei disturbi evolutivi specifici non vengono o possono non venir certificate ai sensi della legge 104/92**, non dando conseguentemente diritto alle provvidenze ed alle misure previste dalla stessa legge quadro”; analogamente, la direttiva sottolinea che “**alcune tipologie di disturbi, non esplicitati nella legge 170/2010, danno diritto ad usufruire delle stesse misure ivi previste** in quanto presentano problematiche specifiche in

presenza di competenze intellettive nella norma”. “Un approccio educativo, non meramente clinico” continua la citata direttiva “dovrebbe dar modo di **individuare strategie e metodologie di intervento correlate alle esigenze educative speciali**, nella prospettiva di una scuola sempre più inclusiva e accogliente, senza bisogno di ulteriori precisazioni di carattere normativo”. Pertanto, “**le scuole** – con determinazioni assunte dai Consigli di classe, risultanti dall’esame della documentazione clinica presentata dalle famiglie e sulla base di considerazioni di carattere psicopedagogico e didattico – **possono avvalersi per tutti gli alunni con bisogni educativi speciali degli strumenti compensativi e delle misure dispensative previste dalle disposizioni attuative della legge 170/2010 (DM 5669/2011)**”.

In forza di tale direttiva interpretativa, la redazione, tra l’altro, del **piano didattico personalizzato** diviene quindi uno strumento **rivolto** non solo agli studenti in situazione di disabilità o di disturbo specifico dell’apprendimento certificati, ma **a tutti gli studenti con bisogni educativi speciali (BES)**. Il piano è utilizzato come strumento di lavoro *in itinere* per gli insegnanti e di documentazione alle famiglie delle strategie di intervento programmate. Più in particolare, la medesima direttiva evidenzia “la necessità di elaborare un **percorso individualizzato e personalizzato per alunni e studenti con BES**, anche attraverso la redazione di un **piano didattico personalizzato**”, riferendosi, tra gli altri, anche agli “alunni con competenze intellettive nella norma o anche elevate, che – per specifici problemi – possono incontrare difficoltà a scuola”.

L’interesse agli alunni con bisogni educativi speciali è stato poi declinato in precise modalità operative dall’Amministrazione scolastica mediante la [circolare ministeriale n. 8 del 6 marzo 2013](#), la [nota MIUR 27 giugno 2013 prot. n. 1551](#) e la [nota MIUR prot. n. 2563 del 22 novembre 2013](#), che delineano le **strategie di intervento** a favore degli alunni e studenti con bisogni educativi speciali, e offrono **indicazioni in merito alla redazione del piano didattico personalizzato (PDP)** per i medesimi alunni e studenti.

I **bisogni educativi speciali** sono citati dalla [legge n. 107 del 2015](#), cosiddetta “**Buona scuola**”, che individua espressamente fra gli obiettivi formativi prioritari del sistema d’istruzione il “potenziamento dell’inclusione scolastica e del diritto allo studio degli alunni con bisogni educativi speciali attraverso **percorsi individualizzati e personalizzati**” (articolo 1, comma 7, lettera l)).

Uno dei **decreti legislativi attuativi della legge “Buona scuola”**, il [n. 62 del 2017](#), cita esplicitamente i **piani didattici personalizzati**, ma, come si è detto, **solo con riferimento agli studenti con disabilità e disturbi specifici di apprendimento**, in particolare in relazione alla valutazione nel primo ciclo d’istruzione (articolo 11) e all’esame di Stato nel secondo ciclo d’istruzione (articolo 20). Un altro decreto legislativo attuativo della legge “Buona scuola”, il [n. 66 del 2017](#), è invece espressamente rivolto all’inclusione scolastica **degli studenti con disabilità**, e reca disposizioni specifiche in materia di “piano educativo individualizzato” ad essi rivolto.

Con più specifico riferimento agli **studenti ad alto potenziale cognitivo** (definiti in ambito internazionale *Gifted children*), con la [nota n. 562 del 3 aprile 2019, l’allora MIUR](#) ha avallato l’interpretazione invalsa presso le istituzioni

scolastiche a seguito dell'emanazione della sopra citata [direttiva 27 dicembre 2012](#) di **considerare la condizione di tali alunni e studenti plusdotati nell'ambito delle prescrizioni sul trattamento dei bisogni educativi speciali**, in quanto ritenuta assolutamente corretta nella prospettiva della **personalizzazione degli insegnamenti**, della valorizzazione degli stili di apprendimento individuali e del principio di responsabilità educativa (v. paragrafo, “Alunni e studenti ad alto potenziale intellettuale”, a pag. 3 della menzionata nota [n. 562](#)). La medesima nota ha, inoltre, chiarito che anche in caso di alto potenziale cognitivo, come per tutti gli altri bisogni educativi speciali, la strategia da assumere è rimessa alla decisione dei consigli di classe (o *team* docenti della primaria) che, in presenza di eventuali situazioni di criticità con conseguenti manifestazioni di disagio, possono adottare **metodologie didattiche specifiche** in un'ottica inclusiva, sia a livello individuale sia di classe, valutando la convenienza di un **percorso di personalizzazione formalizzato** in un **piano didattico personalizzato** (PDP).

Si evidenzia, altresì, che con riferimento alla condizione giuridica degli alunni e studenti ad alto potenziale cognitivo **sono all'esame congiunto della 7^a Commissione permanente del Senato i disegni di legge [AS n. 180](#)**, recante disposizioni per il riconoscimento degli alunni con alto potenziale cognitivo, l'adozione di piani didattici personalizzati e la formazione del personale scolastico all'esame del Senato, e [AS n. 1041](#), riguardante l'istituzione di un piano sperimentale per favorire l'inserimento e il successo scolastico degli alunni con alto potenziale cognitivo e per la formazione specifica dei docenti.

Si ricorda, inoltre, la [raccomandazione n. 1248 \(94\)](#) del Consiglio d'Europa sull'istruzione dei bambini con alto potenziale cognitivo.

Sullo stesso tema è intervenuto anche il **Comitato economico e sociale europeo** che, nella 486^o Sessione plenaria del 16-17 gennaio 2013, ha reso il parere “[Liberare il potenziale dei bambini e dei giovani con alte abilità intellettuali nell'Unione europea](#)”.

Il **comma 3** dell'articolo in esame prevede - con norma che appare di natura programmatica - che lo Stato favorisca **l'accessibilità ai sistemi di intelligenza artificiale** per il **miglioramento del benessere psicofisico** attraverso **l'attività sportiva**, anche ai fini dello sviluppo di soluzioni innovative finalizzate a una maggiore inclusione in ambito sportivo delle persone con disabilità.

Dispone, inoltre, che nel rispetto dei principi generali di cui al presente progetto di legge, i **sistemi di intelligenza artificiale** possano essere utilizzati anche per **l'organizzazione delle attività sportive**.

Articolo 23
***(Investimenti nei settori di intelligenza artificiale,
della cybersicurezza e calcolo quantistico)***

L'**articolo 23** consente investimenti – come precisato nel corso dell'esame in Senato, sotto forma di *equity* e quasi *equity* – fino a **un miliardo di euro** nel capitale di rischio di imprese che operano in Italia nei settori dell'intelligenza artificiale, della cybersicurezza, delle tecnologie quantistiche e dei sistemi di telecomunicazioni. Gli investimenti sono effettuati avvalendosi di Cdp Venture Capital Sgr spa (**comma 1**). Il Ministero delle imprese e del *made in Italy* (MIMIT) è il soggetto investitore (**comma 3**). Per la misura, vengono utilizzate le risorse del Fondo di sostegno al *venture capital* istituito dalla legge di bilancio 2019 (**comma 2**).

L'**articolo 23** qui in esame – che si compone di **tre commi** – reca misure finanziarie a sostegno di imprese operanti in settori dell'intelligenza artificiale, della cybersicurezza, delle tecnologie quantistiche e dei sistemi di telecomunicazioni.

Nello specifico, le misure, per esplicita previsione del **comma 1**, sono finalizzate a **supportare** lo sviluppo di **imprese operanti** nei settori dell'**intelligenza artificiale**, della **cybersicurezza** e, come riformulato nel corso dell'esame in Senato, delle tecnologie per essi abilitanti ivi compresi le **tecnologie quantistiche** e i **sistemi di telecomunicazioni**, anche attraverso la creazione di **poli di trasferimento tecnologico** e programmi di accelerazione operanti nei medesimi settori. Ciò in linea con la **Strategia nazionale** per l'intelligenza artificiale di cui all'articolo 19 (alla cui scheda di lettura si rinvia).

Il comma 1, segnatamente, autorizza, avvalendosi dell'operatività di **Cdp Venture Capital Sgr -Fondo Nazionale Innovazione (FNI)**, l'investimento – fino a 1 miliardo di euro – sotto forma di *equity* e quasi *equity*, nel capitale di rischio direttamente o indirettamente (così a seguito di modifica in Senato), di determinate imprese quali:

- a) **piccole e medie imprese (PMI)** con elevato potenziale di sviluppo e innovative, con **sede operativa** in Italia (la dicitura antecedente alle modifiche apportate nel corso dell'esame in Senato era “aventi sede legale e operativa”), che operano nei settori dell'intelligenza artificiale, della cybersicurezza e, come riformulato in Senato, delle tecnologie per

essi abilitanti ivi compresi le tecnologie quantistiche e i sistemi di telecomunicazioni con particolare riferimento al 5G e alle sue evoluzioni, al *mobile edge computing*, alle architetture aperte basate su soluzioni *software*, al Web 3, all'elaborazione del segnale, anche in relazione ai profili di sicurezza e integrità delle reti di comunicazione elettroniche, e che si trovano in fase di sperimentazione (*seed financing*), di costituzione (*start up financing*), di avvio dell'attività (*early-stage financing*) o di sviluppo del prodotto (*expansion, scale up financing*);

- b) **imprese**, con **sede operativa** in Italia (la dicitura antecedente alle modifiche apportate nel corso dell'esame in Senato era "aventi sede legale e operativa"), **anche diverse da quelle di cui alla lettera a)** di cui sopra, operanti nei suddetti settori e tecnologie, con elevato potenziale di sviluppo e altamente innovative, al fine di promuoverne lo sviluppo come campioni tecnologici nazionali.

Il **comma 3** specifica che **il soggetto investitore** è il **Ministero delle imprese e del made in Italy** (MIMIT).

Alla luce di quanto dispone il comma 3, si valuti l'opportunità di specificare, nel comma 1, laddove si utilizza genericamente la locuzione "è autorizzato", a chi è conferita tale autorizzazione.

La **relazione illustrativa** afferma che la mobilitazione dei suddetti investimenti avviene sulla base di una strategia che si fonda su **tre pilastri**:

- la **creazione di poli di trasferimento tecnologico** (c.d. *tech transfer*) specializzati in intelligenza artificiale, cybersicurezza e *quantum computing*: si tratta di veicoli che federano realtà accademiche, *partner* tecnici e co-investitori, con l'obiettivo di investire nelle predette imprese;
- **investimenti in startup in diverse fasi di vita** (*early* e *late stage*) attraverso **tre modalità**: coordinamento con fondi che si concentrano su specifici settori o industrie al fine di rafforzare le applicazioni verticali degli investimenti; investimenti autonomi in *startup* che operano in un ambito settoriale non ben definito o specifico; investimenti in fondi di *venture capital* che focalizzano la propria attività di investimento su *startup* che operano in ambiti specifici;
- iniziative relative alla creazione e allo sviluppo di **campioni nazionali** (o "**unicorni**") dell'intelligenza artificiale mediante, da un lato, l'implementazione di processi di supporto alla creazione di nuove *startup*, e, dall'altro, l'individuazione di una o più *startup* già esistenti in cui investire per supportarle nei processi di crescita.

Il **comma 2** prevede che gli **investimenti** di cui al comma 1 siano effettuati **attraverso** la **sottoscrizione** diretta o indiretta di **quote o azioni di uno o più fondi per il *venture capital***, **appositamente** istituiti e gestiti da Cdp Venture Capital Sgr spa (CDPVC), oppure attraverso il coinvestimento da parte di altri fondi per il *venture capital* istituiti e gestiti dalla stessa CDPVC.

Si valuti l'opportunità di meglio definire il concetto di "coinvestimento da parte di altri fondi", chiarendo se si intenda indicare una modalità di investimento effettuato in parte mediante fondi di nuova istituzione e in parte mediante fondi già istituiti.

Ai sensi del medesimo comma 2 gli investimenti sono effettuati mediante l'utilizzo delle risorse del **Fondo di sostegno al *venture capital*** di cui all'articolo 1, comma 209, della legge di bilancio 2019 ([L. n. 145/2018](#)), secondo le disposizioni di cui al decreto ministeriale attuativo del medesimo Fondo – [D.M. 27 giugno 2019](#) – del quale viene contestualmente previsto **un aggiornamento** relativo, a seguito alle modifiche apportate nel corso dell'esame in Senato, alle disposizioni del presente articolo, con **adeguamento** per gli investimenti nelle imprese di cui al comma 1, lettera b), non rientranti nella definizione di PMI.

Si ricorda che al fine di perseguire con maggiore efficacia l'obiettivo di promozione degli interventi nel capitale di rischio e garantire una adeguata sinergia con gli strumenti in essere, il citato D.M. ha previsto che il Fondo di sostegno al *venture capital* intervenga in fondi per il *venture capital*, istituiti e gestiti dalla CDPVC o da altre società autorizzate da Banca d'Italia a prestare il servizio di gestione collettiva del risparmio¹⁷. I fondi per il *venture capital* devono investire esclusivamente nel capitale di rischio di PMI con elevato potenziale di sviluppo ed innovative, non quotate in mercati regolamentati, che si trovano nella fase di sperimentazione (*seed financing*), di costituzione (*start-up financing*), di avvio dell'attività (*early-stage financing*) o di sviluppo del prodotto (*expansion, scale-up financing*).

La **relazione tecnica** precisa che la copertura della verticale d'investimento si trova nell'ambito delle **risorse del Fondo per il sostegno al *venture capital* nel suo complesso, già interamente sottoscritte e trasferite a CDPVC**. Il conto corrente di tesoreria in questione (n. 25095) per la gestione (fuori bilancio) degli interventi del Fondo, autorizzato

¹⁷ Contemporaneamente, il D.M. ha destinato agli investimenti nei fondi per il *venture capital* istituiti e gestiti dalla CDPVC o da altre società autorizzate da Banca d'Italia a prestare il servizio di gestione collettiva del risparmio, la somma di 200 milioni di euro già previsti con delibera CIPE n. 14 del 28 febbraio 2018, e assegnati al MISE dal comma 121 della legge di bilancio 2019.

dall'articolo 10, comma 7-*sexies*, ultimo periodo, del [D.L. n. 121/2021](#), ha attualmente una **consistenza di cassa di 1.770.826.854,97** euro.

L'articolo 1 della legge 30 dicembre 2018, n. 145, **legge di bilancio 2019**, ha introdotto disposizioni per una **razionalizzazione del sistema del *venture capital* nazionale** e, in particolare:

- a) il **comma 116**, ha previsto che, al fine di semplificare e rafforzare il settore del *venture capital* e il tessuto economico-produttivo del Paese, l'allora Ministero dello sviluppo economico (ora Ministero delle imprese e del *made in Italy*) potesse **autorizzare la cessione**, a condizioni di mercato, **da parte di Invitalia spa**¹⁸, di una **quota di partecipazione**, anche di controllo, **detenuta nella società di gestione del risparmio Invitalia Ventures Sgr spa - Invitalia Sgr**, nonché di una quota di partecipazione in fondi da essa gestiti, per favorire la gestione sinergica delle risorse (destinate al *venture capital*) del c.d. Fondo per la crescita sostenibile¹⁹, di quelle del c.d. Fondo imprese Sud²⁰, e di quelle del c.d. Fondo "Italia Venture III"²¹;
- b) il **comma 117** ha attribuito il **diritto di opzione a Cassa depositi e prestiti**, per l'**acquisto della quota di partecipazione azionaria** in Invitalia Sgr nonché della quota di partecipazione in fondi da essa gestiti.
In attuazione di quanto sopra previsto, la società CDP *Equity* ha acquistato quote di partecipazione di maggioranza in Invitalia Ventures Sgr. L'assemblea di Invitalia Ventures Sgr (70% CDP *Equity* e 30% Invitalia) tenutasi il 21 gennaio 2020, ha modificato il nome della società in CDP Venture Capital Sgr s.p.a. La **denominazione** è stata modificata in CDP Venture Capital Sgr s.p.a. - Fondo Nazionale Innovazione (qui il [comunicato stampa](#) e il [sito istituzionale dedicato](#));
- c) i **commi 206 e 207** hanno previsto la possibilità di **sottoscrizione** da parte dello **Stato**, tramite il MIMIT, di **quote o azioni** di uno o più **Fondi** per il ***venture capital*** o di uno o più **fondi** che investono in fondi per il ***venture capital***, come definiti dall'articolo 31, comma 2, del **D.L. n. 98 del 2011**²²,

¹⁸ L'Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa S.p.a. – Invitalia S.p.a. è interamente di proprietà del Ministero dell'Economia e finanze (MEF) (cfr. [qui](#)).

¹⁹ di cui all'art. 23 del D.L. n. 83/2012.

²⁰ di cui all'art. 1, comma 897, L. n. 205/2017.

²¹ di cui al comma 121 della stessa L. n. 145/2018.

²² L'**articolo 31 del D.L. n. 98/2011**, ha introdotto nell'ordinamento norme per **favorire l'accesso al *venture capital*** e sostenere i processi di crescita di nuove imprese, utilizzando lo strumento dell'**organismo di investimento collettivo del risparmio chiuso**, nonché delle società di investimento a capitale fisso. Il **comma 2 definisce "Fondi per il *Venture Capital*" (FVC)** gli organismi di investimento collettivo del risparmio chiusi e le società di investimento a capitale fisso, fiscalmente residenti in Italia o in uno degli Stati membri dell'UE o in Stati aderenti all'Accordo sullo Spazio economico europeo (SEE) compresi nell'apposito elenco del MEF, **che investono almeno l'85 per cento del valore degli attivi in piccole e medie imprese (PMI) non quotate in mercati regolamentati**, nella fase di sperimentazione (*seed financing*), di costituzione (*start-up financing*), di avvio dell'attività (*early-stage financing*) o di sviluppo del prodotto (*expansion o scale up financing*) e il residuo in PMI di cui all'articolo 1, comma 1, lettera w-quarter.1), del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58. (281)

anche unitamente ad altri investitori istituzionali, pubblici o privati, privilegiati nella ripartizione dei proventi derivanti dalla gestione dei predetti organismi di investimento. Il **D.M. 27 giugno 2019**, come da ultimo modificato dal **D.M. 16 luglio 2024**, in attuazione di quanto previsto dal comma 208, ha disciplinato le modalità d'investimento statale.

- d) il **comma 209**, ha previsto per le finalità di cui al citato comma 206, l'**istituzione**, nello stato di previsione dell'allora MISE (ora MIMIT), il **Fondo di sostegno al *venture capital***, dotandolo inizialmente di **30 milioni** di euro per ciascuno degli anni **2019, 2020 e 2021** e di **5 milioni** di euro per ciascuno degli anni dal **2022 al 2025**. Contestualmente, il **comma 216** ha previsto, ai fini di una successiva alimentazione del Fondo, che le **entrate** dello **Stato** derivanti dalla distribuzione di utili d'esercizio o di riserve sotto forma di **dividendi** delle **società partecipate** dal **MEF** possano essere utilizzate, **fino al 10 per cento** del loro ammontare, nel rispetto degli obiettivi di finanza pubblica, per gli investimenti in *venture capital* sopra indicati e che le somme introitate a tale titolo siano riassegnate, anche in deroga ai limiti previsti per le riassegnazioni, con decreto del Ministro dell'economia e delle finanze ad apposito capitolo dello stato di previsione della spesa del MEF per essere poi versate al Fondo, iscritto nello stato di previsione della spesa del MIMIT. Le disposizioni hanno trovato applicazione a decorrere dal 1° luglio 2019. Il Fondo è stato anche successivamente rifinanziato e definanziato per via legislativa. I definanziamenti sono stati disposti a titolo di parziale compensazione finanziaria delle misure recate nelle norme che li hanno previsti²³. Quanto ai **rifinanziamenti**, si rammenta che l'**articolo 10, comma 7-sexies**, del **D.L. n. 121/2021** – richiamato nella relazione tecnica del provvedimento in esame – al fine di favorire il settore del *venture capital*, ha autorizzato il MISE, ora MIMIT²⁴, a sottoscrivere fino a un ammontare pari a

²³ L'**articolo 38, comma 3**, del [D.L. n. 34/2020](#) ha disposto uno stanziamento aggiuntivo di **200 milioni** di euro per l'anno **2020**. Queste risorse sono state finalizzate a sostenere investimenti nel capitale, anche tramite la sottoscrizione di strumenti finanziari partecipativi, nonché l'erogazione di finanziamenti agevolati, la sottoscrizione di obbligazioni convertibili, o altri strumenti finanziari di debito che prevedano la possibilità del rimborso dell'apporto effettuato, a beneficio esclusivo delle **startup innovative e delle PMI innovative**. In attuazione, è stato adottato il D.M. 1 ottobre 2020, modificato da ultimo dal D.M. 12 giugno 2023.

L'**articolo 1, comma 107** della **legge di bilancio 2021** (L. n.178/2020) ha stanziato 3 milioni di euro per l'anno 2021 per il Fondo finalizzando tali risorse a sostenere investimenti nel capitale di rischio per progetti di imprenditoria femminile a elevata innovazione ovvero a contenuto di innovazione tecnologica, che prevedono il rientro dell'investimento iniziale esclusivamente nel lungo periodo, realizzati entro i confini del territorio nazionale da società il cui capitale è detenuto in maggioranza da donne. In attuazione, è stato adottato il D.M. 27 dicembre 2021.

Il Fondo ha poi subito una **riduzione** di 300 milioni di euro per l'anno 2024 ad opera dell'articolo 4, comma 4, lett. *b*), della [legge n. 206/2023](#) (c.d. legge sul *made in Italy*) a titolo di parziale compensazione dell'onere derivante dalla costituzione del c.d. Fondo nazionale del *made in Italy*.

²⁴ nel rispetto della disciplina sugli aiuti di stato relativa agli "Orientamenti sugli aiuti di Stato destinati a promuovere gli investimenti per il finanziamento del rischio".

2 miliardi di euro da versare al Fondo²⁵. In attuazione, è stato adottato il **decreto 26 luglio 2022**, che disciplina nel dettaglio le modalità di impiego di tali somme. Come ricordato dalla relazione tecnica del disegno di legge qui in commento, l'**articolo 10, comma 7-sexies** – per la gestione degli interventi – ha autorizzato l'apertura di un **apposito conto corrente** presso la Tesoreria centrale dello Stato, **intestato al MIMIT**, cui affluiscono le **risorse ad esso assegnate** e sul quale la **CDP spa è autorizzata a effettuare operazioni di versamento e di prelevamento**.

Si rileva che a **legge di bilancio 2025** (L. n. 207/2024) il capitolo di spesa 7344/MIMIT, su cui sono iscritte le risorse del Fondo per il sostegno al *venture capital* reca una previsione di 5 milioni per il 2025, e non prevede ulteriori finanziamenti per gli anni successivi. In argomento si veda anche la [relazione annuale al Parlamento](#) presentata dal MIMIT nel 2024 **sullo stato di attuazione** e le *policy* a sostegno di *startup* e PMI innovative (in particolare da p. 56).

Il **comma 3**, dispone che oltre al MIMIT, in qualità di investitore, **partecipano agli organi di governo** dei fondi di *venture capital*, con propri rappresentanti, in ragione delle proprie competenze, la struttura della **Presidenza del Consiglio dei ministri** competente in materia di innovazione tecnologica e transizione digitale e l'**Agenzia per la cybersicurezza** nazionale, in ogni caso senza compensi o indennità.

²⁵ le risorse sono state reperite a valere su quelle, iscritte in conto residui nello stato di previsione del Ministero dell'economia e delle finanze, autorizzate ai sensi dell'art. 27 del D.L. n. 34/2020, per le finalità del cd. "Patrimonio destinato", strumento la cui gestione è stata affidata a CDP.

Articolo 24, commi 1, 2 e 6
(Delega al Governo per l'adeguamento della normativa nazionale al regolamento dell'Unione europea in materia di intelligenza artificiale)

L'**articolo 24, commi 1 e 2**, contiene una delega al Governo per l'adozione, entro dodici mesi dall'entrata in vigore del provvedimento, di uno o più decreti legislativi che adeguino la normativa nazionale al [regolamento \(UE\) 2024/1689 del Parlamento europeo e del Consiglio](#), cd. "AI Act".

L'esercizio della delega è subordinato al rispetto di principi e criteri direttivi specifici, posti dal **comma 2**. Quest'ultimo, inoltre, richiama i principi e criteri generali di delega previsti per l'attuazione delle norme dell'Unione europea.

Le **lettere a), b), c), d)** del **comma 2** (introdotte nel corso dell'esame presso il Senato) dispongono circa l'adeguamento del diritto nazionale in materia di **poteri, anche sanzionatori, delle autorità nazionali competenti**, come individuate dall'**articolo 20**.

La successiva **lettera e)** concerne i percorsi di **alfabetizzazione e formazione** in materia di strumenti di intelligenza artificiale, rivolti anche – **lettera f)** – ai **professionisti** che fanno uso di tali strumenti. La suddetta **lettera f)** prevede anche la possibilità del riconoscimento di un equo compenso, modulabile sulla base dei rischi e delle responsabilità connessi all'uso dell'intelligenza artificiale da parte del professionista.

Le **lettere g), i) ed l)** **recano** principi e criteri direttivi specifici per l'esercizio della delega legislativa in materia di **istruzione scolastica, formazione superiore e ricerca**. Tali principi e criteri direttivi fanno riferimento: al potenziamento, all'interno dei curricula scolastici, dello sviluppo di competenze legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta di percorsi di formazione superiore relativi alle menzionate discipline (**lettera g)**); alla previsione, nei corsi universitari e delle istituzioni AFAM, nonché nei percorsi di istruzione tecnologica superiore offerti dagli ITS *Academy*, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale così come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni (**lettera i)**); alla valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni dell'AFAM, ITS *Academy* ed enti

pubblici di ricerca, mediante disposizioni finalizzate al perseguimento di alcuni obiettivi specificamente indicati (**lettera l**)).

È stato introdotto (dal Senato) un ulteriore criterio di delega concernente la previsione di un'apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'**attività di polizia (lettera h)**).

Le **lettere m) e n)** (introdotte anch'esse in Senato) riguardano, rispettivamente, specifici poteri di vigilanza del mercato nei confronti di fornitori e potenziali fornitori di sistemi di IA e l'adeguamento del sistema sanzionatorio nazionale.

Il **comma 6** reca una clausola di **invarianza finanziaria**.

I **commi 1 e 2** dell'articolo in commento recano una **delega al Governo** per l'adozione, **entro dodici mesi** dall'entrata in vigore del provvedimento, di uno o più **decreti legislativi** per adeguare la normativa nazionale al [regolamento \(UE\) 2024/1689 del Parlamento europeo e del Consiglio](#), cd. "*AI Act*".

Brevi cenni sul regolamento dell'Unione europea

In via di sintesi, il suddetto regolamento dell'Unione europea: stabilisce le pratiche vietate in materia; reca una disciplina specifica per i sistemi di intelligenza artificiale ad alto rischio, prevedendo anche una relativa banca dati; stabilisce alcuni obblighi di trasparenza a carico dei produttori e dei gestori (*deployers*) di determinati sistemi di intelligenza artificiale e pone in capo ai produttori la responsabilità sulla sussistenza di alcuni requisiti dei prodotti (tra i sistemi interessati da tali obblighi o responsabilità figurano quelli destinati ad interagire direttamente con le persone fisiche e quelli che generano contenuti audio, immagine, video o testuali sintetici); reca una disciplina specifica sui modelli di intelligenza artificiale per finalità generali (modelli che presentano un elevato livello di generalità); reca norme sulla sperimentazione in materia di intelligenza artificiale; disciplina la *governance* del settore a livello di Unione europea e di autorità nazionali; disciplina il monitoraggio sul mercato e la condivisione delle informazioni; fa riferimento a codici di condotta e ad orientamenti.

Per un esame più dettagliato della disciplina posta dal regolamento dell'Unione europea si rinvia al paragrafo finale della presente scheda.

Procedura per l'adozione dei decreti legislativi (comma 1)

Per la **procedura per l'adozione** dei decreti legislativi, il **comma 1** del presente **articolo 24** fa rinvio a quella stabilita dall'articolo 31 della [legge](#)

[24 dicembre 2012, n. 234](#), recante “Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea”; il medesimo **comma 1** prevede l'acquisizione del parere – oltre che delle Commissioni parlamentari competenti – del Garante per la protezione dei dati personali nonché della Conferenza unificata Stato-regioni-province autonome-città ed autonomie locali.

L'**articolo 31** della legge 24 dicembre 2012, n. 234, disciplina le procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea²⁶.

Il **comma 2** di tale articolo specifica che i decreti legislativi sono adottati su **proposta** del Presidente del Consiglio dei Ministri o del Ministro per gli affari europei e del Ministro con competenza prevalente nella materia. Questi agiscono di concerto con i Ministri degli affari esteri, della giustizia, dell'economia e delle finanze e con gli altri Ministri interessati. L'amministrazione con competenza istituzionale prevalente predispone una tabella di concordanza tra le disposizioni introdotte e quelle della direttiva da recepire.

Lo **schema procedurale** è disciplinato in via generale dal **comma 3**: gli **schemi di decreto legislativo**, una volta acquisiti gli altri pareri previsti dalla legge, sono trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti. Decorsi **quaranta giorni** dalla data di trasmissione, essi sono emanati anche in assenza del parere. Qualora il termine fissato per l'espressione del parere parlamentare scada nei trenta giorni che precedono il termine per l'esercizio della delega o successivamente, il termine è **prorogato di tre mesi**. Si intende in tal modo permettere al Governo di usufruire in ogni caso di un adeguato periodo di tempo per l'eventuale recepimento, nei decreti legislativi, delle indicazioni emerse in sede parlamentare.

Sugli **schemi** di decreto legislativo che comportino conseguenze finanziarie è previsto anche il **parere delle Commissioni parlamentari competenti per i profili finanziari (comma 4)**; tali schemi devono essere corredati di una **relazione tecnica**; nel caso in cui non intenda conformarsi alle condizioni formulate da tali Commissioni, il Governo ritrasmette al Parlamento i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle medesime Commissioni competenti per i profili finanziari, che devono essere espressi entro venti giorni. Il **comma 9** prevede altresì l'ipotesi che il Governo *non* intenda conformarsi ai pareri espressi dagli organi parlamentari su norme contenenti **sanzioni penali**. In tal caso ritrasmette i testi alle Camere, con

²⁶ Il termine temporale per l'esercizio della delega è stabilito in via diretta, come detto, dal **comma 1** del presente **articolo 24**. Si ricorda in ogni caso che il comma 1 del summenzionato articolo 31 prevede che il termine per l'esercizio delle deleghe sia di quattro mesi antecedenti il termine di recepimento indicato in ciascuna delle direttive. Qualora il termine così determinato sia già scaduto alla data di entrata in vigore della legge di delegazione europea, o scada nei tre mesi successivi, la delega deve invece essere esercitata entro tre mesi dalla data di entrata in vigore della legge. In assenza di termine di recepimento, il termine è di dodici mesi.

osservazioni ed eventuali modificazioni. I decreti sono emanati anche in mancanza di parere dopo venti giorni dalla data di ritrasmissione.

Il **comma 5** prevede la possibilità per il Governo di adottare **disposizioni integrative e correttive entro 24 mesi** dalla data di entrata in vigore di ciascun decreto legislativo. È comunque necessario garantire il rispetto dei principi e criteri direttivi fissati in origine dalla legge stessa. Analoga possibilità è disciplinata dal **comma 6** al fine di recepire il contenuto di atti delegati dell'Unione europea che modificano o integrano le direttive di origine.

I **commi 7 e 8** disciplinano i decreti di recepimento di direttive adottati materie di competenza legislativa delle regioni e delle province autonome.

Principi e criteri direttivi generali per l'esercizio della delega (comma 2, alinea)

Ai sensi del **comma 2** del presente **articolo 24**, l'esercizio della delega è subordinato *in primis* ai **principi e criteri direttivi generali** elencati nell'articolo 32 della citata [legge 24 dicembre 2012, n. 234](#) (principi e criteri di delega posti per l'attuazione delle norme dell'Unione europea).

I principi e criteri direttivi indicati dall'**articolo 32** della legge n. 234 del 2012 sono, in estrema sintesi, i seguenti:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture, secondo il principio della massima **semplificazione dei procedimenti**;

b) ai fini di un migliore **coordinamento con le discipline vigenti** sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il **riassetto e la semplificazione della normativa**;

c) gli atti di recepimento di direttive non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse (c.d. **gold plating**);

d) ove necessario, al fine di assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste **sanzioni amministrative e penali** per le infrazioni alle disposizioni dei decreti stessi. In ogni caso le sanzioni penali sono previste "solo nei casi in cui le infrazioni ledano o esponano a pericolo interessi costituzionalmente protetti". In merito alle norme di delega in materia sanzionatoria, cfr. anche le parti della presente scheda relative alle **lettere a-quinquies) e f-ter)** del **comma 2** nonché la scheda sulla successiva disciplina di delega di cui ai **commi da 3 a 5** del presente **articolo 24**.

Si segnala che l'articolo 99 del regolamento europeo in oggetto prevede che gli Stati membri stabiliscano **sanzioni effettive, proporzionate e dissuasive**, comprese sanzioni **amministrative pecuniarie**, in relazione alle violazioni del regolamento medesimo. Le sanzioni adottate dagli Stati membri sono soggette ad obbligo di comunicazione alla Commissione europea.

Sono stabilite le seguenti **soglie massime, a cui devono attenersi le norme sanzionatorie dei singoli Stati membri:**

- fino a 35 milioni di euro o al 7% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore²⁷) per violazioni relative alle pratiche vietate di cui all'articolo 5 del regolamento (riguardo a tale articolo, cfr. il paragrafo finale della presente scheda);
- fino a 15 milioni di euro o al 3% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore²⁸), per l'inosservanza di qualsiasi altro requisito o obbligo del regolamento, posto in capo a produttori, rappresentanti autorizzati, importatori, distributori, gestori (*deployers*), nonché degli obblighi di trasparenza posti in capo a produttori e *deployers* e dei requisiti e obblighi degli organismi notificati;
- fino a 7,5 milioni di euro o all'1,5% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore²⁹), per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti.

Per le PMI, comprese le *start-up*, si prevede l'applicazione della soglia massima più bassa tra quella in valore percentuale e quella in valore assoluto.

In materia sanzionatoria, cfr. altresì;

e) al recepimento di direttive o di altri atti che modificano precedenti direttive o di atti già attuati con legge o con decreto legislativo si procede **apportando le corrispondenti modificazioni** alla legge o al decreto legislativo di attuazione;

f) nella redazione dei decreti legislativi si tiene conto delle **eventuali modifiche delle direttive**, intervenute fino al momento dell'esercizio della delega;

g) quando si verificano sovrapposizioni di competenze tra amministrazioni diverse o siano coinvolte le **competenze di più amministrazioni statali**, i decreti legislativi individuano le procedure per salvaguardare l'unitarietà dei processi decisionali, l'efficacia e la trasparenza dell'azione amministrativa, nel rispetto dei principi di sussidiarietà e delle competenze delle regioni e degli enti territoriali;

h) le direttive che riguardano le stesse materie o che comportano modifiche degli stessi atti normativi vengono attuate con un **unico decreto legislativo**, compatibilmente con i diversi termini di recepimento;

i) è sempre assicurata la **parità di trattamento** dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea né può essere previsto un trattamento sfavorevole dei cittadini italiani.

Principi e criteri direttivi specifici per l'esercizio della delega (comma 2, lettere a) - n))

²⁷ Per le PMI, comprese le *start-up*, cfr. *infra*.

²⁸ Per le PMI, comprese le *start-up*, cfr. *infra*.

²⁹ Per le PMI, comprese le *start-up*, cfr. *infra*.

Le lettere da *a*) a *n*) del **comma 2** recano i **principi e criteri direttivi di delega specifici**.

Autorità nazionali (comma 2, lettere a), b), c) e d))

Nel corso dell'esame presso il Senato è stata soppressa la lettera *a*) del testo del disegno di legge originario. La **lettera a) del testo originario** prevedeva che nell'attuazione della delega il Governo designasse l'autorità di vigilanza del mercato, l'autorità di notifica, nonché il punto di contatto con le istituzioni dell'Unione europea. Tali soggetti dovevano essere individuati in coerenza con quanto previsto dall'**articolo 20** del presente provvedimento, concernente le autorità nazionali per l'attuazione della disciplina in materia di intelligenza artificiale. Resta fermo che l'**articolo 20**, come modificato dal Senato, disciplina in via diretta le autorità nazionali (cfr. la relativa scheda), mentre è stato soppresso il principio di delega, di cui alla suddetta originaria lettera *a*), relativo all'individuazione delle medesime autorità.

Si ricorda che il capo VII del regolamento dell'Unione europea in oggetto prevede la designazione, da parte dei singoli Stati membri, di almeno un'**autorità di vigilanza del mercato** e di almeno un'**autorità nazionale di notifica**; l'autorità di vigilanza del mercato – o una di esse, in caso di pluralità di autorità designate – funge da **punto di contatto unico**. Tali autorità costituiscono le **autorità nazionali competenti** (ai fini dell'attuazione del regolamento medesimo)³⁰.

La **lettera a)** attribuisce alle suddette autorità nazionali competenti designate tutti i poteri di vigilanza, ispettivi e sanzionatori previsti sia dal [Regolamento \(UE\) 2024/1689](#) per la verifica del rispetto delle disposizioni del Regolamento stesso sia dalla normativa dell'Unione europea attuativa del medesimo Regolamento.

La **lettera b)** dispone l'adeguamento al medesimo Regolamento n. 1689 della normativa nazionale, ivi inclusa quella in materia di servizi bancari, finanziari, assicurativi e di pagamento.

La **lettera c)** stabilisce che, nell'esercizio della delega, si ricorra, ove opportuno, alla disciplina secondaria adottata dalle suddette autorità nazionali competenti, nel rispetto delle competenze delle medesime autorità, nell'ambito e per le finalità specificamente previsti dal Regolamento n. 1689 e dalla normativa dell'Unione europea attuativa del medesimo regolamento.

³⁰ Riguardo al regolamento, cfr. il paragrafo finale della presente scheda.

La **lettera d)** attribuisce alle medesime autorità il potere di imporre le sanzioni e le altre misure amministrative previste dall'articolo 99 del Regolamento (UE) 2024/1689, per la violazione delle norme del Regolamento stesso e dei relativi provvedimenti di attuazione, nel rispetto dei limiti edittali e delle procedure previsti dall'articolo 99 del Regolamento nonché nel rispetto delle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure amministrative da parte delle autorità anzidette. Riguardo alle disposizioni di cui al suddetto articolo 99, si rinvia alla parte della presente scheda relativa ai principi e criteri direttivi generali per l'esercizio della delega (**comma 2, alinea**). Riguardo al quadro sanzionatorio, cfr. anche il criterio di delega di cui alla successiva **lettera n)** nonché la disciplina di delega di cui ai **commi da 3 a 5** del presente **articolo 24**.

Alfabetizzazione e formazione (comma 2, lettere e) e f)

Le **lettere e)** e **f)** stabiliscono che, nell'attuazione della delega, il Governo preveda percorsi di **alfabetizzazione e formazione nell'uso dei sistemi di intelligenza artificiale**.

In particolare, la **lettera e)** stabilisce che gli ordini professionali – nonché, come inserito nel corso dell'esame in Senato, le associazioni di categoria maggiormente rappresentative e le forme aggregative delle associazioni professionali di cui all'articolo 3 della [L. 14 gennaio 2013, n. 4](#)³¹ – possano prevedere percorsi dedicati **ai professionisti e agli operatori del settore di competenza**. La medesima **lettera** prevede la possibilità del riconoscimento **di un equo compenso**, modulabile sulla base dei **rischi** e delle **responsabilità** connessi all'uso dell'intelligenza artificiale da parte del professionista.

Riguardo alle norme in materia di alfabetizzazione di cui all'**articolo 4** del regolamento europeo in oggetto, si rinvia al paragrafo finale della presente scheda.

Si ricorda che la [legge 21 aprile 2023, n. 49](#), reca disposizioni in materia di **equo compenso** delle prestazioni professionali (v. il [dossier di documentazione](#) sull'A.C. 338-B, ultima lettura parlamentare). La legge interviene, tra l'altro, sull'ambito applicativo della disciplina vigente, ampliandolo sia per quanto riguarda i professionisti interessati - tra i quali sono inclusi gli esercenti professioni non ordinistiche - sia per quanto riguarda la committenza che viene estesa anche a tutte le imprese che impiegano più di 50 dipendenti o fatturano più di 10 milioni di euro. L'articolo 1 della citata legge n. 49 stabilisce che per essere considerato "equo" il compenso deve essere proporzionato alla quantità e qualità del lavoro svolto e al contenuto e alle caratteristiche della prestazione

³¹ La suddetta L. n. 4 del 2013 reca norme in materia di professioni non organizzate.

professionale nonché conforme ai parametri per la determinazione dei compensi previsti dalla legge.

Istruzione scolastica, formazione superiore e ricerca (comma 2, lettere g), i), l))

Nel dettaglio, il **comma 2**, alle **lettere g), i), l)**, enuncia i seguenti principi e criteri direttivi specifici ai quali il Governo deve attenersi nell'esercizio della delega conferitagli dal **comma 1**:

- potenziamento, all'interno dei curricula scolastici, dello sviluppo di competenze scientifiche, tecnologiche, ingegneristiche e matematiche legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta da parte delle studentesse e degli studenti, anche attraverso mirate attività di orientamento personalizzato, di percorsi di formazione superiore relativi alle menzionate discipline (**lettera g**);

Per quanto concerne i curricula relativi ai diversi percorsi della scuola secondaria di secondo grado si veda l'apposita [pagina](#) sul sito Unica del Ministero dell'istruzione e del merito.

- previsione, nei corsi universitari e delle istituzioni di alta formazione artistica, musicale e coreutica (AFAM), nonché nei percorsi di istruzione tecnologica superiore offerti dagli istituti tecnologici superiori (ITS *Academy*), coerentemente con i rispettivi profili culturali e professionali, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale così come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni (**lettera i**);

Si rammenta in proposito che un "sistema di IA" è 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 (articolo 3, n. 1), del regolamento 2024/1689 del Parlamento europeo e del Consiglio UE del 2024).

Le istituzioni di alta formazione e specializzazione artistica e musicale (AFAM), ai sensi della legge n. 508 del 1999, sono le seguenti: le Accademie di belle arti, l'Accademia nazionale di arte drammatica, l'Accademia nazionale di danza, gli Istituti superiori per le industrie artistiche (ISIA), i Conservatori di musica e gli Istituti musicali pareggiati.

L'elenco completo dei 105 istituti è riportato [sul sito del Ministero dell'università e della ricerca](#).

Per un approfondimento sulle istituzioni AFAM, si consulti [la sezione](#) ad esse dedicata all'interno dell'area tematica dedicata a "Le misure destinate agli studenti universitari e alle istituzioni AFAM, il diritto allo studio e la formazione professionale" del portale della documentazione della Camera dei Deputati.

Si ricorda che la [legge 15 luglio 2022, n. 99](#) ("*Istituzione del Sistema terziario di istruzione tecnologica superiore*"), composta di 16 articoli, ha introdotto nell'ordinamento una normativa organica di rango legislativo per gli Istituti tecnici superiori (ITS), inizialmente disciplinati - nei loro tratti essenziali - principalmente da una fonte di rango secondario, il [DPCM del 25 gennaio 2008](#) recante "*Linee guida per la riorganizzazione del Sistema di istruzione e formazione tecnica superiore e la costituzione degli Istituti tecnici superiori*". Tale legge è stata approvata in attuazione della riforma del sistema ITS (M4-C1-R.1.2) prevista dal Piano nazionale di ripresa e resilienza (PNRR), la quale aveva come primo traguardo, al 31 dicembre 2022, l'adozione della riforma (attuata, appunto, con l'approvazione della legge n. 99 del 2022). Il successivo (e ultimo) traguardo di tale riforma è stato fissato al 31 dicembre 2023, e consiste nell'entrata in vigore delle disposizioni per l'efficace attuazione e applicazione di tutte le misure relative alla riforma, ove necessario. Per un approfondimento sulle riforme e sugli investimenti del PNRR relativi al settore dell'istruzione, e sul loro stato di attuazione, si rinvia all'[apposita sezione del Portale della documentazione](#) della Camera dei deputati.

- valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni dell'AFAM, ITS *Academy* ed enti pubblici di ricerca, mediante disposizioni finalizzate al perseguimento dei seguenti obiettivi (**lettera I**):

1) agevolare il coinvolgimento del sistema dell'università e della ricerca nella promozione, nella realizzazione e nell'utilizzo di spazi di sperimentazione normativa in collaborazione con il mondo produttivo;

2) incentivare le attività di supporto e semplificare gli strumenti di collaborazione del sistema dell'università e della ricerca e degli ITS *Academy* con le autorità nazionali (individuate dal precedente **articolo 20**) competenti per l'attuazione delle norme in materia di intelligenza artificiale.

In base all'articolo 1, comma 1, del d.lgs. n. 218/2016, gli enti pubblici di ricerca sono i seguenti: Area di Ricerca Scientifica e Tecnologica di Trieste - Area Science Park; Agenzia Spaziale Italiana - ASI; Consiglio Nazionale delle Ricerche - CNR; Istituto Italiano di Studi Germanici; Istituto Nazionale di Astrofisica - INAF; Istituto Nazionale di Alta Matematica "Francesco Severi" - INDAM; Istituto Nazionale di Fisica Nucleare - INFN;

Istituto Nazionale di Geofisica e Vulcanologia - INGV; Istituto Nazionale di Oceanografia e di Geofisica Sperimentale - OGS; Istituto Nazionale di Ricerca Metrologica - INRIM; Museo Storico della Fisica e Centro Studi e Ricerche "Enrico Fermi"; Stazione Zoologica "Anton Dohrn"; Istituto Nazionale per la Valutazione del Sistema Educativo di Istruzione e di Formazione - INVALSI; Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa - INDIRE; Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria - CREA; Agenzia Nazionale per le Nuove Tecnologie, l'energia e lo Sviluppo Sostenibile - ENEA; Istituto per lo Sviluppo della Formazione Professionale dei Lavoratori - ISFOL (a decorrere dal 1° dicembre 2016 denominato Istituto nazionale per l'analisi delle politiche pubbliche - INAPP); Istituto Nazionale di Statistica - ISTAT; Istituto Superiore di Sanità - ISS; Istituto Superiore per la Protezione e la Ricerca Ambientale – ISPRA.

Attività di polizia (comma 2, lettera h)

È stato introdotto un ulteriore criterio di delega concernente la previsione di un'apposita disciplina per l'**utilizzo di sistemi di intelligenza artificiale per l'attività di polizia**.

Si rammenta che il regolamento 2024/1689 reca le definizioni di “autorità di contrasto” e di “attività di contrasto”, ossia le attività inerenti a 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. Il regolamento annovera tra i “sistemi ad alto rischio” quelli utilizzati per le suddette attività di contrasto. L’art. 46 del regolamento prevede deroghe alla procedura di valutazione della conformità ai sistemi di IA ad alto rischio per l’utilizzo di tali sistemi da parte di autorità di contrasto o di protezione civile, salvo l’obbligo di autorizzazione durante o successivamente a tale utilizzo. Inoltre, l’art. 5, par. 1, lett. *h*), del medesimo regolamento prevede la possibilità di utilizzare sistemi di identificazione biometrica remota «in tempo reale», altrimenti vietate, in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per taluni obiettivi connessi alle attività di contrasto, Si veda *infra* il quadro riassuntivo dedicato al regolamento. Si veda anche il Documento EUROPOL “[AI and policing](#)” (2024).

Poteri di vigilanza e sistema sanzionatorio (comma 2, lettere m) ed n)

La **lettera m)** prevede che, nell’attuazione della delega, il Governo definisca i **poteri di vigilanza dell'autorità di vigilanza del mercato**; il presente principio di delega prevede che tale autorità possa: imporre ai fornitori e ai potenziali fornitori di trasmettere informazioni; effettuare ispezioni a distanza o *in loco*, anche senza preavviso; svolgere controlli

sulla conduzione delle prove in condizioni reali e sui relativi sistemi di IA ad alto rischio.

Si segnala che l'articolo 60 del Regolamento reca una disciplina specifica inerente alla prova dei sistemi ad alto rischio in condizioni reali, senza che i fornitori o potenziali fornitori partecipino a uno spazio di sperimentazione normativa per l'IA. Come evidenziato dal considerato n. 141 del medesimo Regolamento, in tali casi, anche tenendo conto delle possibili conseguenze di tali prove sulle persone, è opportuno garantire che le norme applicabili introducano garanzie e condizioni adeguate e sufficienti per i fornitori o potenziali fornitori. A tale riguardo, si rinvia al paragrafo finale della presente scheda sul regolamento (UE) 2024/1689, con particolare riferimento al capo VI sulle misure a sostegno dell'innovazione (artt. 57-63).

La **lettera n)** dispone circa l'**adeguamento del quadro sanzionatorio**, anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera *d*), della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, ivi compresa la definizione delle misure di esecuzione applicabili ai sensi del Regolamento (UE) 2024/1689, nonché del procedimento applicabile per l'irrogazione delle sanzioni o l'applicazione delle misure di esecuzione, anche in coerenza con quanto previsto (riguardo alla disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale) dall'articolo 17, comma 4-*quater*, del [D.L. 14 giugno 2021, n. 82, convertito, con modificazioni, dalla L. 4 agosto 2021, n. 109](#). In materia sanzionatoria, cfr. anche il principio di delega di cui alla precedente **lettera d)** nonché la disciplina di delega di cui ai **commi da 3 a 5** del presente **articolo 24**. *Si segnala che la Commissione Giustizia del Senato, nel [parere](#) espresso il 19 marzo 2025, ha rilevato "l'opportunità di un approfondimento del criterio di delega in esame alla luce della giurisprudenza costituzionale che impone al legislatore delegante, in ambito penale, di adottare principi e criteri direttivi configurati in modo preciso, sia definendo la specie e l'entità massima delle pene, sia dettando il criterio, in sé restrittivo, del ricorso alla sanzione penale solo per la tutela di determinati interessi rilevanti"*.

Per quanto concerne l'art. 32, comma 1, lettera *d*), della [legge n. 234/2012](#), nonché le sanzioni di competenza del singolo Stato membro, previste dall'art. 99 del Regolamento, si rinvia alla parte della presente scheda relativa ai principi e criteri direttivi generali per l'esercizio della delega (**comma 2, alinea**).

Si rammenta che la [legge n. 689/1981](#) ("Modifiche al sistema penale") reca la disciplina generale in tema di sanzioni amministrative. L'articolo 11 della legge n. 90/2024 – che inserisce un comma 4-*quater* nel citato articolo 17 del D.L. n. 82 del 2021 – reca disposizioni in materia di procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la cybersicurezza nazionale. Per

approfondimenti sul suddetto articolo 11 e sulla richiamata legge n. 698/1981, cfr. la scheda su art. 11 del dossier di documentazione sull' [A.S. 1143](#) (approvato definitivamente. L. 90/2024).

Clausola di invarianza finanziaria (comma 6)

Il **comma 6** stabilisce che dall'attuazione del presente **articolo 24** (v. anche la scheda sui **commi da 3 a 5**) non derivino **nuovi o maggiori oneri a carico della finanza pubblica**. Le amministrazioni provvedono con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Quadro sul regolamento del Parlamento europeo e del Consiglio 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)

In via di sintesi (come già detto nella parte precedente della scheda), il [regolamento \(UE\) 2024/1689](#) in oggetto: stabilisce le pratiche vietate in materia; reca una disciplina specifica per i sistemi di intelligenza artificiale ad alto rischio, prevedendo anche una relativa banca dati; stabilisce alcuni obblighi di trasparenza a carico dei produttori e dei gestori (*deployers*) di determinati sistemi di intelligenza artificiale e pone in capo ai produttori la responsabilità sulla sussistenza di alcuni requisiti dei prodotti (tra i sistemi interessati da tali obblighi o responsabilità figurano quelli destinati ad interagire direttamente con le persone fisiche e quelli che generano contenuti audio, immagine, video o testuali sintetici); reca una disciplina specifica sui modelli di intelligenza artificiale per finalità generali (modelli che presentano un elevato livello di generalità); reca norme sulla sperimentazione in materia di intelligenza artificiale; disciplina la *governance* del settore a livello di Unione europea e di autorità nazionali; disciplina il monitoraggio sul mercato e la condivisione delle informazioni; fa riferimento a codici di condotta e ad orientamenti.

Il 13 marzo 2024 il Parlamento europeo ha approvato il regolamento sull'intelligenza artificiale (IA), facendo seguito all'[accordo già raggiunto con il Consiglio dell'Unione europea nel dicembre 2023](#). Il testo è stato formalmente adottato dal Consiglio Telecomunicazioni nella seduta del 21 maggio 2024.

Principali **obiettivi** del regolamento sono (così come esplicitati in particolare ai considerando 1 e 2):

- migliorare il funzionamento del mercato interno dell'Unione, istituendo un quadro giuridico uniforme, in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA);
- 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 nell'Unione;
- promuovere l'innovazione e l'occupazione;
- assicurare all'Unione un ruolo guida in tale settore.

Si traccia di seguito un quadro sulle principali disposizioni contenute nel [regolamento \(UE\) 2024/1689](#).

Il **capo I** definisce l'**oggetto** del regolamento e l'**ambito di applicazione** delle nuove regole, le quali concernono **l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA nell'Unione** (artt. 1-4).

L'art. 1 specifica che il regolamento stabilisce:

- divieti di talune pratiche di IA;
- requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi;
- regole di trasparenza armonizzate per determinati sistemi di IA;
- regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali;
- regole in materia di monitoraggio del mercato, vigilanza del mercato, *governance* ed esecuzione;
- misure a sostegno dell'innovazione, con particolare attenzione alle PMI, comprese le *start-up*.

Il regolamento **si applica** ai soggetti pubblici e privati, all'interno e all'esterno dell'UE, con riferimento ai casi in cui il sistema di IA sia immesso sul mercato dell'Unione o in cui il suo uso abbia effetti su persone situate nell'UE.

L'art. 3 contiene le '**definizioni**' applicate ai fini del regolamento. In particolare, per **sistema di IA** si intende "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".

L'art. 4 stabilisce che i produttori e i gestori³² adottino misure per garantire, “nella misura del possibile”, un **livello sufficiente di alfabetizzazione** in materia di intelligenza artificiale del personale e degli altri soggetti che facciano uso di sistemi di IA per conto dei medesimi produttori o gestori.

Il capo I è integrato dall'**allegato I**, contenente un elenco della normativa di armonizzazione dell'Unione (elenco a cui fanno riferimento alcune norme del regolamento, cfr. *infra* in merito).

Il **capo II** stabilisce le **pratiche di IA vietate** (art. 5).

Sono vietati l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA volto a:

1. utilizzare **tecniche subliminali** che agiscano 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;
2. **sfruttare 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, in un modo che provochi o possa ragionevolmente provocare un danno significativo;
3. la valutazione o la classificazione delle persone fisiche o di gruppi di persone **sulla base del loro comportamento sociale o di caratteristiche** (personali o della personalità) note, inferite o previste, qualora il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:
 - a. un trattamento pregiudizievole o sfavorevole in contesti sociali che non siano collegati ai contesti in cui i dati siano stati originariamente generati o raccolti;
 - b. un trattamento pregiudizievole o sfavorevole che sia ingiustificato o sproporzionato rispetto al comportamento sociale dei soggetti o alla sua gravità;
4. 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 del coinvolgimento di una persona in un'**attività criminosa**);

³² Riguardo ai termini, usati nella presente esposizione, di produttori e gestori, cfr. *infra*, anche in nota.

5. creare o ampliare le banche dati di riconoscimento facciale mediante *scraping*³³ **non mirato di immagini facciali** da internet o da filmati di telecamere a circuito chiuso;
6. **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 utilizzato a **fini medici o di sicurezza**);
7. classificare 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 sulla base della categorizzazione di dati biometrici³⁴, nel settore delle **attività di contrasto**³⁵;
8. l'uso di **sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto**, a meno che (e nella misura in cui) tale uso sia strettamente necessario per uno degli obiettivi seguenti:
 - a. la **ricerca mirata di vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale**, nonché la **ricerca di persone scomparse**;
 - b. 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**;
 - c. la localizzazione o l'identificazione di una persona sospettata di aver commesso uno dei reati di cui all'allegato II del regolamento, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni³⁶.

³³ Il *web scraping* (dall'inglese *to scrape*, grattare/raschiare) è una particolare tecnica di *crawling*. Un *crawler* – chiamato anche *bot* o *spider* – è un *software* che ha lo scopo di raccogliere tutte le informazioni necessarie per indicizzare in modo automatico le pagine di un sito, analizzare i collegamenti ipertestuali e trovare associazioni fra termini di ricerca e classificarli (definizione fornita dal sito [Agenda digitale europea](#)).

³⁴ Si ricorda che il presente regolamento definisce la "categorizzazione biometrica" come l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici.

³⁵ Le attività di contrasto sono così definite dal regolamento in oggetto: "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".

³⁶ Il regolamento specifica che ogni uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto dovrà essere subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui avviene

Si ricorda che, anche in considerazione della decorrenza, dal 2 febbraio 2025, dell'applicazione del presente articolo 5³⁷, la Commissione europea, il 4 febbraio 2025, ha pubblicato, ai sensi dell'articolo 96 del presente regolamento³⁸, una comunicazione recante, in allegato, lo schema degli orientamenti sulle pratiche vietate in materia di intelligenza artificiale³⁹. Tali orientamenti saranno formalmente adottati dalla Commissione in un secondo momento, quando saranno disponibili tutte le versioni, nelle varie lingue nazionali, degli stessi.

Il **capo III** stabilisce la **disciplina relativa ai sistemi di IA ad alto rischio** (artt. 6-49).

La **sezione 1** si riferisce alla **classificazione dei sistemi di IA “ad alto rischio”**.

In primo luogo, rientrano in tale categoria i sistemi per i quali ricorrono entrambe le seguenti condizioni:

- il sistema di IA è destinato a essere utilizzato come **componente di sicurezza** di un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nel suddetto allegato I, ovvero il sistema **costituisce di per sé un prodotto** rientrante nell'ambito della medesima normativa di armonizzazione;
- la componente di sicurezza o il prodotto summenzionato 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 di cui all'allegato I.

Sono inoltre considerati ad alto rischio i sistemi di IA di cui all'**allegato III** del regolamento⁴⁰, a meno che essi **non presentino un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali**

l'uso. Tuttavia, in una situazione di urgenza debitamente giustificata, sarà 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 verrà respinta, l'uso sarà interrotto con effetto immediato e tutti i dati, nonché i risultati e gli *output* di tale uso, saranno immediatamente eliminati e cancellati.

³⁷ Riguardo a tale termine temporale, cfr. la parte di scheda relativa all'articolo 113 del presente regolamento.

³⁸ Riguardo a tale articolo, cfr. *infra*.

³⁹ Per il testo in oggetto, cfr. le seguenti url:

<https://ec.europa.eu/newsroom/dae/redirection/document/112366> e

<https://ec.europa.eu/newsroom/dae/redirection/document/112367>.

⁴⁰ Alla Commissione è conferito il potere di adottare atti delegati al fine di modificare l'elenco di cui all'allegato III, aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio se sono soddisfatte entrambe le seguenti condizioni: i sistemi di IA sono destinati a essere usati in uno dei settori elencati nell'allegato III; 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.

delle persone fisiche; tali esclusioni non possono riguardare i sistemi di cui all'allegato III che effettuino **profilazione di persone fisiche**.

Si segnala che, in base a tali definizioni, tra i sistemi ad alto rischio rientrano, in particolare, quelli riguardanti:

- l'**identificazione biometrica remota**, la **categorizzazione biometrica** e il **riconoscimento delle emozioni**;
- le **infrastrutture critiche** (sistemi di IA destinati a essere utilizzati come **componenti di sicurezza** nella gestione e nel funzionamento delle **infrastrutture digitali critiche** e del **traffico stradale** e nella fornitura di **acqua, gas, riscaldamento o elettricità**);
- l'accesso, l'ammissione o l'assegnazione agli **istituti di istruzione e formazione professionale**;
- l'**occupazione**, la **gestione dei lavoratori** e l'**accesso al lavoro autonomo** (sistemi di IA destinati all'assunzione o alla selezione di persone fisiche, in particolare mediante pubblicazione di annunci di lavoro mirati o valutazione dei candidati, e sistemi destinati a essere utilizzati per adottare decisioni in merito alle condizioni dei rapporti di lavoro, per assegnare compiti o per monitorare le prestazioni);
- l'**accesso a servizi e a prestazioni, pubblici e privati, essenziali** (compresi l'assistenza sanitaria e compresi i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza), la valutazione dell'**affidabilità creditizia delle persone fisiche**, la valutazione dei **rischi finanziari**, la **determinazione dei prezzi** in relazione ad **assicurazioni sulla vita e assicurazioni sanitarie**;
- le **attività di contrasto** (nella misura in cui il diritto dell'Unione o nazionale ne consenta l'uso)⁴¹;
- la gestione della **migrazione**, dell'**asilo** e del **controllo delle frontiere**;
- l'**amministrazione della giustizia** e i **processi democratici** (sistemi di IA destinati a essere usati per assistere le autorità giudiziarie nella ricerca e nell'interpretazione dei fatti e sistemi destinati a influenzare l'esito di un'elezione o di un referendum).

Nella misura in cui sono integrati in piattaforme *online* di dimensioni molto grandi o motori di ricerca *online* di dimensioni molto grandi, i sistemi di IA sono soggetti al quadro di gestione dei rischi di cui al regolamento (UE) 2022/2065 ([regolamento sui servizi digitali](#))⁴².

⁴¹ Riguardo alla nozione di attività di contrasto, cfr. *supra*, in nota.

⁴² Cfr. anche il [regolamento sui mercati digitali](#) (regolamento (UE) 2022/1925).

La **sezione 2** disciplina i **requisiti per i sistemi di IA classificati ad alto rischio**, mentre nella **sezione 3** sono stabiliti gli **obblighi dei produttori⁴³ e dei gestori (*deployers*⁴⁴)** di tali sistemi.

Per i sistemi ad alto rischio vige l'obbligo di valutare e ridurre i rischi, mantenere registri d'uso, essere accurati e garantire la sorveglianza umana. In particolare, tali sistemi dovranno essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente e da consentire ai *deployers* di interpretare l'*output* del sistema e utilizzarlo adeguatamente.

I produttori di sistemi di IA ad alto rischio dovranno istituire un **sistema di gestione della qualità** che garantisca la conformità al regolamento in oggetto. Tale sistema dovrà essere documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprendere almeno: a) una strategia per la conformità normativa; 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, 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; g) il sistema di gestione dei rischi; h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato; i) le procedure relative alla segnalazione di un **incidente grave⁴⁵**; j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, gli organismi notificati, altri operatori, clienti o altre parti interessate;

⁴³ Riguardo a tale categoria, si ricorda che, sotto il profilo letterale, il regolamento adopera il termine fornitore, il quale viene ivi definito come “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”.

⁴⁴ Il regolamento definisce "*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, ad eccezione dei casi in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

⁴⁵ Viene definito "incidente grave": un incidente o malfunzionamento di un sistema di IA che, direttamente o indirettamente, determina una delle conseguenze seguenti:

1. il decesso di una persona o gravi danni alla salute di una persona;
2. una perturbazione grave e irreversibile della gestione o del funzionamento delle infrastrutture critiche;
3. la violazione degli obblighi posti a norma del diritto dell'Unione e intesi a proteggere i diritti fondamentali;
4. gravi danni alle cose o all'ambiente.

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.

Prima di utilizzare un sistema di IA ad alto rischio, i *deployers* (di diritto pubblico o privato) che forniscono servizi pubblici e i *deployers* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), dovranno effettuare una **valutazione dell'impatto sui diritti fondamentali** che l'uso di tale sistema può produrre.

Il **capo IV** stabilisce gli **obblighi di trasparenza per i produttori e i *deployers* di determinati sistemi di IA** (art. 50).

I produttori dovranno garantire che i sistemi di IA destinati a interagire direttamente con le persone fisiche siano 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.

I produttori di sistemi di IA, compresi i sistemi di IA per finalità generali⁴⁶, che generano contenuti audio, immagine, video o testuali sintetici, devono garantire che gli *output* del sistema di IA siano marcati in un **formato leggibile meccanicamente** e rilevabili come **generati o manipolati artificialmente**⁴⁷.

Inoltre, i *deployers* di un sistema di **riconoscimento delle emozioni** o di un sistema di categorizzazione biometrica dovranno informare le persone fisiche che vi sono esposte in merito al funzionamento del sistema e trattare i dati personali in conformità dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680, a seconda dei casi⁴⁸.

⁴⁶ Riguardo a questi ultimi sistemi, cfr. *infra*.

⁴⁷ “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 produttori 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” (considerando 133 del regolamento).

⁴⁸ 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,

Il presente regolamento definisce la "**categorizzazione biometrica**" come l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici.

Si prevede che l'**Ufficio per l'IA** (già istituito all'interno della Commissione europea⁴⁹) incoraggi e agevoli 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 europea può adottare atti di esecuzione per approvare uno o più di tali codici di buone pratiche⁵⁰.

Il **capo V** stabilisce le norme relative ai **modelli di IA per finalità generali** (artt. 51-56). In base alla nozione posta dal regolamento⁵¹, si considera come un modello di IA per finalità generali un modello (anche se addestrato con grandi quantità di dati mediante l'autosupervisione su larga scala) "che sia caratterizzato da 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".

Con riferimento agli **obblighi dei produttori di modelli di IA per finalità generali (sezione 2)**, si dispone che tali soggetti siano tenuti a:

- redigere la documentazione tecnica del modello, relativa anche al processo di addestramento e prova e ai risultati della sua valutazione; la documentazione deve contenere almeno le informazioni di cui all'**allegato XI**, affinché possa essere trasmessa, su richiesta, all'Ufficio per l'IA⁵² e alle autorità nazionali competenti;
- elaborare informazioni e documentazioni per i produttori di sistemi di IA che intendano 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

fatte salve le tutele adeguate per i diritti e le libertà dei terzi e conformemente al diritto dell'Unione.

⁴⁹ Cfr. la parte della scheda relativa al capo VII del presente regolamento.

⁵⁰ A quest'ultimo riguardo, cfr., anche in nota, la parte di scheda relativa all'articolo 56 del presente regolamento.

⁵¹ All'art. 3, primo comma, punto 63). Riguardo a tali modelli, l'Ufficio per l'IA istituito all'interno della Commissione cura delle *faq*, reperibili alla seguente url: <https://digital-strategy.ec.europa.eu/it/faqs/general-purpose-ai-models-ai-act-questions-answers>. Riguardo a tale Ufficio, cfr., come detto, la parte della scheda relativa al capo VII del presente regolamento.

⁵² Riguardo a tale Ufficio, cfr., come detto, la parte della scheda relativa al capo VII del presente regolamento.

diritto dell'Unione e nazionale), le informazioni e le documentazioni devono:

- consentire ai produttori di sistemi di IA di avere una buona comprensione delle capacità e dei limiti del modello di IA per finalità generali e di adempiere i loro obblighi a norma del regolamento;
- contenere almeno gli elementi di cui all'allegato XII⁵³;
- attuare una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e di diritti ad esso collegati e, in particolare, a individuare e rispettare, anche attraverso tecnologie all'avanguardia, una riserva di diritti espressa dal titolare in modo appropriato a norma dell'art. 4, paragrafo 3, della [direttiva \(UE\) 2019/790](#);
- redigere e mettere 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.

Nella **sezione 3** sono stabiliti gli **specifici obblighi posti (in via aggiuntiva) a carico dei produttori di modelli di IA per finalità generali con rischio sistemico**.

Si ricorda che (in base alla **sezione 1** del capo in esame) un modello di IA per finalità generali è classificato come “**modello di IA per finalità generali con rischio sistemico**” se rientra in una delle fattispecie seguenti:

- presenta capacità di **impatto elevato**, valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento;
- presenta capacità di impatto **equivalenti** a quelle suddette; tale equivalenza è stabilita con decisione della Commissione – *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici – sulla base dei **criteri di cui all'allegato XIII**.

Per tali modelli, le norme poste dalla suddetta sezione 3 richiedono di:

- effettuare 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;

⁵³ Gli obblighi di informazione e documentazione fin qui ricordati (di cui alla sezione 2 in oggetto) non si applicano ai produttori 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.

- valutare e attenuare i possibili rischi sistemici, a livello dell'Unione, che possano derivare dallo sviluppo, dall'immissione sul mercato o dall'uso del modello;
- tenere traccia, documentare e riferire “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;
- garantire un livello adeguato di protezione – in termini di cibersicurezza – del modello e dell'infrastruttura fisica dello stesso⁵⁴.

Nella **sezione 4** (costituita dall'art. 56) si prevede la possibilità sia di elaborazioni di **codici di buone pratiche** a livello dell'Unione europea per l'attuazione del presente regolamento sia di adozione di **un codice di buone pratiche** (avente validità generale all'interno dell'Unione) da parte della Commissione europea⁵⁵.

Il **capo VI** disciplina le **misure a sostegno dell'innovazione** (artt. 57-63).

Gli Stati membri devono provvedere affinché le loro **autorità competenti** istituiscano almeno uno **spazio di sperimentazione normativa per l'IA**, a livello nazionale o congiuntamente con le autorità competenti di altri Stati membri⁵⁶; lo spazio deve essere operativo entro due anni dalla data di entrata in vigore del presente regolamento. In base alla definizione posta da quest'ultimo⁵⁷, lo spazio in oggetto è “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”.

Gli spazi di sperimentazione normativa per l'IA devono garantire un ambiente controllato che promuova l'innovazione e faciliti lo sviluppo,

⁵⁴ “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” (considerando 115).

⁵⁵ A quest'ultimo riguardo, si ricorda che l'11 marzo 2025 è stata pubblicata la [terza bozza](#) di tale codice; il testo reca in particolare indicazioni inerenti alla trasparenza e al diritto d'autore per tutti i produttori di modelli di IA per finalità generali e indicazioni specifiche, relative alla sicurezza, per i produttori di modelli di IA per finalità generali con rischio sistemico.

⁵⁶ La Commissione europea può fornire in merito assistenza tecnica, consulenza e strumenti.

⁵⁷ Cfr. l'art. 3, primo comma, punto 55).

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 fra i produttori o i potenziali produttori e l'autorità competente. Tali spazi di sperimentazione possono comprendere “**prove in condizioni reali**”, soggette a controllo nei medesimi spazi.

Le prove in condizioni reali possono essere effettuate solo se sussistono garanzie specifiche. Tra l'altro, gli utenti dei sistemi sottoposti a prova in condizioni reali devono fornire un consenso informato; tale condizione non si applica per le attività di contrasto⁵⁸, qualora la richiesta di consenso sia sostanzialmente incompatibile con la prova (in questo caso, si richiede che le prove e i risultati delle stesse non abbiano alcun effetto negativo sugli utenti e che i relativi dati personali siano cancellati dopo la conclusione delle prove). Una protezione speciale nello svolgimento delle prove deve essere riservata alle persone vulnerabili (a causa della loro età o della disabilità fisica o mentale).

L'autorità competente fornisce una relazione di uscita che illustra in dettaglio le attività svolte nello spazio di sperimentazione normativa, i relativi risultati e le conclusioni dell'apprendimento. I produttori possono utilizzare tale documentazione per dimostrare la conformità al presente regolamento (nell'ambito della procedura di valutazione della conformità o nell'ambito dei loro rapporti con i soggetti che esercitano le attività di vigilanza sul mercato).

La previsione degli spazi di sperimentazione normativa per l'IA è intesa ai seguenti **obiettivi**: a) migliorare la certezza del diritto; b) sostenere la condivisione delle migliori pratiche; 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*.

Il **capo VII** disciplina la **governance** del settore a livello di Unione europea e di autorità nazionali (artt. 64-70).

Nell'ambito dell'Unione, sono istituiti:

- un **Ufficio per l'IA** all'interno della Commissione, volto a sviluppare le competenze e le capacità dell'Unione nel settore dell'IA. Più precisamente, tale Ufficio, a cui fa riferimento il regolamento in esame, è stato già istituito con la [decisione](#) della Commissione del 24 gennaio 2024 (C (2024) 390);

L'Ufficio per l'IA 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. In particolare, l'Ufficio ha il compito di applicare e supervisionare le nuove regole per i modelli di IA per finalità generali, con

⁵⁸ Riguardo alla nozione di attività di contrasto, cfr. *supra*, in nota.

il potere di richiedere documentazione, condurre valutazioni dei modelli, indagare sulle segnalazioni e chiedere ai produttori di adottare misure correttive. L'Ufficio deve inoltre garantire il coordinamento per quanto riguarda la politica in materia di IA e la collaborazione fra le istituzioni, gli organi e le agenzie dell'Unione coinvolti, nonché con gli esperti e i portatori di interessi. A tal fine, l'Ufficio per l'IA deve dialogare con la comunità scientifica, l'industria, la società civile e altri esperti.

- un **Comitato europeo per l'intelligenza artificiale**, composto da rappresentanti degli Stati membri e incaricato di fornire consulenza e assistenza alla Commissione e agli Stati membri, al fine di agevolare la coerenza e il coordinamento fra le autorità nazionali nell'attuazione del regolamento sull'IA. Alle riunioni del Comitato partecipano anche l'Ufficio per l'IA (senza diritto al voto) e, in qualità di osservatore, il Garante europeo della protezione dei dati parteciperà. Altre autorità, organismi o esperti nazionali e dell'Unione possono essere invitati alle riunioni qualora le questioni discusse siano di loro pertinenza;
- un **gruppo di esperti scientifici indipendenti**, con funzione di sostegno delle attività dell'Unione europea di esecuzione del presente regolamento;
- un **forum consultivo**, volto a fornire consulenza e competenze tecniche al Comitato europeo per l'IA e alla Commissione. Il *forum* deve essere costituito da una 'selezione equilibrata' di portatori di interessi, fra cui l'industria, le *start-up*, le PMI, la società civile e il mondo accademico.

Il capo VII prevede inoltre la designazione, da parte dei singoli Stati membri, di almeno un'**autorità di vigilanza del mercato** e di almeno un'**autorità nazionale di notifica**; l'autorità di vigilanza del mercato – o una di esse, in caso di pluralità di autorità designate – funge da **punto di contatto unico**⁵⁹. Tali autorità costituiscono le **autorità nazionali competenti** (ai fini dell'attuazione del regolamento in oggetto).

Il **capo VIII** disciplina la **banca dati della UE sui sistemi di IA ad alto rischio** (art. 71); tale banca dati ricomprende anche i sistemi che, pur

⁵⁹ L'art. 3, primo comma, punto 26), del regolamento in esame definisce l'autorità di vigilanza del mercato quale l'autorità nazionale che svolge le attività e adotta le misure a norma del [regolamento \(UE\) 2019/1020](#) (recante disposizioni "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").

Riguardo al tema della vigilanza del mercato, la relazione della Commissione europea annessa alla schema del regolamento in esame ([COM\(2021\) 206 final](#)) afferma che non sono previste disposizioni "eccessivamente prescrittive", lasciando "spazio a diversi livelli di azione da parte degli Stati membri in relazione ad aspetti che non pregiudicano il conseguimento degli obiettivi dell'iniziativa".

rientrando nell'ambito dell'allegato III, non siano classificati come ad alto rischio⁶⁰.

Il **capo IX** riguarda il **monitoraggio successivo all'immissione sul mercato**, la **condivisione delle informazioni** e la **vigilanza del mercato** (artt. 72-94).

Per i sistemi di IA ad alto rischio, il monitoraggio successivo all'immissione sul mercato raccoglie, documenta e analizza attivamente e sistematicamente i dati pertinenti – che possono essere forniti dai gestori (*deployers*) o che possono essere raccolti tramite altre fonti – sulle prestazioni dei sistemi per tutta la durata del loro ciclo di vita; il monitoraggio consente in tal modo al produttore di valutare la costante conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo III, sezione 2.

Nella **sezione 4** del presente capo IX sono definiti i **mezzi di ricorso**. Viene stabilito che, 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 regolamento in oggetto può presentare un reclamo alla pertinente autorità di vigilanza del mercato. Conformemente al [regolamento \(UE\) 2019/1020](#)⁶¹, 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 dalle medesime autorità di vigilanza. Inoltre, qualsiasi persona interessata oggetto di una decisione adottata dal gestore (*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 incida significativamente su tale persona, in un modo che, secondo quest'ultima, abbia 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.

Il **capo X** fa riferimento a **codici di condotta e orientamenti** (artt. 95-96).

Si prevede che l'Ufficio per l'IA e gli Stati membri incoraggino e agevolino l'elaborazione di **codici di condotta** (comprensivi di relativi meccanismi di *governance*) intesi a promuovere l'applicazione (su base volontaria) ai sistemi di IA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti previsti per i sistemi di IA ad alto rischio (di cui al capo III, sezione 2), tenendo conto delle soluzioni tecniche disponibili e

⁶⁰ Cfr. la parte della presente scheda relativa al capo III del regolamento in oggetto.

⁶¹ Regolamento recante disposizioni “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”.

delle migliori pratiche del settore che consentano l'applicazione di tali requisiti.

I produttori di sistemi di IA non ad alto rischio possono creare e attuare i codici di condotta autonomamente, sulla base di obiettivi chiari e di indicatori chiave di prestazione. In merito, l'art. 95, paragrafo 2, del regolamento indica a titolo esemplificativo alcuni elementi.

Il regolamento demanda inoltre alla Commissione l'elaborazione di **orientamenti sull'attuazione pratica** della presente disciplina, con particolare riferimento a: a) l'applicazione dei requisiti e degli obblighi per i sistemi ad alto rischio; b) le pratiche di IA vietate⁶²; c) l'attuazione delle disposizioni relative alla modifica sostanziale di un sistema di IA; d) l'attuazione degli obblighi di trasparenza (di cui al suddetto art. 50 del regolamento); e) i rapporti fra il regolamento e altre normative dell'Unione, anche per quanto riguarda la coerenza nella loro applicazione; f) l'applicazione della definizione di sistema di IA.

Nell'adozione degli orientamenti, la Commissione deve prestare particolare attenzione alle esigenze delle PMI, comprese le *start-up*, delle autorità pubbliche locali e dei settori maggiormente interessati dal regolamento. Su richiesta degli Stati membri o dell'Ufficio per l'IA, o di propria iniziativa, la Commissione aggiorna gli orientamenti qualora lo ritenga necessario.

Il **capo XI** disciplina la **delega di potere** e la **procedura di comitato** (artt. 97-98).

Il regolamento prevede un ampio ricorso a misure di attuazione e modificative, demandate alla Commissione europea, al fine sia di definire aspetti di dettaglio della disciplina sia di aggiornarla in base all'evoluzione tecnologica e di contesto. A questo scopo diverse disposizioni del regolamento potranno essere modificate o integrate mediante **atti delegati e di esecuzione**, adottati **dalla Commissione europea** secondo le norme procedurali poste o richiamate dal capo XI in oggetto.

Il **capo XII** dispone in ordine alle **sanzioni** da adottare (artt. 99-101).

Riguardo alle sanzioni di competenza del singolo Stato membro, previste dall'art. 99, si rinvia alla parte della presente scheda relativa ai principi e criteri direttivi generali per l'esercizio della delega (esame del **comma 2, alinea**, del presente **articolo 24**).

L'art. 100 prevede sanzioni per eventuali inadempimenti da parte di istituzioni, organi e organismi dell'Unione europea, mentre l'art. 101 contempla le sanzioni per le violazioni di obblighi nei confronti dei soggetti summenzionati (sia le sanzioni di cui all'art. 100 sia quelle di cui all'art. 101 sono comminate a livello di Unione).

Il **capo XIII** reca le **disposizioni finali** (artt. 102-113).

⁶² Riguardo agli orientamenti sulle pratiche vietate, cfr. la parte di scheda relativa all'articolo 5 del presente regolamento.

Il regolamento (ai sensi dell'articolo 113) è entrato in vigore venti giorni dopo la pubblicazione nella *Gazzetta ufficiale dell'Unione europea* (avvenuta il 12 luglio 2024) e si applica dal 2 febbraio 2026, salvo per quanto riguarda: il capo I e il capo II (relativo, quest'ultimo, alle pratiche vietate), che si applicano a partire dal 2 febbraio 2025; alcune sezioni normative – tra cui quella sui sistemi di IA per finalità generali e le norme sanzionatorie di cui agli articoli 99 e 100 – che si applicano dal 2 agosto 2025; alcune norme sui sistemi ad alto rischio, le quali si applicano dal 2 agosto 2027.

Si ricorda che il 5 settembre 2024 la [Commissione europea](#) ha firmato – a nome dell'Unione europea – la “**Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e sui diritti umani, la democrazia e lo Stato di diritto**”, il primo accordo internazionale giuridicamente vincolante sull'intelligenza artificiale (IA). In base all'ordinamento dell'Unione europea⁶³, la conclusione dell'accordo deve essere adottata, successivamente alla firma suddetta, con una decisione del Consiglio dell'Unione europea, previa approvazione della proposta di decisione (predisposta dalla Commissione europea) da parte del Parlamento europeo.

La suddetta firma da parte della Commissione europea ha avuto luogo in occasione della conferenza informale dei Ministri della Giustizia del Consiglio d'Europa tenutasi a Vilnius, in Lituania. La Convenzione è stata già firmata, oltre che dall'Unione europea, da altri Stati, ivi compresi alcuni Stati non facenti parte del Consiglio d'Europa.

La Convenzione comprende una serie di concetti e principi tratti dal regolamento europeo sull'IA, fra cui un approccio basato sul rischio, la trasparenza lungo la catena del valore dei sistemi e dei contenuti generati dall'IA, gli obblighi di documentazione dettagliata per i sistemi identificati come ad alto rischio e gli obblighi di gestione dei rischi, con possibilità di introdurre divieti per i sistemi di IA considerati una chiara minaccia per i diritti fondamentali.

Alla stesura del testo hanno contribuito 68 rappresentanti internazionali della società civile, del mondo accademico, dell'industria e di organizzazioni internazionali.

La Convenzione sarà attuata nell'Unione europea mediante il [regolamento \(UE\) 2024/1689 sull'IA](#), insieme ad altre normative pertinenti dell'Unione.

Si segnala che il 3 giugno 2024 il **Garante europeo della protezione dei dati** (GEPD) ha pubblicato le sue [linee guida sull'uso dell'IA generativa da parte delle istituzioni europee](#). Il GEPD Wojciech Wiewiórowski auspica cautela

⁶³ Cfr. l'articolo 218 del [Trattato sul funzionamento dell'Unione europea](#).

nell'uso dell'intelligenza artificiale generativa, in particolare per quanto riguarda i dati raccolti e il tipo di modello utilizzato; sottolinea inoltre che è responsabilità delle istituzioni dell'UE gestire in modo appropriato i rischi connessi a tale uso.

Si segnala, inoltre, la relazione speciale della Corte dei conti europea n. [8/2024](#) “Le ambizioni dell'UE in materia di intelligenza artificiale - Per il futuro, una *governance* più forte e investimenti più consistenti e mirati sono essenziali” (Gazzetta ufficiale dell'Unione europea [C/2024/3540](#) del 31 maggio 2024). A tale relazione sono seguite le risposte della Commissione europea, pubblicate unitamente alla relazione speciale (il documento contenente le risposte della Commissione è reperibile sul sito della Corte dei conti europea al link: <https://www.eca.europa.eu/it/publications/sr-2024-08>).

Articolo 24, commi 3-5
(Delega per la definizione organica della disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite)

L'articolo 24, commi da 3 a 5, reca delega al Governo, indicandone anche **specifici principi e criteri direttivi**, per la definizione organica della disciplina nei casi di uso di sistemi di **intelligenza artificiale per finalità illecite**.

Più nel dettaglio il **comma 3** delega il Governo ad adottare, entro 12 mesi dalla entrata in vigore della legge, uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di **realizzazione e di impiego illeciti di sistemi di intelligenza artificiale**.

Con riguardo alla **procedura di adozione** dei suddetti decreti, il **comma 4** prevede che siano adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con il Ministro dell'interno. Di ciascuno schema è prevista la successiva trasmissione alle Camere per l'espressione dei **pareri delle Commissioni parlamentari competenti**, che si pronunciano entro il termine di 60 giorni dalla data di trasmissione, decorso il quale i decreti legislativi possono essere comunque emanati. La disposizione prevede inoltre il principio dello "**scorrimento**" in base al quale se il termine previsto per il parere cade nei trenta giorni che precedono la scadenza del termine previsto o successivamente, la scadenza medesima è prorogata di sessanta giorni.

Il comma 5 dell'articolo 24, reca i **principi e criteri direttivi** ai quali il Governo è tenuto ad attenersi nell'esercizio della delega di cui ai commi precedenti.

Come si evidenzia anche nella relazione illustrativa la delega "realizza un intervento complementare a quello contenuto nell'articolo 25 del disegno di legge (ora articolo 26 n.d.r.), che contempla invece l'introduzione di una fattispecie di reato, di una circostanza aggravante comune e di limitate circostanze aggravanti ad effetto speciale per alcuni reati".

Nel dettaglio, il legislatore delegato è chiamato, in primo luogo, a prevedere **strumenti**, anche cautelari, (nel corso dell'esame in sede referente è stato espunto l'inciso «in ambito civile, amministrativo e penale»), **finalizzati a inibire la diffusione** e a rimuovere **contenuti generati illecitamente anche con sistemi di intelligenza artificiale**,

assistiti da un sistema di **sanzioni** effettive, proporzionate e dissuasive (**lett. a)**);

Ancora, ai sensi della **lett. b)**, il Governo dovrà introdurre **autonome fattispecie di reato**, punite a titolo di dolo o di colpa, incentrate sulla omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, **quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato**.

Si segnala che la formulazione originaria della **lett. b)**, modificata nel corso dell'esame in Senato, disponeva l'introduzione di ulteriori fattispecie di reato, punite a titolo di dolo, dirette a tutelare specifici beni giuridici esposti a rischio, in modo da evitare un eccessivo aumento delle ipotesi di reato correlate all'impiego di sistemi di intelligenza artificiale.

In terzo luogo, in sede di esercizio della delega dovrà essere attuata una **precisazione dei criteri di imputazione della responsabilità penale** delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del **c.d. "controllo umano significativo"**, ossia del livello effettivo di controllo dei sistemi predetti da parte dell'agente (**lett. c)**).

Si evidenzia che la disposizione originaria di cui alla **lett. c)**, interamente sostituita nel corso dell'esame in Senato, prevedeva l'introduzione di circostanze aggravanti prive di una caratterizzazione ulteriore e diversa rispetto all'assetto normativo vigente, già in grado di reagire ai fenomeni illeciti dotati di maggiore offensività.

Ai sensi della **lett. d)**, il legislatore delegato dovrà prevedere, nei casi di responsabilità civile, **strumenti di tutela del danneggiato**, anche attraverso una **regolamentazione specifica dei criteri di ripartizione dell'onere della prova**, tenendo in considerazione la classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal Regolamento (UE) 2024/1689.

In base alla **lett. e)** il Governo dovrà disporre, inoltre, una **regolazione dell'utilizzo di sistemi di intelligenza artificiale nelle indagini preliminari**, nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza.

Il dibattito sull'opportunità del ricorso alle tecnologie di intelligenza artificiale nelle indagini preliminari ha preso avvio in ambito europeo già dal 2018, quando la Commissione Europea per l'Efficacia della Giustizia (CEPEJ) del Consiglio d'Europa ha emanato la "Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti" individuando, oltre allo sviluppo degli strumenti e dei servizi della IA, i principi ai quali dovranno attenersi i soggetti pubblici e privati responsabili del progetto. Il tema è stato poi ripreso dalla Commissione stessa nel "Libro bianco sull'intelligenza artificiale" del 2020 allo scopo di definire le opzioni politiche per la promozione dello sviluppo dell'AI, garantendo, necessariamente, al contempo la tutela dei principi e dei diritti fondamentali.

Infine, il legislatore delegato è chiamato a **modificare, a fini di coordinamento e di razionalizzazione del sistema**, la normativa sostanziale e processuale vigente, in conformità ai criteri enunciati alle lettere sopra citate (**lett. f**).

CAPO IV – DISPOSIZIONI A TUTELA DEGLI UTENTI E IN MATERIA DI DIRITTO D’AUTORE

Articolo 25 *(Tutela del diritto d’autore delle opere generate con l’ausilio dell’intelligenza artificiale)*

L’**articolo 25** disciplina la **tutela del diritto d’autore** con riguardo alle opere generate con l’ausilio dell’**intelligenza artificiale**. In particolare, tramite novelle alla legge n. 633 del 1941, si precisa: in primo luogo che le “opere dell’ingegno” protette ai sensi della predetta legge devono essere di **origine “umana”**; in secondo luogo, che **anche le opere create con l’ausilio di strumenti di intelligenza artificiale** sono protette dal diritto d’autore, a condizione che la loro creazione derivi del lavoro intellettuale dell'autore.

Viene inoltre consentita la **riproduzione** e **l’estrazione** da opere o da altri materiali contenuti in rete o in banche di dati cui si ha legittimamente accesso, effettuata **tramite l’utilizzo di modelli e sistemi di intelligenza artificiale**, compresi quelli generativi, in conformità a talune disposizioni della medesima legge n. 633 del 1941.

Nello specifico, l’articolo in commento, composto di un **unico comma**, è **suddiviso in due lettere**.

La **lettera a)** modifica [l’articolo 1, primo comma, della legge n. 633 del 1941](#), specificando che l’ingegno che crea le opere tutelate dalla predetta legge è “umano”. Si prevede, inoltre, con una ulteriore integrazione al medesimo articolo 1, primo comma, che le opere dell’ingegno sono protette anche **laddove create con l’ausilio di strumenti di intelligenza artificiale**, purché costituenti **risultato del lavoro intellettuale dell'autore**.

La **lettera b)**, sostituita nel corso dell’**esame al Senato**, inserisce il nuovo **articolo 70-septies** alla legge n. 633 del 1941, composto da un unico comma, il quale prevede che, fermo restando quanto previsto dalla Convenzione di Berna sulla protezione delle opere letterarie e artistiche, ratificata e resa esecutiva con [legge 20 giugno 1978, n. 399](#), le **riproduzioni e le estrazioni da opere o da altri materiali contenuti in rete** o in banche di dati cui si ha legittimamente accesso, ai fini dell’estrazione di testo e di dati attraverso **modelli e sistemi di intelligenza**

artificiale, anche generativa, sono consentite in conformità alle disposizioni di cui agli articoli 70-ter e 70-quater.

Si ricorda che l'[articolo 70-ter della legge n. 633 del 1941](#) prevede, in particolare, che sono consentite le **riproduzioni** compiute da **organismi di ricerca** e da **istituti di tutela del patrimonio culturale**, per scopi di **ricerca scientifica**, ai fini **dell'estrazione di testo e di dati da opere o da altri materiali** disponibili in **reti o banche di dati** cui essi hanno lecitamente accesso, nonché la **comunicazione al pubblico degli esiti della ricerca** ove espressi in nuove opere originali.

L'[articolo 70-quater della medesima legge n. 633 del 1941](#), poi, autorizza le **riproduzioni** e le **estrazioni da opere o da altri materiali** contenuti in **reti o banche di dati** cui si ha legittimamente accesso **ai fini dell'estrazione di testo e di dati**, quando l'utilizzo delle opere e degli altri materiali non sia stato espressamente riservato dai titolari del diritto d'autore e dei diritti connessi nonché dai titolari delle banche dati, e purché le riproduzioni e le estrazioni siano conservate solo per il tempo necessario ai fini dell'estrazione di testo e di dati.

Si ricorda che la **Convenzione di Berna** per la protezione delle opere letterarie e artistiche, firmata il 9 settembre 1886, disciplina il riconoscimento reciproco del diritto d'autore fra i Paesi aderenti, stabilendo regole fondamentali per la protezione del diritto d'autore su opere letterarie e artistiche in tutti gli Stati membri. Essa è stata rivista e integrata più volte e ratificata in Italia con la legge n. 399 del 1978.

In base all'articolo 2, paragrafo 1, della Convenzione, l'espressione "**opere letterarie ed artistiche**" comprende tutte le produzioni nel campo letterario, scientifico e artistico, qualunque ne sia il modo o la forma di espressione, come: i libri, gli opuscoli ed altri scritti; le conferenze, allocuzioni, sermoni ed altre opere della stessa natura; le opere drammatiche o drammatico-musicali; le opere coreografiche e pantomimiche; le composizioni musicali con o senza parole; le opere cinematografiche, alle quali sono assimilate le opere espresse mediante un procedimento analogo alla cinematografia; le opere di disegno, pittura, architettura, scultura, incisione e litografia; le opere fotografiche, alle quali sono assimilate le opere espresse mediante un procedimento analogo alla fotografia; le opere delle arti applicate; le illustrazioni, le carte geografiche, i piani, schizzi e plastici relativi alla geografia, alla topografia, all'architettura o alle scienze.

Secondo quanto disposto dall'articolo 3, paragrafo 1, sono **protetti in forza della Convenzione**:

- a) gli autori appartenenti a uno dei Paesi firmatari, per le loro opere, siano esse pubblicate oppure no;
- b) gli autori non appartenenti ad alcuno dei Paesi firmatari, per le opere che essi pubblicano per la prima volta in uno di tali Paesi o simultaneamente in un Paese estraneo all'Unione e in un Paese dell'Unione.

Quanto agli autori non appartenenti ad alcuno dei Paesi firmatari, ma aventi la loro residenza abituale in uno di essi, sono assimilati, ai fini dell'applicazione della Convenzione, agli autori appartenenti al predetto Paese.

La Convenzione di Berna si basa su **tre principi fondamentali**:

- a) le opere originarie di uno degli Stati contraenti (vale a dire le opere il cui autore è cittadino di tale Stato o le opere pubblicate per la prima volta in tale Stato) devono beneficiare in ciascuno degli altri Stati contraenti della stessa protezione che quest'ultimo accorda alle opere dei propri cittadini (principio del "trattamento nazionale");
- b) la protezione non può essere subordinata al rispetto di alcuna formalità (principio di protezione "automatica");
- c) la protezione è indipendente dall'esistenza di una protezione nel Paese di origine dell'opera (principio di "indipendenza" della protezione). Tuttavia, se uno Stato contraente prevede un termine di protezione più lungo del minimo prescritto dalla Convenzione e l'opera cessa di essere protetta nel Paese di origine, la protezione può essere negata una volta cessata la protezione nel Paese di origine.

Per maggiori approfondimenti si rimanda all'apposita [pagina](#) del sito internet della World Intellectual Property Organization (WIPO).

CAPO V – DISPOSIZIONI PENALI

Articolo 26 (Norme penali)

L'**articolo 26**, modificato nel corso dell'esame in Senato, reca disposizioni riguardanti: a) l'introduzione di una **circostanza aggravante comune**, qualora il reato sia commesso mediante sistemi di intelligenza artificiale; b) l'inserimento nel codice penale di una **circostanza aggravante ad effetto speciale** legata all'impiego di sistemi di intelligenza artificiale nella commissione del delitto di **attentati contro i diritti politici del cittadino** di cui all'art. 294 c.p.; c) l'introduzione del nuovo reato di **illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale**.

In particolare, il **comma 1** reca **modifiche al codice penale**.

La **lett. a)** modifica l'art. 61, primo comma, c.p. in materia di **circostanze aggravanti comuni**, integrando l'elenco delle aggravanti con l'inserimento del numero 11-*decies*, volto a prevedere tra le predette aggravanti l'**aver commesso il fatto mediante sistemi di intelligenza artificiali** quando:

- gli stessi, per la loro natura o le modalità di utilizzo, abbiano costituito **mezzo insidioso**;
- il loro impiego abbia comunque **ostacolato la pubblica o privata difesa**;
- il loro impiego abbia **aggravato le conseguenze del reato**.

Si ricorda che l'art. 61, primo comma, c.p. prevede, tra l'altro, le aggravanti dell'aver profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa (n. 5) e dell'aver aggravato o tentato di aggravare le conseguenze del delitto (n. 8).

L'aggravante di cui la norma in commento propone l'introduzione si applica ai casi in cui l'ostacolo alla pubblica o privata difesa o l'aggravamento delle conseguenze del reato derivino dall'impiego di sistemi di intelligenza artificiale.

La **lett. b)**, prevede l'introduzione di una **circostanza aggravante** del delitto di **attentati contro i diritti politici del cittadino** di cui all'art. 294 c.p.

L'art. 294 c.p. nel testo vigente punisce con la reclusione da uno a cinque anni chiunque con violenza, minaccia o inganno impedisce in tutto o in parte l'esercizio di un diritto politico, ovvero determina taluno a esercitarlo in senso difforme dalla sua volontà.

Nello specifico, la disposizione in commento introduce un comma aggiuntivo all'art. 294 c.p. volto a prevedere una circostanza aggravante a effetto speciale ai sensi della quale si prevede la **reclusione da due a sei anni** se l'inganno è posto in essere mediante l'**impiego di sistemi di intelligenza artificiale**.

Si segnala che la formulazione originaria della lettera *b*) prevedeva una circostanza aggravante a effetto comune quando il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

La **lett. c)** introduce nel codice penale l'art. 612-*quater*, volto a prevedere il nuovo reato di "***Illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale***", nell'ambito del titolo XII (*Delitti contro la persona*), capo III (*Delitti contro la libertà individuale*), sezione III (*Delitti contro la libertà morale*).

Il nuovo art. 612-*quater* c.p. punisce con la **reclusione da 1 a 5 anni** chiunque cagioni un **danno ingiusto** ad una persona cedendo, pubblicando o diffondendo, senza il suo consenso, **immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale** e idonei a trarre in inganno sulla loro genuinità (primo comma).

Secondo quanto riportato dalla relazione illustrativa, attraverso la disposizione in commento si vuole offrire una tutela rafforzata della persona, incentrando l'offensività della condotta sul pregiudizio all'autodeterminazione ed al pieno svolgimento della personalità, circostanza confermata anche dalla collocazione sistematica della disposizione fra i delitti contro la persona e, segnatamente contro la libertà morale.

Il delitto, inoltre, è punibile a querela, ma si procede d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se il fatto è commesso nei confronti di persona incapace, per età o infermità, o nei confronti di una pubblica autorità a causa delle funzioni esercitate.

Codice penale	
Testo vigente	Testo come modificato dall'A.C. 2316
Art. 61 <i>(Circostanze aggravanti comuni)</i>	Art. 61 <i>(Circostanze aggravanti comuni)</i>
Aggravano il reato, quando non ne sono elementi costitutivi o circostanze aggravanti speciali, le circostanze seguenti:	<i>Identico</i>
1. L'avere agito per motivi abietti o futili;	<i>Identico</i>
2. L'aver commesso il reato per eseguirne od occultarne un altro, ovvero per conseguire o assicurare a sé o ad altri il prodotto o il profitto o il prezzo ovvero la impunità di un altro reato;	<i>Identico</i>
3. L'avere, nei delitti colposi, agito nonostante la previsione dell'evento;	<i>Identico</i>
4. L'avere adoperato sevizie, o l'aver agito con crudeltà verso le persone;	<i>Identico</i>
5. L'avere profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa;	<i>Identico</i>
6. L'avere il colpevole commesso il reato durante il tempo, in cui si è sottratto volontariamente alla esecuzione di un mandato o di un ordine di arresto o di cattura o di carcerazione, spedito per un precedente reato;	<i>Identico</i>
7. L'avere, nei delitti contro il patrimonio, o che comunque offendono il patrimonio, ovvero nei delitti determinati da motivi di lucro,	<i>Identico</i>

Codice penale	
Testo vigente	Testo come modificato dall'A.C. 2316
cagionato alla persona offesa dal reato un danno patrimoniale di rilevante gravità;	
8. L'aver aggravato o tentato di aggravare le conseguenze del delitto commesso;	<i>Identico</i>
9. L'aver commesso il fatto con abuso dei poteri, o con violazione dei doveri inerenti a una pubblica funzione o a un pubblico servizio, ovvero alla qualità di ministro di un culto;	<i>Identico</i>
10. L'aver commesso il fatto contro un pubblico ufficiale o una persona incaricata di un pubblico servizio, o rivestita della qualità di ministro del culto cattolico o di un culto ammesso nello Stato, ovvero contro un agente diplomatico o consolare di uno Stato estero, nell'atto o a causa dell'adempimento delle funzioni o del servizio;	<i>Identico</i>
11. L'aver commesso il fatto con abuso di autorità o di relazioni domestiche, ovvero con abuso di relazioni di ufficio, di prestazione d'opera, di coabitazione, o di ospitalità.	<i>Identico</i>
11-bis. L'aver il colpevole commesso il fatto mentre si trova illegalmente sul territorio nazionale.	<i>Identico</i>
11-ter. L'aver commesso un delitto contro la persona ai danni di un soggetto minore all'interno o nelle adiacenze di istituti di istruzione o di formazione.	<i>Identico</i>

Codice penale	
Testo vigente	Testo come modificato dall'A.C. 2316
<p>11-<i>quater</i>. L'avere il colpevole commesso un delitto non colposo durante il periodo in cui era ammesso ad una misura alternativa alla detenzione in carcere.</p>	<i>Identico</i>
<p>11-<i>quinquies</i>. L'avere, nei delitti non colposi contro la vita e l'incolumità individuale e contro la libertà personale, commesso il fatto in presenza o in danno di un minore di anni diciotto ovvero in danno di persona in stato di gravidanza.</p>	<i>Identico</i>
<p>11-<i>sexies</i>. L'avere, nei delitti non colposi, commesso il fatto in danno di persone ricoverate presso strutture sanitarie o presso strutture sociosanitarie residenziali o semiresidenziali, pubbliche o private, ovvero presso strutture socio-educative.</p>	<i>Identico</i>
<p>11-<i>septies</i>. L'avere commesso il fatto in occasione o a causa di manifestazioni sportive o durante i trasferimenti da o verso i luoghi in cui si svolgono dette manifestazioni.</p>	<i>Identico</i>
<p>11-<i>octies</i>. L'avere agito, nei delitti commessi con violenza o minaccia, in danno degli esercenti le professioni sanitarie e socio-sanitarie nonché di chiunque svolga attività ausiliarie di cura, assistenza sanitaria o soccorso, funzionali allo svolgimento di dette professioni, a causa o nell'esercizio di tali professioni o attività.</p>	<i>Identico</i>
<p>11-<i>novies</i>. L'avere agito, nei delitti</p>	<i>Identico</i>

Codice penale

Testo vigente

commessi con violenza o minaccia, in danno di un dirigente scolastico o di un membro del personale docente, educativo, amministrativo, tecnico o ausiliario della scuola, a causa o nell'esercizio delle loro funzioni.

Testo come modificato dall'A.C. 2316

11-decies. L'aver commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato.

Art. 294

(Attentati contro i diritti politici del cittadino)

Chiunque con violenza, minaccia o inganno impedisce in tutto o in parte l'esercizio di un diritto politico, ovvero determina taluno a esercitarlo in senso difforme dalla sua volontà, è punito con la reclusione da uno a cinque anni.

Art. 294

(Attentati contro i diritti politici del cittadino)

Identico

La pena è della reclusione da due a sei anni se l'inganno è posto in essere l'impiego di sistemi di intelligenza artificiale

Codice penale	
Testo vigente	Testo come modificato dall'A.C. 2316
	Art. 612-<i>quater</i> <i>(Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale)</i>

Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni.

Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate.

Articolo 26, commi da 2 a 4
(Modifiche alla disciplina dei reati di aggioaggio, plagio e manipolazione del mercato)

I commi da 2 a 4 - quest'ultimo modificato nel corso dell'esame in Senato - dell'articolo 26, oltre ad introdurre specifiche circostanze aggravanti per i reati di aggioaggio e di manipolazione del mercato quando i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale, sanzionano anche le condotte di plagio commesse attraverso sistemi di intelligenza artificiale.

Il comma 2 modifica l'articolo 2637, primo comma, del codice civile, che disciplina il reato di aggioaggio (punito con la reclusione da uno a cinque anni) prevedendo un aggravamento di pena (la reclusione da due a sette anni) quando il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

Codice civile	
Testo vigente	Modificazioni apportate dall'A.S.1146-A
Art. 2637 <i>(Aggioaggio)</i>	Art. 2637 <i>(Aggioaggio)</i>
Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni .	Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni. La pena è della reclusione da due a

Codice civile

Testo vigente

Modificazioni apportate
dall'A.S.1146-A

sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

Il **comma 3** dell'articolo in esame interviene sulla disciplina del **plagio artistico** dettata dall'articolo 171, comma 1, della legge 22 aprile 1941, n. 633.

L'articolo 171 definisce il plagio artistico come la appropriazione, intesa come riproduzione, in tutto o in parte di un'opera creativa altrui senza averne diritto, punendo tali condotte con la pena della multa da 51 a 2.065 euro.

Il disegno di legge estende la punibilità anche alla riproduzione o estrazione di testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater (che disciplinano riproduzioni ed estrazioni di testi e dati) anche attraverso **sistemi di intelligenza artificiale.**

Legge 22 aprile 1941, n.633

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Testo vigente

Modificazioni apportate dall'A.S.
1146-A**Art. 171****Art. 171**

Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 (lire 100.000) a euro 2.065 (lire 4 milioni) chiunque senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

Identico

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero

a) Identica

Legge 22 aprile 1941, n.633***Protezione del diritto d'autore e di altri diritti connessi al suo esercizio***

Testo vigente	Modificazioni apportate dall'A.S. 1146-A
<p>contrariamente alla legge italiana;</p> <p>a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;</p>	<p><i>a-bis) Identica</i></p>
<p>b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;</p>	<p>a-ter) riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale;</p> <p><i>b) Identica</i></p>
<p>c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;</p>	<p><i>c) Identica</i></p>
<p>d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;</p>	<p><i>d) Identica</i></p>
<p>[e] riproduce con qualsiasi processo di duplicazione dischi o altri apparecchi analoghi o li smercia, ovvero introduce</p>	

Legge 22 aprile 1941, n.633***Protezione del diritto d'autore e di altri diritti connessi al suo esercizio***

Testo vigente	Modificazioni apportate dall'A.S. 1146-A
nel territorio dello Stato le riproduzioni così fatte all'estero;]	
f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.	<i>f) Identica</i>
Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.	<i>Identico</i>
La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 (lire 1.000.000), se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicità ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onere od alla reputazione dell'autore.	<i>Identico</i>
La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione dell'attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione	<i>Identico</i>

Legge 22 aprile 1941, n.633***Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*****Testo vigente****Modificazioni apportate dall'A.S.
1146-A**

amministrativa pecuniaria da euro
1.032 a euro 5.164 (due a dieci milioni
di lire).

Il **comma 4**, come **modificato nel corso dell'esame in Senato**, intervenendo sull'articolo 185 TUIF, introduce **un'aggravante ad effetto speciale, per la quale le** condotte di **manipolazione del mercato** perpetrate **mediante l'impiego di sistemi di intelligenza artificiale** sono sanzionate con la pena della reclusione da due a sette anni e multa da euro venticinquemila a euro sei milioni (nel testo originario del comma 4 per tali condotte era invece previsto un aggravamento di pena fino a un terzo).

Occorre rammentare che l'articolo 185 TUIF punisce con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizii concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

D.Lgs. 24/02/1998, n. 58***Testo unico delle disposizioni in materia di intermediazione finanziaria*****Testo vigente****Modificazioni apportate dall'A.S.
1146-A****Art. 185*****Manipolazione del mercato***

1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizii concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da due a dodici anni e con la multa da euro ventimila a euro cinque milioni.

Art. 185***Manipolazione del mercato***

1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizii concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da due a dodici anni e con la multa da euro ventimila a euro cinque milioni. **La pena è della reclusione da due a sette anni e della multa da euro venticinquemila a euro**

D.Lgs. 24/02/1998, n. 58***Testo unico delle disposizioni in materia di intermediazione finanziaria*****Testo vigente****Modificazioni apportate dall'A.S.
1146-A**

sei milioni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

1-bis. Non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del regolamento (UE) n. 596/2014.

1-bis) Identico

2. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

2) Identico

[2-bis. Nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numeri 2), 2-bis) e 2-ter), limitatamente agli strumenti finanziari il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario di cui ai numeri 2) e 2-bis) ovvero ha un effetto su tale prezzo o valore, o relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni, la sanzione penale è quella dell'ammenda fino a euro centotremila e duecentonovantuno e dell'arresto fino a tre anni.]

D.Lgs. 24/02/1998, n. 58***Testo unico delle disposizioni in materia di intermediazione finanziaria*****Testo vigente****Modificazioni apportate dall'A.S.
1146-A**

[2-ter. Le disposizioni del presente articolo si applicano anche:

a) ai fatti concernenti i contratti a pronti su merci che non sono prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari di cui all'articolo 180, comma 1, lettera a);

b) ai fatti concernenti gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari;

c) ai fatti concernenti gli indici di riferimento (benchmark).]

CAPO VI – DISPOSIZIONI FINANZIARIE E FINALI

Articolo 27 *(Clausola di invarianza finanziaria)*

L'articolo 27 reca la clausola di invarianza finanziaria.

La disposizione stabilisce che dall'attuazione del presente disegno di legge, ad eccezione dell'**articolo 21**, non derivino nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni provvedono con le risorse umane, strumentali e finanziarie, disponibili a legislazione vigente.

Per l'**articolo 21** qui richiamato, concernente “Applicazione sperimentale dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale”, v. la relativa scheda.

Articolo 28, comma 1
(Funzioni dell'Agenzia per la cybersicurezza nazionale)

L'**articolo 28, comma 1** prevede che l'Agenzia per la cybersicurezza nazionale, nello svolgimento delle proprie funzioni, possa concludere accordi di collaborazione, comunque denominati, con soggetti privati.

Il comma in esame (introdotto nel corso dell'esame presso il Senato) reca una modifica all'[articolo 7, comma 1, lettera z\), del decreto-legge n. 82 del 2021](#) (convertito dalla legge n. 109 del 2021) che, tra l'altro, ha istituito l'Agenzia per la cybersicurezza nazionale.

Tale novella interviene sulla disciplina delle funzioni dell'Agenzia per la cybersicurezza nazionale per consentire all'Agenzia medesima di concludere accordi di collaborazione, comunque denominati, con soggetti privati, in aggiunta alla possibilità, già prevista dal testo vigente, di costituire e partecipare a partenariati pubblico-privato sul territorio nazionale.

Si segnala che la novella in esame presenta contenuto analogo alla modifica al medesimo articolo 7, comma 1, del decreto-legge n. 82 recata dall'**articolo 18** del presente disegno di legge (come modificato **in sede referente**) alla cui scheda si rinvia.

L'articolo 7, comma 1, individua le funzioni dell'Agenzia che viene qualificata quale **Autorità nazionale** per la cybersicurezza (ACN), ai fini del complesso di relazioni e funzioni disegnato dalle norme europee ed interne, incluse quelle di certificazione della cybersicurezza. In tale quadro, predispone in primo luogo la strategia nazionale di cybersicurezza; assume compiti precedentemente attribuiti a diversi soggetti, quali il Ministero dello sviluppo economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza, l'Agenzia per l'Italia digitale; promuove iniziative per lo sviluppo di competenze e capacità; è Autorità di gestione delle crisi informatiche; provvede alla diffusione di standard, linee guida e raccomandazioni e alla qualificazione dei servizi cloud per la pubblica amministrazione; svolge compiti inerenti alla prevenzione e alla gestione degli incidenti e attacchi informatici.

Decreto legge 14 giugno 2021, n. 82

Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

Testo vigente**Modificazioni apportate dall'art. 28, comma 1**

Art. 7

(Funzioni dell'Agenzia per la cybersicurezza nazionale)

1. L'Agenzia:

(...)

z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

(...)

Art. 7

(Funzioni dell'Agenzia per la cybersicurezza nazionale)

1. L'Agenzia:

(...)

z) per le finalità di cui al presente articolo, può **concludere accordi di collaborazione, comunque denominati, con soggetti privati**, costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

(...)

Articolo 28, comma 2 ***(Obblighi di notifica di incidenti)***

L'**articolo 28, comma 2**, introdotto nel corso dell'esame **del Senato**, effettua operazioni di coordinamento normativo intervenendo, in particolare, in materia di obblighi di notifica di incidenti.

In particolare, la disposizione in commento interviene anzitutto sull'articolo 1, comma 1, della legge 90/2024, che stabilisce in capo a una serie di soggetti pubblici l'obbligo di notificare gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge 105/2019 (c.d. decreto Perimetro).

Si ricorda che i soggetti obbligati ad adempiere al richiamato obbligo sono:

- le pubbliche amministrazioni centrali individuate annualmente dall'ISTAT con proprio provvedimento;
- le regioni e le province autonome di Trento e di Bolzano;
- le città metropolitane;
- i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione;
- le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- le aziende sanitarie locali.

La disposizione da ultimo richiamata – oggi abrogata (v. *infra*) – era stata inserita nel corpo del c.d. decreto Perimetro dall'articolo 37-*quater* del decreto-legge n. 115/2022 (c.d. Aiuti-*bis*), al fine di estendere gli obblighi di notifica già previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica (beni ICT), anche agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (diversi quindi dai beni ICT), ma che sono di pertinenza di soggetti inclusi nel Perimetro stesso.

In base a tale disposizione si prevedeva che la tassonomia degli incidenti oggetto di notifica venisse indicata con determinazioni tecniche del direttore generale, sentito il vice direttore generale, dell'Agenzia per la cybersicurezza nazionale.

Il D.Lgs. 138/2024, nel recepire la direttiva (UE) 2022/2555 (c.d. direttiva NIS 2), relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, ha abrogato il comma 3-*bis* dell'articolo 1 del D.L. n. 105/2019, al fine di assicurare coerenza normativa con gli obblighi dal medesimo previsti in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente e con le disposizioni recate in materia di monitoraggio, vigilanza ed esecuzione.

La novella in esame interviene, dunque, sull'articolo 1, comma 1, della legge 90/2024, sostituendo il rinvio all'articolo 1, comma 3-*bis*, del decreto-legge 105/2019 con la previsione per cui gli incidenti oggetto dell'obbligo di notifica ivi disciplinato sono quelli indicati nella tassonomia "adottata con determinazione tecnica del direttore generale dell'Agenzia per la cybersicurezza nazionale".

In secondo luogo, e a fini di coordinamento normativo, la disposizione in esame inserisce nella legge 90/2024 il nuovo articolo 15-*bis*, ove si dispone che ogni riferimento al D.Lgs. 65/2018 – con il quale si è proceduto a dare attuazione alla direttiva (UE) 2016/1148, c.d. direttiva NIS – è da intendersi riferito alle corrispondenti disposizioni di cui al D.lgs. 138/2024 – attuativo, come già accennato, della direttiva NIS 2 –, a decorrere dal momento in cui le stesse acquistano efficacia.