CORTE SUPREMA DI CASSAZIONE

UFFICIO DEL MASSIMARIO E DEL RUOLO

SERVIZIO CIVILE E PENALE

Relazione su novità normativa.

Rel. 63 **Roma, 11 novembre 2026**

Redattori Maria Laura Paesano e Francesco Barracca

OGGETTO: SICUREZZA PUBBLICA - IN GENERE -

Regolamento (UE) 2024/1689 - Attuazione nazionale – Utilizzo di sistemi di intelligenza artificiale da parte delle forze di polizia – Attività consentite - Limiti - Riconoscimento biometrico, per finalità preventive – Procedimento.

REATI CONTRO L'INCOLUMITA' PUBBLICA - DELITTI - IN GENERE -

Regolamento (UE) 2024/1689 - Attuazione nazionale – Modifiche al codice penale - Art. 437-*bis* cod. pen. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi – Elementi integrativi delle fattispecie – Individuazione.

INDAGINI PRELIMINARI - 001 IN GENERE -

Regolamento (UE) 2024/1689 - Attuazione nazionale – Modifiche al codice di procedura penale - Art. 359-*ter* cod. proc. pen. – Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale – Procedimento – Caratteri.

RESPONSABILITA' CIVILE - IN GENERE –

Regolamento (UE) 2024/1689 - Attuazione nazionale – Risarcimento del danno – Nesso di causalità - Accesso alle prove- Azione diretta contro l'assicuratore – Modifiche.

****

Questione oggetto della relazione:

adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale.
(d.lgs. 9 settembre 2026, n. 160, pubblicato sulla Gazzetta Ufficiale, Serie generale n. 214 del 15/09/2026 ed entrato in vigore il 30/09/2026).

SOMMARIO:

1. Introduzione.
2. Utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia.
2.1. Principi generali.
2.2. Sistemi di intelligenza artificiale "ad alto rischio".
2.3. Obblighi di formazione e sperimentazione in funzione dell'utilizzo nell'attività di polizia.
2.4. Intelligenza artificiale utilizzata in specifiche attività di polizia. Il trattamento dei dati biometrici.
2.4.1. L'identificazione biometrica.
2.5. La videosorveglianza integrata con componenti di IA e il riconoscimento facciale "a posteriori" di un indiziato di reato.
3. Disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiali.
3.1. Definizioni utilizzate dal testo.
3.2. Modifiche al c.p.
3.3. Il delitto di cui all'art. 437-*bis* c.p. (Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi).
3.3.1. Il delitto di omessa adozione di misure di sicurezza.
3.3.2. Il delitto omissivo colposo.
3.3.3. Il delitto di alterazione illecita dei sistemi.
3.3.4. Il delitto di omessa adozione delle misure di sorveglianza umana.
3.4. Le modifiche al codice di procedura penale. L'impiego investigativo dei sistemi di identificazione biometrica remota *in tempo reale* nel nuovo art. 359-*ter* c.p.p.
3.4.1. Oggetto e presupposti del procedimento.
3.4.2. Il procedimento autorizzativo.
3.4.3. Rilevanza indiziaria e probatoria.

3.5. Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale: il sequestro preventivo sui contenuti generati con intelligenza artificiale.

3.6. La responsabilità amministrativa degli enti per reati commessi con l'uso dell'intelligenza artificiale.

4. Modifiche alla legislazione processuale per i profili risarcitori civili.

4.1. Introduzione agli artt. 16-20 del Capo II del Titolo II. Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale.

4.1.1. Il d.lgs. 9 settembre 2026, n. 160. Premessa.

4.2. Il quadro normativo europeo ed interno.

4.2.1. La dichiarazione comune sui diritti e i principi digitali e la Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto, adottata il 13 maggio 2026.

4.2.2. Il Regolamento (UE) 2024/1689.

4.2.3. Il Regolamento (UE) 2026/1744 (il c.d. «Digital Omnibus sull'IA»).

4.2.4. La legge 23 settembre 2025, n. 132. Cenni.

4.2.5. La Direttiva (UE) n. 2024/2853.

4.2.6. La legislazione europea sui servizi digitali e la proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (cd. "AILD", Artificial Intelligence liability Directive).

4.3. Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale. Il Titolo II Capo II del d.lgs. n. 160 del 2026.

4.4. Il risarcimento del danno cagionato nell'utilizzo di un sistema di intelligenza artificiale.

4.5. Segue.

4.6. L'art. 16, comma 2, e le presunzioni legali.

4.7. L'art. 16, comma 3: la clausola di salvezza dei regimi speciali di responsabilità.

4.8. L'art. 16, comma 4: il foro del consumatore.

4.9. L'accesso alle prove: La disciplina dell'art. 17.

4.10. La ripartizione dell'onere probatorio nelle azioni risarcitorie del danno cagionato da sistemi di intelligenza artificiale.

4.11. La rilevanza della conformità dei sistemi di intelligenza artificiale rispetto alle prescrizioni del Regolamento (UE) 2024/1689 (AI Act) nell'ambito dei giudizi di responsabilità civile.

4.12. L'azione diretta nei confronti dell'impresa di assicurazione (art. 20).

4.13. La colpa nelle azioni risarcitorie del danno cagionato dall'utilizzo di sistemi di intelligenza artificiale.
4.14. Aspetti problematici della disciplina della responsabilità civile da utilizzo di sistemi di intelligenza artificiale.
4.15. Le questioni che possono assumere rilievo nell'attività nomofilattica.
5. Disposizioni di chiusura.
5.1. Disposizioni transitorie e finali.

****

1. Introduzione.

Il d.lgs. 9 settembre 2026, n. 160 (da qui in avanti decreto legislativo), intende dare attuazione *in parte qua* alla legge delega 23 settembre 2025, n. 132 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale[1].

Quest'ultima, a sua volta, trova la propria cornice normativa nel regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024[2].

Tenendo conto dell'apparato definitorio utilizzato dallo stesso d.lgs. (art. 2), nella presente relazione la legge delega verrà individuata come "**legge IA**" e il regolamento (UE) 2024/1689 come "**regolamento IA**".

Nel preambolo, il d.lgs. richiama **l'art. 24, commi 1, 2 lett. h, 3 e 5 della legge IA[3]**, in quanto la scelta del Governo è stata quella di scomporre gli obblighi derivanti dalla delega,

---

• Nell'ambito di una elaborazione unitaria della relazione, la dott.ssa Maria Laura Paesano ha redatto i parr. 1 2 3 e 5, mentre il dott. Francesco Barracca ha redatto il par. 4.

[1] Per un primo commento sul contenuto della legge IA con riferimento alle funzioni di polizia e di indagini preliminari, si veda S. QUATTROCOLO, *La legge 132/2025: uno strumento "ordinario" per governare lo straordinario*, in *Riv. it. dir. proc. pen*., 2026, 1, in particolare pagg. 291 ss.

[2] Il regolamento IA, fondato sull'art. 114 TFUE, è volto primariamente a garantire il corretto funzionamento del mercato unico digitale, adottando un'impostazione marcatamente settoriale, basata sulla classificazione dei sistemi di IA in relazione al livello di rischio, v. D. CARDAMONE, *La Convenzione quadro del Consiglio d'Europa sull'IA: verso una regolazione umano-centrica tra diritti fondamentali, democrazia e Stato di diritto*", in *Quest. giust.*, 3, 2026, p. 46. Va segnalato che, con successivo Regolamento del Parlamento europeo e del Consiglio dell'8 luglio 2026, pubblicato in GUUE il 24 luglio 2026 ed entrato in vigore il 27 luglio 2026, noto come ***Digital Omnibus sull'IA*** sono state apportate modifiche al regolamento IA. Di interesse, per le materie affrontate dal testo, è l'ampliamento delle pratiche vietate di cui all'art. 5 del regolamento IA con l'introduzione delle lettere b-*bis*) e b-*ter*) al paragrafo 1 (relativo a sistemi di intelligenza artificiale che generano o manipolano immagini, video o audio realistici raffiguranti le parti intime di una persona fisica riconoscibile, o la stessa mentre compie atti sessualmente espliciti, in assenza di consenso); la chiarificazione della nozione di "componente di sicurezza" di cui all'art. 3 punto 14); l'ampiamento dell'obbligo di alfabetizzazione previsto per i *deployer* dall'art. 4; lo spostamento dell'entrata in vigore di alcune norme del regolamento IA (v. infra).

[3] Art. 24, comma 5, della legge n. 132 del 2025: "*Nell'esercizio della delega di cui al comma 3, il Governo si attiene ai seguenti principi e criteri direttivi: a) previsione di strumenti, anche cautelari, 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; b) introduzione di autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'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; c) 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 livello effettivo di controllo dei sistemi predetti da parte dell'agente; d) nei casi di responsabilità civile, previsione di strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689; e) regolazione dell'utilizzo dei 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*

dandone attuazione con separati decreti legislativi in relazione all'ambito delle materie di intervento.

Va subito chiarito che il testo non affronta le problematiche etiche, tecniche, organizzative e giuridiche che attengono all'ingresso dell'intelligenza artificiale nel settore della giustizia[4] che pur sono, per quanto limitatamente, affrontate dal regolamento IA e dall'art. 15 della legge IA[5], ma attiene principalmente all'utilizzo dei sistemi di intelligenza artificiale nelle attività di prevenzione delle forze di polizia con specifico riguardo alle conseguenze, pericolose o dannose, che derivano dall'uso non corretto o non conforme alla legislazione di detti sistemi.

Siamo dunque nel campo della prevenzione e della sicurezza, più che in quello della elaborazione di principi utili all'esercizio della giurisdizione influenzata dall'utilizzo di un sistema di IA.

Il decreto legislativo si occupa, inoltre, delle ricadute che le disposizioni determinano sulle attività di indagine della PG; introduce una nuova fattispecie di reato (**art. 437-*bis* c.p.**); delinea un nuovo procedimento penale per l'utilizzo dei sistemi di intelligenza artificiale finalizzati all'identificazione biometrica remota in tempo reale **(art. 359-*ter* c.p.p.)**; disciplina le azioni di **risarcimento del danno**, sia contrattuale che extracontrattuale, cagionato per l'utilizzo di un sistema di intelligenza artificiale.

Va anticipato che, pur avendo una portata tecnica e applicativa, il testo è permeato dello spirito del regolamento IA, mirando all'armonizzazione a fini definitori dei sistemi di intelligenza artificiale e delle pratiche connesse al loro utilizzo e a dettare cautele per l'utilizzo dell'intelligenza artificiale, con particolare riferimento ai sistemi "ad alto rischio".

Per quanto attiene all'attività di polizia, si coglie nel decreto legislativo l'aspetto precipuamente *delimitativo* dell'utilizzo dell'intelligenza artificiale per "assicurare la diffusione di una intelligenza artificiale «*antropocentrica, coerente, affidabile ed eticamente valida*», al fine di garantire un livello elevato di protezione dei diritti fondamentali sanciti dalla Carta dell'Unione, della democrazia e dello stato di diritto contro gli effetti nocivi dei sistemi di IA"[6].

In questa breve introduzione, si intende fornire un'anticipazione sulla struttura del testo, che agevoli la sua comprensione generale.

---

trasparenza; f) modifica, a fini di coordinamento e di razionalizzazione del sistema, della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b), c), d) ed e)."

[4] Si veda, in proposito, S. MAFFEI, *L'AI Act e il sistema giustizia: brevi riflessioni*, in *Quest. giust.*, 3, 2026, p. 33 ss.. Va anche ricordato che il CSM ha adottato, con delibera dell'8 ottobre 2025, le *Raccomandazioni sull'uso dell'intelligenza artificiale nell'amministrazione della giustizia*, aggiornate con delibera del 22 luglio 2026.

[5] **L'art. 15** della **legge IA**, recante "Impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria", stabilisce: "1. Nei casi di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria è sempre riservata al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti. 2. Il Ministero della giustizia disciplina gli impieghi dei sistemi di intelligenza artificiale per l'organizzazione dei servizi relativi alla giustizia, per la semplificazione del lavoro giudiziario e per le attività amministrative accessorie. 3. Fino alla compiuta attuazione del regolamento (UE) 2024/1689, la sperimentazione e l'impiego dei sistemi di intelligenza artificiale negli uffici giudiziari ordinari sono autorizzati dal Ministero della giustizia, sentite le Autorità nazionali di cui all'articolo 20. 4. Il Ministro della giustizia, nell'elaborazione delle linee programmatiche sulla formazione dei magistrati di cui all'articolo 12, comma 1, lettera a) , del d.lgs. 30 gennaio 2006, n. 26, promuove attività didattiche sul tema dell'intelligenza artificiale e sugli impieghi dei sistemi di intelligenza artificiale nell'attività giudiziaria, finalizzate alla formazione digitale di base e avanzata, all'acquisizione e alla condivisione di competenze digitali, nonché alla sensibilizzazione sui benefici e rischi, anche nel quadro regolatorio di cui ai commi 2 e 3 del presente articolo. Per le medesime finalità di cui al primo periodo, il Ministro cura altresì la formazione del personale amministrativo."

[6] Così G. CANZIO, *Indagini e giudizio fra regolamento (UE) 2024/1689 (AI Act) e legge n. 132 del 2025*, in *Giust. ins*., 13/01/2026.

Il testo si compone di **tre titoli**:

- il **titolo I** disciplina l'**utilizzo** dei sistemi di intelligenza artificiale per **l'attività di polizia**" (artt. 1-10);
- il **titolo II** detta disposizioni **penali**, **sostanziali** e **processuali**, in materia di **realizzazione e impiego illeciti** dei sistemi di intelligenza artificiale e disposizioni **processuali civili** in materia di **risarcimento dei danni cagionati** dall'utilizzo dei medesimi sistemi (artt. 11-20);
- il **titolo III** ha infine ad oggetto le disposizioni finali (transitorie e finanziarie) (artt. 21-22).

Il titolo I, destinato all'attività di polizia, si suddivide, a sua volta, in tre capi.

Il **primo capo** è composto delle disposizioni generali e di due articoli (artt. 1-2).

L'art. 1, rubricato "**Oggetto e finalità**" (come meglio si illustrerà nel paragrafo 2.1. della relazione), enuncia, da un lato, la stretta aderenza del testo ai principi regolamentari europei di cui al regolamento IA e alla legge n. 132 del 2025, dall'altro, ribadisce solennemente, nel quadro di quei principi, la necessità di ispirare le attività al rispetto dei diritti fondamentali.

L'art. 2 fornisce le **coordinate definitorie** di base, normative e tecniche, utilizzate dal decreto (per le quali si rimanda nel dettaglio a quanto sarà esposto nel paragrafo 2.1.). Si anticipa solo che, da un punto di vista tecnico, vengono definite le nozioni di "**sistema di IA**", "**di sistema di IA ad alto rischio**", di "**pratiche vietate**", di "**output**", di "**scraping non mirato**" e le categorie di "**dati personali**" rilevanti per l'utilizzo dell'IA.

Il **capo II** (artt. da 3 a 6) detta le disposizioni in materia di **ricerca, sviluppo, addestramento, formazione, sperimentazione** e **utilizzo** dei sistemi di intelligenza artificiale **nelle attività di polizia.**

L'art. 3, rubricato "Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attività di polizia", dispone (come meglio si illustrerà nel paragrafo 2.3.), che queste ultime avvengano nel rispetto dei diritti fondamentali, secondo un approccio **antropocentrico**, **proporzionato** e **fondato sul rischio.** Le attività devono essere orientate alla funzionalità e affidabilità operativa, al miglioramento delle valutazioni e delle decisioni ed in funzione strumentale e di supporto dei fini istituzionali. L'utilizzo dell'IA deve prevedere adeguate forme di **revisione umana**, deve essere tracciabile e deve rispettare la normativa in materia di protezione dei dati personali.

L'art. 4, rubricato "**Collaborazione** nell'ambito della **ricerca** e **sperimentazione scientifica** finalizzata alla realizzazione di sistemi e modelli di intelligenza artificiale per l'attività di polizia" (come meglio si illustrerà nel paragrafo 2.3.), incentiva esperienze di collaborazione delle forze di polizia con università, enti di ricerca e soggetti pubblici e privati.

L'art. 5, rubricato "Sviluppo, realizzazione e prova di determinati sistemi di IA per finalità di polizia negli **spazi di sperimentazione normativa**" (come meglio si illustrerà nel paragrafo 2.3.), intende fornire la base giuridica per il trattamento di dati personali effettuato dalle forze di polizia nell'ambito di spazi di sperimentazione normativa, in particolare per le attività ad alto rischio, anche tramite il coinvolgimento del Garante della protezione dei dati

personali[7]. Viene demandata ad un successivo DPCM la definizione delle modalità di coordinamento tra lo spazio di sperimentazione e le attività di polizia.

Infine, **l'art. 6,** rubricato "**Formazione** del personale di polizia", (come meglio si illustrerà nel paragrafo 2.3.), prescrive l'attivazione, presso i rispettivi istituti di formazione delle forze di polizia, di specifici corsi in materia di intelligenza artificiale per assicurare il conseguimento di risultati formativi minimi che comportino, oltre alla comprensione del funzionamento dei sistemi di IA, anche la consapevolezza delle implicazioni giuridiche, etiche e di responsabilità, nonché dei rischi relativi all'utilizzo.

Il capo III del titolo I (artt. da 7 a 10) è dedicato ai "sistemi di intelligenza artificiale utilizzati nelle attività di polizia per **l'etichettatura, il filtraggio e la categorizzazione di dati biometrici, per l'identificazione biometrica remota in tempo reale** per finalità di prevenzione o di protezione e per il **riconoscimento facciale a posteriori** a fini di contrasto dei reati" e contiene la regolazione degli aspetti più delicati e problematici dell'utilizzo dell'intelligenza artificiale da parte delle forze dell'ordine, disciplinando le specifiche attività tecniche consentite dall'IA, che pongono rilevanti questioni di rispetto dei diritti fondamentali, della libertà e della privacy degli individui. Per questo, le disposizioni sono concepite come volte, più che a indicare gli approcci operativi, a enunciare delle vere e proprie limitazioni e condizioni per l'utilizzo delle nuove tecnologie.

L'art. 7 , (come meglio si illustrerà nel paragrafo 2.4.), consente le attività di **etichettatura, filtraggio e categorizzazione di dati biometrici** per le funzioni di polizia in ipotesi tassative (che impediscano impieghi finalizzati a trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale), sempre che siano esclusivamente finalizzate alle necessità di contrasto, che ne venga impedito il reimpiego per altri fini, che non costituiscano l'unico fondamento di decisioni che producono effetti giuridici nei confronti di persone fisiche e che rispettino la normativa in materia di protezione dei dati personali.

L'a**rt. 8** si occupa dei "sistemi di intelligenza artificiale per **l'identificazione biometrica remota in tempo reale** per finalità di prevenzione, nonché di ricerca delle persone scomparse e delle vittime di specifici reati". La norma (come meglio si illustrerà nel paragrafo 2.4.1.), disciplina l'utilizzo dei sistemi per la ricerca di una persona scomparsa o di persone specifiche, vittime dei reati di sequestro di persona, tratta di esseri umani o sfruttamento sessuale, procedimentalizzando l'attività con una interlocuzione con il **pubblico ministero**, diversamente connotata a seconda che sia inserita o meno in un contesto di urgenza.

L'**art. 9** richiede una **valutazione d'impatto** sui diritti fondamentali, conservazione delle registrazioni e notifica dell'utilizzo dei sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale. Con tale norma (come meglio si illustrerà nel paragrafo 2.4.1.), viene onerato il titolare del trattamento a completare in via preventiva la valutazione indicata, in conformità con quanto previsto dall'articolo 27 del regolamento IA, e ad effettuare

[7] Si veda, in proposito, il parere reso il 14 luglio 2026 dal Garante per la protezione dei dati personali sui Titoli I e III dello schema di decreto legislativo.

la valutazione d'impatto sulla protezione dei dati prevista dagli artt. articoli 23 e 24 del d.lgs. n. 101 del 2018. È inoltre disciplinata la tenuta di un registro per la conservazione dei dati utilizzati dall'IA e la notifica da parte del titolare del trattamento al Garante per la protezione dei dati personali.

L'a**rt. 10** detta disposizioni in materia di sistemi di videosorveglianza dotati della tecnologia di **riconoscimento facciale "a posteriori"**, integrata dall'intelligenza artificiale, per il contrasto dei reati.

La norma (come meglio si illustrerà nel paragrafo 2.5.) stabilisce che i sistemi di videosorveglianza possano essere integrati, a determinate condizioni, con componenti di intelligenza artificiale destinate al riconoscimento facciale.

È previsto uno specifico procedimento che regola le modalità di effettuazione del riconoscimento facciale a posteriori di una persona oggetto di ricerca mirata in quanto indiziata della commissione di un reato, che prevede una interlocuzione **fra il pubblico ministero e il giudice per le indagini preliminari** che deve autorizzarne l'utilizzo.

L'autorizzazione non è richiesta quando il riconoscimento facciale è utilizzato esclusivamente dopo la commissione di un reato al solo fine dell'identificazione iniziale di una persona potenzialmente indiziata della commissione del reato, sulla base di elementi oggettivi e verificabili direttamente connessi al fatto di reato.

Il **Titolo II** (artt. 11-20) detta d**isposizioni penali, sostanziali e processuali** in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale e **disposizioni processuali civili** in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi e si articola in due capi.

Il capo I, rubricato "**Disposizioni sanzionatorie e in materia di procedimento penale**", si compone di 5 articoli (artt. 11-15), che forniscono un nuovo sistema sanzionatorio e procedimentale penale con riferimento a condotte illecite ritenute di particolare gravità, anche tenendo conto della individuazione della misura della pena.

L'art. 11 si limita a richiamare, quanto alle **definizioni**, quelle fornite dall'art. 3 del regolamento IA (come meglio si vedrà nel paragrafo 3.1.).

L'art. 12 (come meglio si illustrerà nei paragrafi da 3.2. a 3.3.4.), inserisce nel **codice penale** il delitto di cui all'**art. 437-*bis*** prevedendo le condotte di **"omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale"** (comma 1) e di **"alterazione illecita dei sistemi"** (comma 2). Per la prima condotta, di forma omissiva, è prevista una ipotesi aggravata qualora dal fatto derivi un pericolo per la sicurezza dello Stato (comma 1, ultimo periodo) ed una fattispecie colposa, limitata alla "colpa grave" (comma 3). Anche per la condotta di alterazione illecita è configurata l'ipotesi aggravata qualora dal fatto derivi un pericolo per la sicurezza dello Stato (comma 2 ultimo periodo). È introdotto, infine, un reato proprio omissivo dell'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio, anch'esso in forma semplice o aggravata (comma 4).

All'art. 13 (come meglio si illustrerà nei paragrafi da 3.4. a 3.4.3), si rinvengono **modifiche al codice di procedura penale** attraverso l'inserimento dell'**art. 359-*ter*,**

rubricato "**Identificazione** e **localizzazione** mediante sistemi di intelligenza artificiale per **l'identificazione biometrica remota in tempo reale**". La norma, nell'ambito **dell'attività di indagine del pubblico ministero**, detta la scansione procedimentale necessaria per l'impiego di sistemi di IA utili alla conferma dell'identificazione di una persona indagata di delitti individuati, ovvero per procedere alla ricerca mirata, ivi compresa la localizzazione, di una persona indiziata di tali delitti.

Nel procedimento ordinario, è necessaria l'**autorizzazione del giudice per le indagini preliminari su richiesta del PM.** In presenza di **ragioni di urgenza**, è il **pubblico ministero** a disporre l'utilizzo del sistema di intelligenza artificiale per l'identificazione biometrica remota in tempo reale, salvo convalida successiva del Gip. Ove le ragioni di urgenza siano tali da non consentire neanche l'attesa del decreto del PM, all'attivazione del sistema provvedono gli **ufficiali di polizia giudiziaria** i quali, senza ritardo e comunque entro le successive dodici ore, trasmettono la richiesta di autorizzazione al PM che ne richiede la convalida al GIP entro ventiquattro ore dall'avvio del sistema. Il mancato rispetto del procedimento o l'impiego dei dati fuori dei casi consentiti dalla legge, determina l'inutilizzabilità dei risultati ottenuti.

L'art. 14 (come meglio si vedrà nel paragrafo 3.5.) contiene una "Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale". Per ragioni di coordinamento con la nuova disciplina, stabilisce che all'articolo **104, comma 1, disp. att.coord.trans. c.p.p.** alla lettera **e-*bis***), le parole: «del profilo personale» sono sostituite dalle seguenti: «generati anche con sistemi di intelligenza artificiale[8]».

L'art. 15, (come meglio si illustrerà nel paragrafo 3.6.), reca modifiche al d.lgs. 8 giugno 2001, n. 231 sulla **responsabilità amministrativa degli enti**, inserendo, dopo l'articolo 25-undevicies, **l'art. 25-*vicies*** rubricato "Reati commessi con l'uso di sistemi di intelligenza artificiale", ove sono previste le **sanzioni pecuniarie applicabili all'ente** in relazione ai delitti di cui all'articolo **437-*bis* c.p.** e di cui all'art. **612-*quater* c.p.** (già direttamente introdotto dalla legge i.a.), con le conseguenti sanzioni interdittive previste dall'articolo 9, comma 2, lettere b), c), d) ed e).

Il **titolo III**, infine, si compone di un unico capo e di due articoli.

L'**art. 21** detta le **disposizioni transitorie** sull'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia, stabilendo il termine dilatorio di un anno per la **conformazione** dei sistemi di intelligenza artificiale in uso alle forze dell'ordine.

Per le disposizioni del titolo I, la cui applicazione è prevista direttamente, ovvero dipende dal regolamento IA, si osservano i termini di entrata in vigore e di compiuta attuazione dello stesso regolamento IA.

[8]Il testo dell'articolo 104 d.lgs. 28 luglio 1989, n. 271, come modificato dal presente decreto, recita: "Il sequestro preventivo è eseguito: - (omissis) - e-*bis*) sui contenuti online generati anche con sistemi di intelligenza artificiale e sui relativi dati, mediante ordine ai prestatori di servizi di hosting, ai fornitori di piattaforme online o di motori di ricerca o ai prestatori di servizi intermediari della società dell'informazione quali definiti all' del Parlamento europeo e del Consiglio, del 9 settembre 2015, di rimuovere i contenuti e i dati o disabilitare l'accesso al profilo, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite".

L'**art. 22** prevede la **clausola di invarianza finanziaria** in base alla quale le amministrazioni interessate provvedono alle attività previste dal decreto mediante l'utilizzo delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

2. Utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia.

2.1. Principi generali.

Il **titolo I** del decreto legislativo è dedicato all'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e dà attuazione **all'articolo 24, comma 2, lett. *h*),** della legge IA, che delega il Governo a prevedere un'apposita disciplina in materia di utilizzo dei sistemi di intelligenza artificiale nell'attività di polizia.

L'integrazione dell'intelligenza artificiale nei contesti giuridici, istituzionali e sociali rappresenta una delle transizioni più complesse ed emblematiche dell'interazione contemporanea tra diritto e tecnologia.

Secondo quanto si legge nella *Relazione illustrativa*, la disciplina dell'utilizzo dei sistemi di intelligenza artificiale in questo ambito "*persegue l'obiettivo di **coniugare** l'**efficacia** dell'azione di prevenzione e contrasto dei reati con la piena tutela dei **diritti fondamentali** e della protezione dei dati personali(...) ponendo particolare attenzione al **bilanciamento** tra esigenze di sicurezza e tutela dei diritti fondamentali, alla regolazione dei casi operativi più sensibili, quali i trattamenti di dati biometrici, attraverso rigorose garanzie procedurali, tecniche e di controllo, alla promozione di un **uso responsabile** e consapevole dell'IA, anche mediante la **formazione** del personale di polizia e la partecipazione a **«spazi di sperimentazione normativa»**, nonché al coordinamento con la normativa, di matrice euro-unitaria, in materia di protezione dei dati personali, con particolare riferimento al trattamento dei dati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica*".

L'adozione pervasiva di sistemi algoritmici di natura decisionale, predittiva e generativa impone una riflessione profonda: essa non si limita alla verifica della loro conformità con i diritti fondamentali, ma si estende alla valutazione della tenuta dei principi democratici e della stessa architettura dello Stato di diritto[9].

[9] In questo scenario, si colloca l'iniziativa del Consiglio d'Europa che, in linea con le proprie finalità istitutive, ha affrontato la questione dell'intelligenza artificiale superando una logica puramente settoriale o tecnico-regolatoria. L'organismo ha, infatti, configurato la materia come una sfida sistemica, capace di incidere direttamente sulla salvaguardia dei diritti umani, sul corretto svolgimento delle dinamiche democratiche e sul rispetto della *rule of law*. Muovendo da tali premesse, la **Convenzione quadro sull'intelligenza artificiale** e i diritti umani, la democrazia e lo Stato di diritto - **approvata il 17 maggio 2024** dal Comitato dei Ministri del Consiglio d'Europa e aperta alla sottoscrizione il 5 settembre 2024 a Vilnius - si configura come il primo schema pattizio a carattere internazionale e giuridicamente vincolante. Tale strumento mira a strutturare un quadro normativo sovranazionale volto a governare le ripercussioni dei sistemi di IA sul nucleo valoriale degli ordinamenti democratici. Vedi, su tali aspetti, l'interessante riflessione di D. CARDAMONE, *La Convenzione quadro del Consiglio d'Europa,* cit., p. 45 ss..

Il decreto legislativo, pur affrontando questioni tecniche e applicative, si sofferma diffusamente a riaffermare i principi di fondo in cui deve muoversi l'utilizzo dei sistemi di intelligenza artificiale per le ragioni preventive e di sicurezza che intende disciplinare.

La necessità di un **bilanciamento** fra le esigenze di sicurezza e quelle di tutela dei diritti fondamentali è contenuta fin dall'**art. 1** del titolo I che enuncia solennemente, al **comma 2**, la cornice di riferimento nella quale le attività delle forze dell'ordine dovranno essere svolte nell'utilizzo dei sistemi di intelligenza artificiale: "Le disposizioni del presente titolo si applicano nel rispetto dei **diritti fondamentali** e delle **libertà** garantite dalla Costituzione, dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché dei principi di **proporzionalità**, di **non discriminazione**, di **sorveglianza umana** e di **trasparenza** di cui all'articolo 3 della legge n. 132 del 2025"[10].

Da evidenziare che il principio di **proporzionalità**, canone ermeneutico di derivazione euro unitaria (art. 5, par. 3 e 4, Trattato UE; art. 49, par. 3 e art. 52, par. 1, della Carta dei diritti fondamentali UE; art. 8 Cedu), entra espressamente fra i parametri ispiratori dell'utilizzo dei sistemi artificiali nelle attività di contrasto.

Il **comma 3** inserisce una consueta **clausola di invarianza** rispetto agli obblighi previsti dal regolamento IA per i sistemi e i modelli di intelligenza artificiale utilizzati nelle attività e per le finalità di polizia.

In tale contesto, la clausola serve principalmente a chiarire che l'adeguamento è funzionale esclusivamente a porre paletti e garanzie per l'esercizio delle attività (es. il divieto di *scraping* non mirato o l'obbligo di autorizzazione del PM per il riconoscimento biometrico), ma non crea nuove competenze o nuovi obblighi al di fuori di quelli previsti dal regolamento

[10] **L'art. 3** della **legge IA** stabilisce i principi generali in materia di intelligenza artificiale approntando un apparato di "difesa preventiva" delle più avanzate conquiste in materia di diritti fondamentali dello Stato di diritto, così disponendo: "1. La ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale per finalità generali avvengono nel rispetto dei **diritti fondamentali** e delle **libertà previste dalla Costituzione**, del diritto **dell'Unione europea e dei princìpi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità**. 2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale per finalità generali avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la **sicurezza**, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati. 3. I sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità e dei princìpi di cui al comma 1, assicurando la sorveglianza e l'intervento umano. 4. L'utilizzo di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e l'esercizio delle competenze e funzioni delle istituzioni territoriali sulla base dei princìpi di autonomia e sussidiarietà e non deve altresì pregiudicare la libertà del dibattito democratico da interferenze illecite, da chiunque provocate, tutelando gli interessi della sovranità dello Stato nonché i diritti fondamentali di ogni cittadino riconosciuti dagli ordinamenti nazionale ed europeo. 5. La presente legge non produce nuovi obblighi rispetto a quelli previsti dal regolamento (UE) 2024/1689 per i sistemi di intelligenza artificiale e per i modelli di intelligenza artificiale per finalità generali. 6. Al fine di garantire il rispetto dei diritti e dei princìpi di cui al presente articolo deve essere assicurata, quale precondizione essenziale, la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza. 7. La presente legge garantisce alle persone con disabilità il pieno accesso ai sistemi di intelligenza artificiale e alle relative funzionalità o estensioni, 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 ai sensi della legge 3 marzo 2009, n. 18.

IA, che resta dunque il riferimento esclusivo per l'interpretazione e l'applicazione delle disposizioni del decreto legislativo[11].

Di ciò si ha una ulteriore conferma nell'**art. 2**, dove è richiamato espressamente l'apparato di **definizioni** utilizzate dal regolamento IA[12].

Pur richiamando integralmente il contenuto del regolamento, per il necessario adattamento interno il decreto legislativo specifica che, per «**Autorità nazionali** per l'intelligenza artificiale» si devono intendere l'Agenzia per l'Italia digitale (**AgID**) e l'Agenzia per la cybersicurezza nazionale (**ACN**)[13], ai sensi dell'articolo 20, comma 1, della legge 23

---

[11] Vedi F. D'ALESSANDRI, *IA e attività di polizia: le nuove regole del d.lgs. n. 160/2026*, in *Quot. giur*, 21/09/2026: "*Quest'ultima previsione è volta ad evitare il fenomeno negativo del* gold plating*, ovverosia l'introduzione, da parte del legislatore nazionale, di una disciplina interna più restrittiva di quella prevista dalla fonte unionale, con la possibile incompatibilità della normativa nazionale con il diritto dell'Unione europea, peraltro in conformità con quanto previsto dall'art. 32, comma 1, lett. c, della Legge 24 dicembre 2012, n. 234 (Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea), ai sensi del quale gli atti di recepimento di direttive dell'Unione europea non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse, ai sensi dell'art. 14, commi 24-bis, 24-ter e 24-quater, della Legge 28 novembre 2005, n. 246*".

[12] L'**Art. 2** rubricato **Definizioni**, così dispone: "1. Ai fini del presente titolo, si intende per:
a) «regolamento IA»: il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale);
b) «legge IA»: la legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»;
c) «sistema di IA»: un sistema di intelligenza artificiale definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689;
d) «pratiche vietate»: le pratiche di IA vietate a norma dell'articolo 5 del regolamento (UE) 2024/1689;
e) «sistema di IA ad alto rischio»: un sistema di IA classificato ad alto rischio, conformemente all'articolo 6 del regolamento (UE) 2024/1689 in combinato disposto con il suo allegato III;
f) «categorie particolari di dati personali»: le categorie di dati di cui all'articolo 3, punto 37), del regolamento (UE) 2024/1689;
g) «dati relativi a condanne penali e reati»: i dati personali di cui all'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;
h) «dati operativi sensibili»: i dati relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, indicati dall'articolo 3, punto 38), del regolamento (UE) 2024/1689;
i) «output»: previsioni, contenuti, raccomandazioni o decisioni generate da un sistema di IA ai sensi dell'articolo 3, punto 1), del regolamento (UE) 2024/1689;
l) «scraping non mirato»: l'estrazione e la raccolta automatizzata e indiscriminata, su larga scala, mediante l'utilizzo di un sistema di intelligenza artificiale, di immagini facciali dalla rete internet o da filmati di telecamere a circuito chiuso, allo scopo di creare o ampliare banche dati di riconoscimento facciale;
m) «Autorità nazionali per l'intelligenza artificiale»: l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN), ai sensi dell'articolo 20, comma 1, della legge 23 settembre 2025, n. 132;
n) «Garante»: il Garante per la protezione dei dati personali, istituito dal codice in materia di protezione dei dati personali, di cui al d.lgs. 30 giugno 2003, n. 196;
o) «Forze di polizia»: le Forze di polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121;
p) «attività di polizia»: le attività di contrasto definite dall'articolo 3, punto 46), del regolamento (UE) 1689/2024, svolte, nell'esercizio delle rispettive attribuzioni e funzioni, dagli organi, uffici e comandi delle Forze di polizia;
q) «finalità di polizia»: i 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, richiamati nei punti 45) e 46) dell'articolo 3 del regolamento (UE) 1689/2024, e per i quali sono svolte le attività di polizia di cui alla lettera s);
2. Per quanto non espressamente previsto dal presente decreto, si applicano le definizioni di cui all'articolo 2 della legge 23 settembre 2025, n. 132, e all'articolo 3 del regolamento (UE) 2024/1689.

[13] V., con riferimento alle evidenti correlazioni fra attività di contrasto e tutela dei dati personali, le osservazioni critiche di R. LATTANZI, *Protezione dei dati personali tra AI Act e Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale. Spunti di riflessione*, in *Quest. giust*., 3, 2026, p. 52 ss., secondo il quale la legge IA non avrebbe dato corretta attuazione all'art. 74, par. 8, del regolamento IA il quale prevede, per taluni sistemi di IA "ad alto rischio", che le autorità di protezione dei dati personali siano altresì chiamate ad operare, e in questa prospettiva designate dagli Stati membri, quali autorità di vigilanza del mercato: "*La richiamata disposizione, all'evidente scopo di innalzare negli ambiti considerati il livello di garanzia, prevede infatti che «per i sistemi di IA ad alto rischio elencati nell'allegato III del (…) regolamento, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III [dell'AI Act], punti 6, 7 e 8, gli Stati membri [designino] come autorità di vigilanza del mercato ai fini [dell'AI Act] le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680». Come è noto, a questa disposizione il legislatore italiano non ha dato attuazione nei termini*

settembre 2025, n. 132; per «Garante», il **Garante per la protezione dei dati personali**, istituito dal codice in materia di protezione dei dati personali, di cui al d.lgs. 30 giugno 2003, n. 196; per «**Forze di polizia**» quelle di cui all'articolo 16 della legge 1° aprile 1981, n. 121[14].

Le Autorità elencate sono quelle preposte in Italia a stabilire le condizioni e a verificare il corretto utilizzo dei sistemi di intelligenza artificiale.

Ad esse si aggiungono, per le rispettive competenze, il Ministro dell'interno e il Ministro della giustizia (oltre al Ministro dell'economia per l'impatto economico), protagonisti di specifiche interlocuzioni per la stesura di DPCM (v. art. 5, u.c., art. 9, comma 5), o DM attuativi (art. 10, comma 12), norme secondarie a cui è demandato nondimeno il dettaglio di aspetti che possono incidere in maniera significativa sul sistema delle tutele, come si vedrà più innanzi.

2.2. Sistemi di intelligenza artificiale "ad alto rischio".

Uno degli aspetti più significativi del regolamento IA è quello di avere delineato un insieme di sistemi per i quali viene richiesto un innalzamento delle tutele e delle protezioni normative.

Il regolamento IA suddivide i sistemi di intelligenza artificiale in **quattro livelli di rischio**.

Questa classificazione è la parte sistematica maggiormente significativa del testo: da essa dipendono gli obblighi a carico dell'azienda, la documentazione richiesta, i controlli da implementare e le sanzioni in caso di violazione.

I quattro livelli, dal più grave al meno grave, sono: rischio inaccettabile (sistemi vietati), alto rischio (sistemi soggetti a obblighi stringenti), rischio limitato (obblighi di trasparenza) e rischio minimo (nessun obbligo specifico).

La classificazione non riguarda la tecnologia in sé ma l'oggetto, il contesto e le finalità dell'uso.

Per quanto concerne la definizione dei sistemi "**ad alto rischio**" che rilevano per l'applicazione del decreto legislativo, deve rinviarsi all'art. 6 del regolamento IA e all'allegato III, ove sono individuate due macroaree.

---

previsti dall'AI Act, atteso che la l. 23 settembre 2025, n. 132 (in particolare, all'art. 20) ha attribuito la qualità di autorità di vigilanza del mercato negli ambiti testé ricordati all'Agenzia per la cybersicurezza nazionale (ACN) – che non soddisfa i requisiti di indipendenza richiesti dall'art. 75, par. 8, AI Act, in quanto agenzia governativa e non autorità indipendente – e non al Garante per la protezione dei dati personali".

[14] L'art. 16, l. 1° aprile 1981, n. 121 individua le forze di polizia: "Ai fini della tutela dell'ordine e della sicurezza pubblica, oltre alla polizia di Stato sono forze di polizia, fermi restando i rispettivi ordinamenti e dipendenze: a) l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza; b) il Corpo della guardia di finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica. Fatte salve le rispettive attribuzioni e le normative dei vigenti ordinamenti, sono altresì forze di polizia e possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica il Corpo degli agenti di custodia e il Corpo forestale dello Stato. Le forze di polizia possono essere utilizzate anche per il servizio di pubblico soccorso". V. MUSACCHIO, *Utilizzo dell'intelligenza artificiale per rafforzare la cooperazione giudiziaria internazionale e il coordinamento informativo nella lotta alle nuove mafie*, in *Riv. pen*., 2026, 1, p. 7, evidenzia l'importanza della creazione di una rete fra forze di polizia aderenti sfruttando l'utilità dei sistemi di intelligenza artificiale anche nel settore della cooperazione internazionale per contrastare la criminalità organizzata.

In base all'**art**. **6**, un sistema di IA è considerato ad alto rischio se sono soddisfatte *entrambe* le condizioni seguenti:

- il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;
- il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.

Tale definizione si applica, peraltro, quando è soddisfatta almeno una qualsiasi delle condizioni seguenti:

a) il sistema di IA è destinato a eseguire un compito procedurale limitato; b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata; c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

Oltre ai sistemi di IA ad alto rischio così individuati, sono considerati ad alto rischio anche i sistemi di IA di cui **all'allegato III**, ove si rinviene una individuazione per settori.

Affinché un sistema di IA di cui all'allegato III sia considerato ad alto rischio deve, in ogni caso, presentare un **rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali** delle persone fisiche.

Sinteticamente e per approssimazione, in tali settori sono ricompresi: la biometria, le infrastrutture critiche (i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità); l'istruzione e formazione professionale; l'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; l'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; migrazione, asilo e gestione del controllo delle frontiere, etc.

Rilevano fra questi, per i sistemi preposti alla sicurezza pubblica e per quelli giudiziari, i settori intitolati: 6. **Attività di contrasto** e 8. Amministrazione della **giustizia** e processi **democratici.**

Un sistema di IA di cui all'allegato III, infine, è sempre considerato ad alto rischio qualora esso effettui **profilazione** di persone fisiche.

In sostanza, il regolamento IA adotta una duplice definizione: *strutturale* che determina l'alto rischio nell'ipotesi in cui il sistema di intelligenza artificiale sia componente di sicurezza di un prodotto o esso stesso un prodotto (regolato dalla disciplina di armonizzazione legislativa in ambito UE), e *funzionale*, legata al settore di impiego dell'IA.

Per la prima definizione soccorre il ***considerando* 50** del regolamento IA che chiarisce che "Per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, **macchine, giocattoli, ascensori**, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente **esplosiva**, apparecchiature **radio**, attrezzature a **pressione**, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano **carburanti** gassosi, **dispositivi medici**, dispositivi medico-diagnostici in vitro, **veicoli automobilistici e aeronautici**".

Per la definizione che abbiamo definito invece *funzionale*, si deve rilevare che i sistemi di intelligenza artificiale ad alto rischio sono per lo più quelli adottati dalle autorità pubbliche per la gestione di compiti istituzionali primari legati all'istruzione, al lavoro, alla gestione dell'immigrazione e, ovviamente, alle attività di contrasto e alla giustizia.[15]

Nell'allegato III del regolamento IA, i sistemi ad alto rischio utilizzati per le **attività di contrasto** sono individuati come segue:

- i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto o per loro conto, per determinare **il rischio** per una persona fisica di diventare **vittima** di reati;
- i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, come **poligrafi** e strumenti analoghi;
- i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'**affidabilità degli elementi probatori** nel corso delle **indagini** o del perseguimento di **reati**;
- i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per determinare il **rischio di commissione del reato** o di **recidiva** in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;
- i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per

[15] Per gli orientamenti della Commissione sulla classificazione dei sistemi di intelligenza artificiale ad alto rischio, è possibile consultare il link https://digital-strategy.ec.europa.eu/it/library/draft-commission-guidelines-classification-high-risk-ai-systems ove sono reperibili le linee guida pubblicate in data 19 maggio 2026.

effettuare la **profilazione** delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'**indagine**, dell'**accertamento** e del **perseguimento** di **reati**.

Tanto premesso, si evince che, con l'espressione «**attività di contrasto**», il legislatore eurounitario ha inteso ricomprendere l'ampio spettro delle funzioni di prevenzione, indagine, accertamento o perseguimento dei reati, nonché l'esecuzione di sanzioni penali e la salvaguardia contro le minacce alla sicurezza pubblica.

Come anticipato, l'oggetto specifico del decreto legislativo in commento per quanto concerne le attività di polizia, va dunque individuato nell'ambito delle attività di contrasto ove, qualora vengano in rilievo profili delicati attinenti al rispetto dei diritti fondamentali e delle libertà individuali, è previsto l'intervento dell'Autorità giudiziaria.

I sistemi ad alto rischio funzionali **all'amministrazione della giustizia** e per processi democratici sono invece:

- i sistemi di IA destinati a essere usati da **un'autorità giudiziaria** o per suo conto per assistere un'autorità giudiziaria nella **ricerca** e nell'**interpretazione** dei fatti e del diritto e **nell'applicazione della legge** a una serie concreta di fatti, o a essere utilizzati in modo analogo nella **risoluzione alternativa delle controversie**[16];
- i sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'**elezione** o di un **referendum** o il comportamento di **voto** delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum. Sono esclusi i sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.

Nella Sezione 2 del regolamento IA sono disciplinati i requisiti richiesti per i sistemi di IA ad alto rischio. Detti sistemi devono possedere requisiti di conformità che tengano conto delle loro previste **finalità,** dello **stato dell'arte** generalmente riconosciuto in materia di IA e di tecnologie correlate all'IA (art. 8 del regolamento IA), nonché del **sistema di gestione dei rischi** previsto dall'art. 9 del regolamento[17].

---

[16] Sul diverso ambito applicativo del regolamento IA e della legge delega IA v. F. PALAZZO, *Notazioni minime su intelligenza artificiale e ruolo del giurista*, in *Cass. pen*. 2026, 2, p. 287. Sull'impatto dell'IA nella valutazione della prova penale v. R.E. KOSTORIS, *Intelligenza artificiale e prove penali*, in *Cass. pen*., 2025, 9, p. 2601.

[17] L'art. 9 del regolamento IA così dispone: "Sistema di gestione dei rischi": 1. In relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un **sistema di gestione dei rischi**. 2. Il sistema di gestione dei rischi è inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. Esso comprende le **fasi** seguenti: a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista; b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72; d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lettera a). 3. I rischi di cui al presente articolo riguardano solo quelli che possono essere ragionevolmente attenuati o eliminati attraverso lo sviluppo o la progettazione del sistema di IA ad alto rischio o la fornitura di informazioni tecniche adeguate. 4. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), tengono in debita considerazione gli effetti e la possibile interazione derivanti dall'applicazione combinata dei requisiti di cui alla presente sezione, al fine di ridurre al minimo i rischi con maggiore efficacia e raggiungere nel contempo un equilibrio adeguato nell'attuazione delle misure volte a soddisfare tali requisiti. 5. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili. Nell'individuare le misure di gestione dei rischi più appropriate, occorre garantire quanto segue: a) l'eliminazione o la riduzione dei rischi individuati e valutati a norma del paragrafo 2, per quanto possibile dal punto di vista tecnico attraverso un'adeguata progettazione e fabbricazione del sistema di IA ad alto rischio; b) ove

I sistemi devono essere sviluppati sulla base di **set di dati** di addestramento, convalida e prova che soddisfino criteri di qualità prestabiliti (art. 10 del regolamento IA).

Il sistema di IA ad alto rischio deve essere accompagnato da **documentazione tecnica** redatta prima dell'immissione sul mercato o della essa in servizio di tale sistema ed è tenuta aggiornata.

Gli eventi (log) devono essere registrati automaticamente per la durata del ciclo di vita del sistema.

A carico dei soggetti che progettano e sviluppano sistemi di IA ad alto rischio, vi sono obblighi di **trasparenza** al fine di consentire ai *deployer*, ossia agli utilizzatori professionali, di usare e di interpretare adeguatamente il sistema (art. 13 del regolamento IA).

L'art. 14 del regolamento IA, infine, detta la norma cardine del sistema introducendo la misura di chiusura della **sorveglianza umana**[18] tanto nella fase della progettazione che dello sviluppo del sistema, in modo che sia garantita *sempre* la possibilità di controllo da parte di persone fisiche durante l'utilizzo.

La definizione di sistemi di intelligenza artificiale "ad alto rischio" è di rilievo fondamentale ai fini delle nuove disposizioni interne introdotte che attengono al settore "attività di contrasto" e "giustizia".

Solo in caso di intervento su sistemi ad alto rischio, ad esempio, può essere integrata la nuova fattispecie incriminatrice introdotta dall'art. 12 del d.lgs. con l'art. 437-*bis* c.p. (paragrafo 3.3.).

---

opportuno, l'attuazione di adeguate misure di attenuazione e di controllo nell'affrontare i rischi che non possono essere eliminati; c) la fornitura delle informazioni richieste a norma dell'articolo 13 e, ove opportuno, la formazione dei *deployer*. Al fine di eliminare o ridurre i rischi connessi all'uso del sistema di IA ad alto rischio, si tengono debitamente in considerazione le conoscenze tecniche, l'esperienza, l'istruzione e la formazione che ci si può aspettare dal *deployer* e il contesto presumibile in cui il sistema è destinato ad essere usato.

[18] L'art. 14 regolamento IA disciplina il sistema di sicurezza della **"Sorveglianza umana**", così prevendo: "1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso. 2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione. 3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti: a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile; b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal *deployer*. 4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al *deployer* in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili; 60/144 ELI: http://data.europa.eu/eli/reg/2024/1689/oj IT GU L del 12.7.2024 d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza. 5. In aggiunta, per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 del presente articolo sono tali da garantire che il *deployer* non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità. Il requisito di una verifica separata da parte di almeno due persone fisiche non si applica ai sistemi di IA ad alto rischio utilizzati a fini di contrasto, migrazione, controllo delle frontiere o asilo, qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito".

2.3. Obblighi di formazione e sperimentazione in funzione dell'utilizzo nell'attività di polizia.

Per la disciplina delle attività di polizia, il decreto legislativo si preoccupa, in primo luogo, di predisporre un adeguato impianto di **strumenti culturali** ed **operativi** volti a fare interiorizzare agli stessi apparati organizzativi la necessità di un uso delle attività di prevenzione dell'intelligenza artificiale proporzionato e strettamente funzionale ad aumentare efficienza ed efficacia degli interventi, che non si distanzi mai dal controllo e dalla riflessione critica sui limiti del suo utilizzo.

Riprendendo la visione antropocentrica e incentrata sul rispetto dei diritti fondamentali che il regolamento IA ha adottato, il capo II del titolo I del decreto legislativo risulta interamente dedicato a formulare e a ribadire la necessità che l'attività delle forze di polizia, che preveda l'utilizzo di sistemi di intelligenza artificiale, sia sottoposta a rigorosi **limiti interni ed esterni**.

Il **capo II**, rubricato "Disposizioni in materia di ricerca, sviluppo, addestramento, formazione, sperimentazione e utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia", si compone di quattro articoli **(artt. 3, 4, 5 e 6)** e si configura come una sorta di introduzione generale all'effettiva normazione sui sistemi di intelligenza artificiale che, in sede applicativa ed in relazione ai diversi utilizzi utili alle attività di sicurezza pubblica allo stato disponibili, verrà sviluppata nel successivo capo III.

Con essa si intende sottolineare che quei sistemi devono essere gestiti in un contesto solido di principi, di formazione, di adeguamento culturale, di sensibilità e, soprattutto, di **controllo umano**.

Specialmente sui sistemi ad "alto rischio", il controllo richiesto si deve concretizzare in attività di sorveglianza preventiva che renda *sempre* necessario l'intervento dell'uomo prima dell'utilizzo finale del sistema.

La **sorveglianza umana** si delinea dunque come **condizione operativa** che entra direttamente nella predisposizione del funzionamento tecnico del sistema di intelligenza artificiale ma anche un parametro di controllo e di interpretazione delle responsabilità che, a partire da tale fondamentale declinazione, si sviluppano nella catena degli interventi che portano all'immissione sul mercato e all'utilizzo dei dispositivi.

L'art. 3 del d.lgs., rubricato "**Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attività di polizia"**[19], ribadisce i principi ispiratori fondamentali adottati dal regolamento IA, disponendo

[19] Art. 3: "**Ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo di sistemi e modelli di intelligenza artificiale per le attività di polizia**". 1. La ricerca, la sperimentazione, lo sviluppo, l'addestramento, l'adozione, l'applicazione, la convalida e l'utilizzo di sistemi e modelli di intelligenza artificiale per le attività e le finalità delle Forze di polizia avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di cui all'articolo 3 della legge IA, secondo un approccio antropocentrico, proporzionato e fondato sul rischio, che tenga conto della classificazione dei sistemi di IA e delle diverse categorie di interessati.2. Le attività di ricerca, sperimentazione, sviluppo e addestramento sono orientate al perseguimento della funzionalità e dell'affidabilità operativa dei sistemi e dei modelli di IA destinati a essere utilizzati dalle Forze di polizia, nella prospettiva di migliorare l'apporto tecnologico dell'intelligenza artificiale alle valutazioni e alle decisioni umane nella relativa attività.3. Le Forze di polizia, in conformità con l'assetto istituzionale vigente e nell'ambito delle proprie competenze, utilizzano i sistemi e i modelli di intelligenza artificiale e i relativi output in funzione strumentale e di

che ricerca, sperimentazione, sviluppo, addestramento e l'utilizzo di sistemi e modelli di intelligenza artificiale per le attività e le finalità delle forze di polizia debbano avvenire nel **rispetto dei diritti fondamentali** e delle **libertà** previste dalla Costituzione, del diritto dell'Unione europea e dei principi di cui all'articolo 3 della legge IA, secondo un approccio **antropocentrico**, **proporzionato** e **fondato sul rischio**, che tenga conto della classificazione dei sistemi di IA e delle diverse categorie di interessati.

I sistemi devono essere affidabili, funzionali, tracciabili e sottoposti a sorveglianza umana.

Si tratta di un vero e proprio manifesto fondativo dell'utilizzo legittimo dell'intelligenza artificiale per ragioni di sicurezza pubblica che deve indurre l'intero settore interessato ad una riflessione attenta e continua.

Ciò significa che l'adozione dell'intelligenza artificiale in tali attività non è un mero esercizio di efficienza tecnologica, ma un processo guidato dal principio cardine della centralità umana, dove ogni algoritmo è progettato per servire l'attività di polizia e di indagine ma senza mai oltrepassare il perimetro invalicabile dei diritti fondamentali dei cittadini.

Il progresso tecnologico e l'efficacia investigativa traggono la loro legittimazione solo dalla capacità di coesistere in perfetto equilibrio con la Costituzione e la Carta dei diritti UE; per questo motivo, la sperimentazione di sistemi avanzati mette al primo posto la trasparenza e lo scudo della protezione dei dati personali.

I sistemi di intelligenza artificiale applicati alla tutela dei cittadini nascono dunque con un **vincolo etico e giuridico** imprescindibile: l'algoritmo deve fermarsi ovunque inizi il diritto fondamentale dell'individuo.

Non vi può essere vera, utile, innovazione senza la garanzia di una supervisione umana qualificata e consapevole, strutturata specificamente per prevenire discriminazioni, riconoscere i limiti degli algoritmi e neutralizzare i *bias* tecnologici prima che possano impattare sulle libertà delle persone.

Il legislatore, inoltre, promuove espressamente **accordi e partenariati** fra forze di polizia e università, enti di ricerca nonché altre istituzioni, pubbliche o private, conscio che, nel moderno scenario della sicurezza pubblica e delle indagini preliminari, l'efficacia e la legittimità dei sistemi di intelligenza artificiale dipendono in modo cruciale dalla loro capacità

---

supporto alle relative attività di polizia, allo scopo di incrementarne l'efficacia e l'efficienza.4. L'utilizzo dei sistemi e dei modelli di IA nell'attività di polizia, conformemente agli obblighi stabiliti dal regolamento IA e fermo restando quanto previsto dal comma 5 in ordine alla sorveglianza umana sui sistemi di IA ad alto rischio, deve prevedere adeguate forme di revisione umana qualificata dei risultati delle elaborazioni automatiche prima del loro impiego in atti e provvedimenti incidenti sulla sfera giuridica degli interessati, nel rispetto dell'autonomia e delle sfere di competenza dei procedimenti decisionali degli appartenenti alle Forze di polizia. La revisione è effettuata da personale individuato dalle procedure interne di ciascuna Forza di polizia ed è documentata in modo da assicurarne la tracciabilità.5. Le Forze di Polizia assicurano che per i sistemi di IA ad alto rischio la sorveglianza umana sia effettiva e conforme a quanto previsto dall'articolo 14 del regolamento IA e che il personale preposto possieda le necessarie competenze e formazione al fine di prevenire e ridurre al minimo i rischi per la salute, la sicurezza e i diritti fondamentali.6. Il trattamento di dati personali nelle attività di cui al comma 1, incluse le categorie particolari di dati personali, i dati operativi sensibili e i dati relativi a condanne penali e reati nella disponibilità delle Forze di polizia in forza di norme di legge o regolamentari ovvero di atti amministrativi generali, è svolto nel rispetto della normativa in materia di protezione dei dati personali, di cui al d.lgs. 18 maggio 2018, n. 51, ferme restando le specifiche disposizioni dettate dal regolamento IA per i sistemi ad alto rischio e quelle contenute nel capo III del presente titolo.7. Le attività di cui al presente articolo sono effettuate senza nuovi od ulteriori obblighi rispetto a quanto disposto dal regolamento IA, ferme restando le esclusioni previste dallo stesso regolamento.

di rimanere costantemente adeguati, tecnologicamente avanzati e conformi ai più alti standard etici e normativi.

L'**art. 4,** rubricato "**Collaborazione nell'ambito della ricerca e sperimentazione scientifica finalizzata alla realizzazione di sistemi e modelli di intelligenza artificiale per l'attività di polizia**", prevede un sistema di collaborazione permanente fra forze dell'ordine e istituzioni di formazione e ricerca.

Per garantire l'aggiornamento continuo dei sistemi complessi ed evitare l'obsolescenza dei sistemi di prevenzione e contrasto al crimine, diventa indispensabile strutturare una collaborazione organica tra le forze di polizia e tali istituzioni.

Tale sinergia, espressamente valorizzata dal legislatore nazionale nell'ambito di specifici progetti di ricerca e sperimentazione scientifica, rappresenta il canale fondamentale per un **trasferimento tecnologico guidato** che consenta di sviluppare soluzioni investigative d'avanguardia nel pieno rispetto dell'approccio antropocentrico, della trasparenza e dei diritti fondamentali dei cittadini richiesti dal regolamento IA.

In tale ambito, particolare attenzione dovrà essere prestata al rispetto della normativa in tema di trattamento dei dati personali.

Non vi è dubbio che il conferimento di dati personali in sede di sperimentazione e studio anche ad enti privati dovrà prevedere elevate forme di cautela circa gli obblighi del trattamento e dell'utilizzo.

Di completamento risulta, dunque, l'**art. 5** rubricato "**Sviluppo, realizzazione e prova di determinati sistemi di IA per finalità di polizia negli spazi di sperimentazione normativa**"[20].

La norma costituisce la base legale per consentire alle forze di polizia di addestrare e testare software di intelligenza artificiale – inclusi quelli ad alto rischio investigativo – all'interno di ambienti digitali protetti e vigilati, denominati "spazi di sperimentazione normativa".

La *sandbox* è un ambiente controllato e vigilato dalle Autorità competenti (in Italia, AgID e ACN), che consente a sviluppatori e fornitori di IA di progettare, addestrare, testare e convalidare i propri sistemi innovativi prima che questi vengano ufficialmente immessi sul mercato o utilizzati.

[20] L'**art. 5** del d.lgs. stabilisce: **"**Il presente articolo costituisce base giuridica ai sensi dell'articolo 59, paragrafo 2, del regolamento IA, nonché del d.lgs. 18 maggio 2018, n. 51, per il trattamento di dati personali, inclusi i dati relativi a reati e le categorie particolari di dati di cui all'articolo 3, punto 37), dello stesso regolamento IA, effettuato dalle Forze di polizia nell'ambito di spazi di sperimentazione normativa per l'intelligenza artificiale, quando tale trattamento è necessario per finalità di polizia. 2. La partecipazione delle Forze di polizia agli spazi di sperimentazione di cui al comma 1 è finalizzata allo sviluppo, alla realizzazione e alla prova di sistemi di IA, in particolare ad alto rischio, destinati alle attività di polizia, nel rispetto della protezione dei dati personali e della tutela dei diritti e delle libertà fondamentali. 3. Negli spazi di cui al presente articolo, la sperimentazione avviene nel rispetto delle condizioni cumulativamente previste dall'articolo 59, paragrafo 1, del regolamento IA, prevede il coinvolgimento del Garante laddove la stessa comporti, per il suo funzionamento, il trattamento di dati personali, ed è oggetto di collaborazione e raccordo con le Autorità nazionali per l'intelligenza artificiale, fermo restando la tutela dei dati operativi sensibili e l'esclusiva titolarità e responsabilità del trattamento degli stessi da parte delle amministrazioni competenti. 4. Con regolamento adottato con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta delle Autorità nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'interno, sentiti il Ministro dell'economia e delle finanze e il Garante, sono definite le modalità di coordinamento tra lo spazio di sperimentazione di cui all'articolo 57 del regolamento IA e le attività del presente articolo.

La sperimentazione deve avvenire sotto costante controllo per garantire che non vengano violati i diritti fondamentali e le norme sulla protezione dei dati.

La norma autorizza eccezionalmente il trattamento di dati personali sensibili, giudiziari e biometrici strettamente necessari alle finalità di sicurezza, a patto che vengano rispettati i vincoli europei del regolamento IA[21] e che vi sia un costante raccordo con le Autorità nazionali dell'IA (AgID e ACN) e con il Garante per la protezione dei dati personali, ferma restando l'esclusiva responsabilità delle forze dell'ordine sulle informazioni operative che debbano restare segrete.

I dettagli applicativi su come coordinare questi test saranno successivamente definiti da un apposito DPCM, su proposta delle Autorità nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'interno, sentiti il Ministro dell'economia e delle finanze e il Garante.

L'**art. 6** del d.lgs. disciplina l'obbligo di **formazione tecnologica e giuridica** per il personale delle forze dell'ordine, delineando le modalità di attivazione dei corsi e le competenze minime da acquisire per l'uso dei sistemi di IA[22]. Le modalità di attivazione sono a **invarianza finanziaria** (comma 1): ciascuna amministrazione di polizia è tenuta a istituire, presso le proprie scuole e istituti di formazione, corsi specifici sull'uso dell'IA applicata alla sicurezza. L'attivazione di tali percorsi deve avvenire in modo autonomo e senza richiedere nuovi stanziamenti economici, sfruttando esclusivamente le risorse umane e finanziarie già a disposizione.

---

[21] L'**Articolo 57 del regolamento IA** disciplina l'istituzione e il funzionamento degli **spazi di sperimentazione normativa** (*AI regulatory sandboxes*), disponendo l'obbligo per gli Stati membri di istituire almeno uno spazio di sperimentazione normativa a livello nazionale, che deve essere operativo dal 2 agosto 2026 (o partecipare a uno spazio già esistente in condivisione con altri Stati). L'**Articolo 59 del regolamento IA** disciplina invece il trattamento secondario dei dati personali all'interno degli spazi di sperimentazione normativa, permettendo in via eccezionale e dunque, sotto strette condizioni, di addestrare i sistemi di IA usando dati reali raccolti inizialmente per altri scopi. Le deroghe investono **finalità di interesse pubblico,** fra cui la prevenzione, accertamento e il contrasto dei reati, ossia le **finalità di polizia**. Il **trattamento dei dati** è ammesso solo se vengono rispettati **rigorosi requisiti cumulativi**: i sistemi di IA devono essere sviluppati per rispondere a un rischio sistemico o elevato in quegli specifici settori di interesse pubblico; vi deve essere la certezza che il test non possa essere effettuato efficacemente usando dati anonimi, sintetici o non personali; devono essere attuati meccanismi di monitoraggio per interrompere immediatamente il test in caso di rischi per i diritti fondamentali; i dati trattati non devono essere condivisi con terzi esterni alla sperimentazione e non possono essere usati per prendere decisioni o misure che influenzino le persone reali coinvolte nei dati. Inoltre, tutti i dati devono essere cancellati o resi anonimi non appena il test è concluso o il periodo di conservazione è terminato; le autorità di vigilanza e i partecipanti devono redigere una relazione dettagliata sulle attività svolte nella *sandbox*. Questo documento viene inserito in un registro pubblico europeo per garantire la massima trasparenza verso i cittadini.

[22] **Art. 6 Formazione** del personale di polizia: "1. Le Forze di polizia provvedono ad attivare, presso i rispettivi istituti di formazione, specifici corsi in materia di intelligenza artificiale applicata alle attività di polizia, secondo modalità stabilite da ciascuna amministrazione nell'ambito delle risorse disponibili a legislazione vigente.
2. I corsi di cui al comma 1 assicurano, in attuazione dell'articolo 4 del regolamento IA, il conseguimento dei seguenti risultati formativi minimi:
a) comprensione dei principi di funzionamento e delle potenzialità dei sistemi di intelligenza artificiale, con particolare riferimento alle loro applicazioni nelle attività di polizia;
b) conoscenza dei limiti, dei bias e degli errori dei sistemi di intelligenza artificiale, con specifica attenzione al riconoscimento biometrico e all'analisi predittiva;
c) capacità di interpretazione critica degli output dei sistemi di intelligenza artificiale e consapevolezza del ruolo della sorveglianza umana qualificata;
d) consapevolezza delle implicazioni giuridiche, etiche e di responsabilità connesse all'utilizzo dei sistemi di intelligenza artificiale a fini di polizia, con specifico riferimento alla disciplina di cui al regolamento IA, al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e al d.lgs. 18 maggio 2018, n. 51;
e) consapevolezza dei rischi di cybersicurezza connessi all'utilizzo dei sistemi di intelligenza artificiale, anche con riferimento alle indicazioni dell'Agenzia per la cybersicurezza nazionale.
3. I risultati formativi di cui al comma 2, lettere b), c) ed e), sono assicurati nell'ambito degli specifici corsi concernenti i sistemi di IA ad alto rischio in uso nelle attività di polizia ovvero destinati a essere utilizzati nelle medesime attività".

In linea con il principio di alfabetizzazione informatica richiesto dal regolamento IA, i corsi devono garantire il raggiungimento di cinque obiettivi didattici chiave (comma 2). Essi consistono nel **funzionamento**: comprendere le potenzialità tecniche dell'IA nel contesto operativo; nel riconoscimento dei **limiti e distorsioni (*bias*)**: riconoscere i margini di errore del software, specialmente nei sistemi di riconoscimento biometrico e analisi predittiva dei reati; nella **valutazione critica:** imparare a interpretare i risultati generati dall'algoritmo, mantenendo centrale il ruolo della **supervisione e del controllo umano** (evitando l'affidamento cieco alla macchina); nel **quadro giuridico ed etico**: acquisire piena consapevolezza delle responsabilità legali e delle tutele della *privacy* (GDPR e normativa penale sulla protezione dei dati); nella **sicurezza informatica**: conoscere i rischi cibernetici legati ai software di IA, seguendo le linee guida fornite dall'Agenzia per la cybersicurezza nazionale **(ACN)**.

Un particolare focus è incentrato, ancora una volta, sui **sistemi ad alto rischio** (comma 3).

La norma determina un vincolo stringente per il quale l'insegnamento relativo agli errori dei sistemi (lettera b), alla sorveglianza umana (lettera c) e ai rischi *cyber* (lettera e) deve essere obbligatoriamente e specificamente inserito in moduli didattici dedicati all'uso dei sistemi di IA classificati ad "alto rischio", sia che siano già operativi, sia che siano di imminente adozione da parte delle forze di polizia.

La consueta clausola di invarianza finanziaria, presente già nella legge delega all'art. 27, lascia grandi perplessità sulle declamate necessità di una formazione completa, attenta e sempre aggiornata, che dovrà affidarsi a competenze elevate e adeguatamente attrezzate per i delicati scopi perseguiti.

2.4. Intelligenza artificiale utilizzata in specifiche attività di polizia. Il trattamento dei dati biometrici.

Dopo avere ribadito i principi generali per l'utilizzo dei sistemi di intelligenza artificiale nell'ambito delle attività di polizia, il decreto legislativo regolamenta nel dettaglio, di fatto, esclusivamente un macrosettore di intervento che è quello della **rilevazione e del trattamento dei dati biometrici**.

Il capo III del decreto legislativo è rubricato: "Sistemi di intelligenza artificiale utilizzati nelle attività di polizia per l'etichettatura, il filtraggio e la categorizzazione di dati biometrici, per l'identificazione biometrica remota in tempo reale per finalità di prevenzione o di protezione e per il riconoscimento facciale a posteriori a fini di contrasto dei reati".

Si tratta, almeno all'attualità, del **settore centrale** dell'utilizzo dell'intelligenza artificiale da parte delle forze di polizia, sia per i vantaggi investigativi delle tecniche di riconoscimento

biometrico, che per le implicazioni in materia di rischio di violazione dei diritti fondamentali che le attività ad esse connesse comportano[23].

Le disposizioni del decreto costituiscono dunque un pacchetto di "condizioni" il cui rispetto è essenziale per l'utilizzo legittimo delle informazioni raccolte, pena l'inutilizzabilità dei risultati.

Va premesso che lo stesso regolamento IA definisce la nozione di "dati biometrici" e di identificazione biometrica:

«**dati biometrici**» (articolo 3, n. 34): i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici;

«**identificazione biometrica**» (articolo 3, n. 35): il riconoscimento automatizzato di caratteristiche umane di tipo fisico, fisiologico, comportamentale o psicologico, allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di persone memorizzati in una banca dati;

«**verifica biometrica**» (articolo 3, n. 36): la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza.

«**sistema di categorizzazione biometrica**» (articolo 3, n. 40): un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive.

L'art. 7 detta limiti per le attività di **etichettatura, filtraggio o categorizzazione di set di dati biometrici**[24].

Il comma 1 dell'art. 7 stabilisce che, nell'ambito delle attività di polizia, l'etichettatura, il filtraggio o la categorizzazione di set di dati biometrici acquisiti in conformità alla normativa vigente, ai sensi dell'articolo 5, paragrafo 1, lettera g), del regolamento IA (inseriti cioè fra le "**attività vietate**"), sono consentiti **a condizione** che:

---

[23] Si veda L. CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. proc. pen*., 2024, 1, p. 245 ss. Sulle tecniche investigative, L. BELVINI, *Intelligenza artificiale e circuito investigativo*, Cacucci, Bari, 2025, pagg. 147 ss..

[24] Il regolamento IA, al *considerando (16)* definisce la nozione di "**categorizzazione biometrica**" come quella riguardante "*l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico. Ciò non comprende i sistemi di categorizzazione biometrica che sono una caratteristica puramente accessoria intrinsecamente legata a un altro servizio commerciale* (…)*"*. L'operazione di "**etichettatura**" è contemplata, invece, all'art. 10, lett. c) del regolamento fra le operazioni di trattamento pertinenti ai fini della preparazione dei dati. A fini descrittivi, si fa presente che tale operazione (*data labeling*) consiste nell'assegnare un nome o una descrizione a un dato biometrico grezzo per spiegare alla macchina cosa sta guardando. È la base per insegnare all'IA a riconoscere le persone (per es*.:* mostrare all'IA mille foto di volti e contrassegnare manualmente ciascuna foto con la scritta "viso", "occhio destro", o associare l'immagine al nome di un sospettato). Il **filtraggio** (*data filtering*) è l'operazione di selezione e pulizia dei dati. Serve a scartare le informazioni inutili, danneggiate o pericolose per evitare che l'algoritmo impari male o sia distorto (*bias*) (per es.: eliminare da un database di impronte digitali quelle sfocate, oppure rimuovere immagini che violano la privacy o che potrebbero indurre l'IA a fare errori di discriminazione).Tale termine viene utilizzato nel sistema SARI Real Time in uso alle forze di polizia, che è stato oggetto di un parere negativo da parte del Garante per la protezione dei dati personali (n. 9575877 del 25/03/2021), proprio per come è progettato il *filtraggio* dei dati in quanto consente di "*analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (watchlist) di 10.000 volti*".

a) non siano finalizzati a inferire o dedurre le caratteristiche di cui all'articolo 5, paragrafo 1, lettera g), del regolamento IA[25];
b) siano funzionali ad attività di comparazione o ricerca ovvero ad ulteriori attività, comunque effettuate conformemente alla normativa vigente ed esclusivamente per finalità di polizia;
c) non costituiscano l'unico fondamento di decisioni che producono effetti giuridici nei confronti di persone fisiche;
d) il titolare del trattamento adotti misure idonee a prevenire il reimpiego dei dati e dei risultati per finalità incompatibili con quelle per cui sono stati raccolti.

In sintesi, l'art. 7, così come previsto dall'ultimo periodo del paragrafo 1, lett. g) dell'art. 5 del regolamento IA, stabilisce che le forze di polizia possono compiere le operazioni di etichettatura, filtraggio o categorizzazione di set di dati biometrici **solo nel rispetto dei limiti imposti dalle lettere da a) a d)**.

Particolare attenzione deve porsi fin da ora alla previsione di cui alla **lett. c) del comma 1 dell'art. 7** del d.lgs., che diventa un vero e proprio canone ermeneutico per l'assunzione di decisioni nel contesto in riferimento, ossia quello dell'ambito di intervento autonomo delle forze dell'ordine, impedendo che qualsiasi decisione possa essere assunta *solo* sulla base dei risultati ottenuti tramite l'utilizzo dell'intelligenza artificiale.

La lettera c) fa espresso riferimento a **decisioni** che producono **effetti giuridici** nei confronti di persone fisiche.

Nell'ambito dell'attività di prevenzione in senso stretto delle forze dell'ordine vengono in rilievo, sotto tale profilo, tutte le misure amministrative personali che possono essere adottate prima o indipendentemente dalla commissione di un reato come, a titolo esemplificativo, l'avviso orale del questore (art. 3 d.lgs. 6/9/2011, n. 159), il divieto di accedere alle manifestazioni sportive D.A.SPO. (art. 6 l. 13/12/1989, n. 401), il divieto di accesso ad aree urbane (artt. 9 e 10 d.l. 20/02/2017, n. 14, convertito, con modificazioni, dalla l. 18/04/2017, n. 48), l'ammonimento nei casi di atti persecutori e di violenza domestica (art. 3 d.l. 14/08/2013, n. 93 convertito con modificazioni dalla l. 15/10/2013, n. 119 e art. 3 l. 19/06/2019, n. 69), il fermo di prevenzione di polizia (art. 7, comma 2, d.l. n. 23 24 febbraio 2026, n. 23, convertito, con modificazioni, dalla l. 24 aprile 2026, n. 54), le perquisizioni personali di iniziativa (art. 4 l. 22/05/1975, n. 152; art. 41 TULPS; art. 103 comma 2, DPR 9/10/1990, n. 309).

Il comma 2 dell'art. 7 stabilisce che il **trattamento di dati personali** nelle attività di etichettatura, filtraggio o categorizzazione di set di dati biometrici debba tener conto della classificazione dei sistemi di IA (con particolare riferimento, dunque, ai sistemi "ad alto rischio"), avuto riguardo anche agli **orientamenti della Commissione europea**

[25] L'**art. 5** del regolamento IA stabilisce quali siano le **pratiche vietate** di intelligenza artificiale. Fra di esse vi sono quelle definite al paragrafo 1, lett. g): "l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a **razza**, **opinioni politiche**, **appartenenza sindacale**, convinzioni **religiose** o **filosofiche**, **vita sessuale** o **orientamento sessuale;** tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto".

sull'attuazione pratica del regolamento IA, ai sensi degli articoli 6, paragrafo 5, e 96, dello stesso regolamento, ed è svolto nel rispetto di quanto previsto dal d.lgs. 18 maggio 2018, n. 51 in materia di *privacy*.

Gli orientamenti della Commissione europea[26], oltre ad individuare esempi pratici applicativi delle specifiche attività consentite e vietate, hanno l'essenziale compito di consentire l'aggiornamento costante delle stesse alla luce della velocità di modifica delle tecniche utilizzate dai sistemi, costituendo uno strumento flessibile e, al contempo, necessario, per l'uniformità delle pratiche nello spazio europeo.

2.4.1. L'identificazione biometrica remota in tempo reale.

Nell'**art. 8** è inserita la disciplina delle attività di polizia maggiormente efficaci da un punto di vista delle esigenze della sicurezza e, per questo motivo, anche più incisive dal punto di vista della compressione dei diritti individuali, costituite dalla **identificazione biometrica remota in tempo reale**.

Va ribadito che tale disciplina riguarda esclusivamente l'attività di polizia in chiave preventiva e non ancora repressiva.

Il legislatore limita in maniera chiara l'ambito di intervento nel quale operano le forze di polizia attraverso il procedimento delineato dall'art. 8 e lo tiene distinto, sia con riferimento alla struttura che rispetto all'utilizzo dei dati acquisiti, da quello introdotto per le attività di indagine in senso stretto, disciplinato dal successivo art. 13 che inserisce l'art. 359-ter nel codice di procedura penale (paragrafo 3.4).

Tale limitazione viene rafforzata dal comma 8 dell'art. 8 che, richiamando l'art. 226, comma 5 in tema di intercettazioni, vieta espressamente l'utilizzazione nel procedimento penale dei risultati ottenuti attraverso le attività preventive *fatti salvi i fini investigativi*.

Pur con tali distinzioni, la consapevolezza del legislatore in ordine al rischio connesso all'utilizzo di tali tecnologie sui diritti della persona si è tradotta, anche per l'identificazione in tempo reale a meri fini di prevenzione, nella procedimentalizzazione dell'attività e nell'intervento necessario, per l'utilizzazione dei risultati agli scopi espressamente previsti, dell'Autorità giudiziaria che si identifica, come si vedrà, nel pubblico ministero.

Va premesso che l'identificazione biometrica remota in tempo reale consiste in un procedimento nel quale l'oggetto del trattamento sono dati biometrici, ossia relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica (come, ad es. riconoscimento facciale, analisi della camminata o della voce), che vengono convertiti *in via immediata* in un modello algoritmico univoco per consentire l'identificazione.

---

[26] L'**art. 6** del regolamento IA, rubricato "**Regole di classificazione per i sistemi di IA ad alto rischio",** al paragrafo 5 stabilisce che "Dopo aver consultato il consiglio europeo per l'intelligenza artificiale («consiglio per l'IA»), ed entro il 2 febbraio 2026, la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo in linea con l'articolo 96, insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio". Come già anticipato alla nota 14, per la consultazione degli orientamenti della Commissione sulla classificazione dei sistemi di intelligenza artificiale ad alto rischio, è possibile andare al link https://digital-strategy.ec.europa.eu/it/library/draft-commission-guidelines-classification-high-risk-ai-systems ove sono reperibili le linee guida pubblicate in data 19 maggio 2026.

Ai sensi dell'art. 3, n. 41 del Regolamento IA, un sistema è "remoto" quando è destinato all'**identificazione** di persone fisiche tipicamente **a distanza** e, elemento cruciale, **senza il loro coinvolgimento attivo**[27].

Ciò differenzia radicalmente la fattispecie, ad es., dai sistemi di verifica biometrica standard, in cui l'utente collabora attivamente (come lo sblocco di uno smartphone tramite impronta o FaceID): il sistema remoto rileva invece una moltitudine di soggetti in modo passivo e simultaneo all'interno di un determinato contesto.

L'identificazione si realizza mediante il **confronto automatizzato** dei dati biometrici della persona intercettata con i dati biometrici preesistenti e memorizzati all'interno di una banca dati di riferimento.

Il successivo n. 42 dell'art. 3 del regolamento specifica che l'acquisizione dei dati biometrici, il confronto e l'identificazione devono avvenire **«senza ritardi significativi»**. La norma precisa rigorosamente che la nozione di "sistema di identificazione biometrica remota in tempo reale" include l'**identificazione istantanea** e quella che avviene con **brevi e limitati ritardi temporali**, al fine di evitare qualsiasi elusione.

L'art. 8 del d.lgs. disciplina l'ambito *ristretto e controllato* di attività che le forze di polizia possono compiere utilizzando tali sistemi.

A tale fine, i principi ispiratori della disposizione vanno rinvenuti nell'art. **5 paragrafo 1 lett. h del regolamento IA** che inserisce, fra le **attività vietate** di utilizzazione dei sistemi di intelligenza artificiale, anche 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** al conseguimento di specifici obiettivi.

Fra tali obiettivi si collocano le attività di prevenzione e investigative demandate alle forze di polizia, parte integrante delle funzioni di contrasto che il regolamento assume, come si è visto, nell'ambito delle attività "ad alto rischio".

Specularmente, il regolamento IA ha circoscritto la liceità dell'impiego dell'IA - ancorandola rigorosamente al criterio della stretta necessità - al solo perseguimento di tre tassativi e imperativi obiettivi:

- la ricerca mirata e selettiva di specifiche vittime di reati di particolare gravità, quali il sequestro di persona, la tratta di esseri umani o lo sfruttamento sessuale, nonché il rintraccio di persone scomparse (i);

- la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche, ovvero il contrasto a un pericolo reale e attuale - o concretamente prevedibile - connesso al compimento di attacchi terroristici (ii);

[27] Nelle linee-guida in materia di riconoscimento biometrico e firma grafometrica di cui all'Allegato A del provvedimento del Garante per la protezione dei dati personali del 12.11.2014 è contenuta la seguente definizione: "*I sistemi biometrici sono detti **interattivi** o partecipativi laddove prevedono la cooperazione dell'interessato e richiedono la sua consapevole partecipazione durante la fase di raccolta del dato biometrico (si pensi, ad esempio, alla scansione della retina o all'apposizione della firma autografa). I sistemi biometrici **passivi**, invece, raccolgono il dato biometrico senza che l'interessato ne abbia piena percezione o consapevolezza (si pensi, ad esempio, all'acquisizione delle immagini del volto o alla registrazione della voce senza che l'interessato ne sia a conoscenza)*".

- la localizzazione o l'identificazione di un soggetto sospettato di aver commesso un illecito penale, finalizzata allo svolgimento delle indagini, all'esercizio dell'azione penale o all'esecuzione di una sanzione, purché si tratti di fattispecie delittuose espressamente contemplate dall'Allegato II e punibili nello Stato membro interessato con una pena o misura di sicurezza privativa della libertà personale della durata massima non inferiore a quattro anni (iii).

L'art. 8 del d.lgs. disciplina le ipotesi di utilizzo in deroga **limitatamente agli obiettivi ricompresi ai punti i) e ii)**, dunque limitatamente alle attività di prevenzione in senso stretto delle forze di polizia[28].

La norma formula, infatti, una espressa riserva con riferimento all'introduzione dell'art. 359 c.p.p. ad opera del successivo art. 13, che procedimentalizza l'attività di utilizzo di tali sistemi nell'ambito delle indagini per il perseguimento dei reati (e sul quale si tornerà più oltre al paragrafo 3.4.), riferendosi al terzo obiettivo previsto dalla lett. h) (iii), dunque all'attività di indagine vera e propria.

Si noti che, mentre per gli obiettivi di cui al punto i) richiamato, vi è un riferimento alla *gravità* del reato di cui la persona da ricercare sia vittima, l'obiettivo di cui al punto (ii) è circoscritto in relazione alla minaccia incombente per la vita o l'incolumità fisica personale (dunque anche con riferimento a potenziali lesioni personali), o al pericolo concreto di attacchi terroristici.

In base al comma 2 dell'art. 8 l'utilizzo dei sistemi di IA è consentito **esclusivamente per confermare l'identità delle persone** specificamente interessate ovvero per la **ricerca mirata**, anche in modo dinamico e compresa la localizzazione, di persone specificamente individuate o individuabili in relazione alla minaccia da prevenire o alla ricerca da eseguire.

Il comma 3 disciplina il procedimento di utilizzo dei dati acquisiti attraverso il sistema di videosorveglianza remota, imponendo che il confronto biometrico avvenga esclusivamente con **una banca dati** di riferimento adeguata per ciascuna delle finalità consentite, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate anagraficamente, di cui al comma 2[29].

La banca dati può essere derivata da dati contenuti in ulteriori banche dati in uso alle forze di polizia o tenute da altre pubbliche amministrazioni e accessibili alle predette forze, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle attività di polizia.

---

[28] Il carattere "preventivo" dell'attività delle forze di polizia, si contrappone a quello "repressivo" proprio della polizia giudiziaria, ed è tipico dell'attività di polizia amministrativa, nel cui ambito è riconducibile l'attività di polizia di sicurezza, finalizzata a neutralizzare tutti i pericoli e le turbative che pregiudicano incolumità e ordine pubblico. V. P. TONINI, *Polizia giudiziaria e magistratura*, Giuffrè 1979, p. 119. Non appena giunge la notizia che è stato commesso un reato, viene esercitata invece la funzione di p.g. con uso dei poteri coercitivi, v. P. TONINI-C. CONTI, *Lineamenti di diritto processuale penale*, Giuffrè, 2024, p. 70.

[29] Secondo G.M. RICCIO, *d.lgs. 160/2026: l'adeguamento all'AI Act tra attività di polizia e responsabilità civile*, in *Quot. giur.,* 17/09/26, la creazione di una banca dati specifica costituisce una garanzia strutturale che merita apprezzamento, poiché limita il rischio, di una progressiva costituzione di "banche dati generali" di riconoscimento facciale per accumulo di autorizzazioni singole. Resta, tuttavia, da verificare, sul piano pratico, l'effettività del controllo sulla cancellazione, affidato in larga parte a un decreto attuativo del Ministro dell'interno non ancora adottato.

Il contenuto della banca dati è formato appositamente per ciascun utilizzo con i soli dati biometrici pertinenti alla specifica finalità, che **sono cancellati al termine della validità dell'autorizzazione**, in modo da garantire che il set di confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto alle autorizzazioni pregresse.

È in ogni caso vietato l'uso di banche dati biometriche alimentate, in tutto o in parte, mediante tecniche di ***scraping*** non mirato, ovvero costituite in violazione delle disposizioni vigenti in materia di protezione dei dati personali[30].

È soprattutto il profilo della **raccolta indiscriminata** che preoccupa il legislatore che intende dunque limitare e, per quanto è possibile, controllare, ogni rischio di profilazione a priori e di impiego sistematico di dati personali con l'uso dei sistemi di intelligenza artificiale.

E' stato evidenziato, infatti, come la diffusione massiva, incontrollata e priva di idonee garanzie procedimentali di sistemi di sorveglianza dotati di tali prerogative tecnologiche negli spazi pubblici determinerebbe la configurazione di un regime di vigilanza permanente e panottica, che finirebbe per concretizzare le più severe distopie dottrinali in materia di controllo biopolitico e intrusione capillare delle autorità di pubblica sicurezza nelle esistenze dei consociati, arrecando un *vulnus* definitivo al nucleo essenziale dei diritti fondamentali, con particolare riferimento alle libertà di movimento, di riunione e al diritto alla riservatezza (*ex* artt. 7 e 8 della Carta dei Diritti Fondamentali dell'UE) [31].

Da tali premesse, deriva il principio secondo cui, negli ordinamenti fondati sul costituzionalismo di matrice liberale e democratica, le esigenze di sicurezza e di prevenzione dei reati non possono assurgere a scriminante per un impiego indiscriminato o sproporzionato dello strumento tecnologico.

L'utilizzo dell'identificazione biometrica remota in tempo reale deve pertanto configurarsi quale *extrema ratio*, deve essere rigidamente confinato in ambiti specifici e subordinato a ipotesi eccezionali, tipiche e tassative, governate dai canoni di adeguatezza e stretta proporzionalità.

Per tale ragione, il legislatore ha configurato **obblighi procedimentali stringenti,** che prevedono l'interlocuzione con l'Autorità giudiziaria e che si concretizzano nella necessità di

---

[30] Si veda in materia di ***scraping*** il provvedimento del Garante per la protezione dei dati personali del 20 maggio 2024, pubblicato sulla Gazzetta Ufficiale Serie Generale n. 132 del 7 giugno 2024 e la relativa nota informativa. Lo *scraping*, letteralmente "raschiamento dei dati", si definisce come un insieme di tecniche informatiche automatizzate finalizzate all'estrazione, raccolta e archiviazione sistematica di dati e contenuti liberamente accessibili sul web, al fine di riutilizzarli per scopi differenti da quelli originari che, benché su informazioni, compie un'estrazione con modalità massive, programmatiche e non autorizzate. L'attività viene eseguita con un meccanismo tecnico tramite script informatici, bot, *crawler* o *spider* che interrogano i server web a ritmi e volumi infinitamente superiori rispetto alle capacità di un utente umano, simulando la navigazione ma duplicandone in automatico i contenuti. Il software non si limita a visualizzare la pagina web, ma esamina il codice sorgente (HTML, XML, JSON), estrae i dati specifici d'interesse (es. elenchi di prezzi, indirizzi email, post di social network, immagini) e li organizza in un database strutturato (es. in formati CSV o database SQL).Lo *scraping standard* si concentra su dati pubblicati in chiaro sul web, senza superare barriere informatiche o sistemi di autenticazione (credenziali) e può non essere intrinsecamente illegale ma lo può diventare quando vengano, ad es., utilizzati con modalità massive dati personali per finalità non consentite, in assenza di consenso o di informativa all'utenza, violando la normativa in materia di protezione dei dati personali. Se lo scraping viene eseguito forzando protezioni informatiche, eludendo blocchi IP o superando meccanismi di autenticazione, la condotta potrebbe integrare anche la fattispecie di accesso abusivo a un sistema informatico o telematico (art. 615-*ter* c.p.).

[31] Vedi N. ROSSI, *L'intelligenza artificiale entra nelle attività di polizia e nelle indagini preliminari,* in *Quest. giust*., 2/10/2026.

una richiesta a motivazione vincolata e stringente che deve promanare dai vertici delle forze di polizia coinvolte nell'utilizzo.

L'Autorità giudiziaria individuata in questo troncone procedimentale è esclusivamente il **pubblico ministero**.

In base al comma 4 dell'art. 8 del d.lgs., l'utilizzo dei sistemi di IA ai fini indicati è subordinato a una **richiesta** del questore o del comandante provinciale dell'Arma dei carabinieri e della Guardia di finanza, ovvero dei responsabili dei Servizi centrali di cui all'articolo 12 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203[32], rivolta **al procuratore della Repubblica**[33] presso il Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione ovvero di ricerca, con indicazione della **finalità** perseguita, della **durata** prevista, dell'**area territoriale** interessata, delle **persone** interessate e ricercate, delle **banche dati** di riferimento utilizzate e dei **sistemi** e delle **tecnologie** impiegati.

Anche l'autorizzazione del pubblico ministero è sottoposta a vincoli di specificità, oltre che temporali e spaziali.

Il successivo comma 5 dell'art. 8 stabilisce che "L'**autorizzazione** deve essere concessa con riguardo a uno specifico evento o per il tempo strettamente necessario, in ogni caso non superiore a **quindici giorni**, prorogabili dal procuratore della Repubblica, con decreto motivato per periodi successivi di quindici giorni qualora permangano le condizioni di cui al comma 1, nonché con riferimento ad una area territoriale delimitata e alla indicazione delle persone specificamente interessate e ricercate. La medesima autorizzazione può essere concessa, altresì, soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento IA"[34].

---

[32] Si tratta dei servizi specializzati centrali e interprovinciali interforze come ad. es. presso la polizia di Stato lo S.c.o. e i centri interprovinciali criminalpol; presso l'Arma dei carabinieri il R.o.s. e la sezione anticrimine, presso la Guardia di finanza lo S.c.i.c.o. e il G.i.c.o.

[33] Per G.M. RICCIO, *d.lgs. 160/2026,* cit., "*la scelta di affidare l'autorizzazione al pubblico ministero, anziché a un organo giurisdizionale terzo, si espone a un raffronto non scontato con l'art. 5, paragrafo 3, dell'AIAct, che discorre di «autorizzazione preventiva [...] rilasciata da un'autorità giudiziaria o amministrativa indipendente»: la qualificazione del pubblico ministero italiano come «autorità giudiziaria» ai fini della norma europea è difendibile alla luce della collocazione ordinamentale della magistratura requirente, ma la questione della sua «indipendenza» rispetto all'organo che richiede la misura (le stesse Forze di polizia con cui il procuratore coopera nelle indagini) potrà essere oggetto di ulteriori chiarimenti, eventualmente da parte della Corte di giustizia, ove le prassi applicative dovessero mostrare un'autorizzazione sostanzialmente automatica".*

[34] In base **all'art. 5, paragrafo 2**, del regolamento IA: "L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), è applicato ai fini di cui a tale lettera, solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti: - la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema; - le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze. L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), del presente articolo rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali. L'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico è autorizzato solo se l'autorità di contrasto ha completato una valutazione d'impatto sui diritti fondamentali come previsto all'articolo 27 e ha registrato il sistema nella banca dati UE conformemente all'articolo 49. Tuttavia, in situazioni di urgenza debitamente giustificate, è possibile iniziare a usare tali sistemi senza la registrazione nella banca dati dell'UE, a condizione che tale registrazione sia completata senza indebito ritardo".

Il richiamo all'art. 5, paragrafo 2 del Regolamento IA, comporta che il pubblico ministero possa ritenere utilizzabile il sistema di identificazione in oggetto ***solo*** **al fine di confermare l'identità** della persona specificamente interessata e che sia vincolato al compimento di una valutazione rigorosa sul rispetto del principio di proporzionalità che tenga conto del bilanciamento fra la gravità delle esigenze di individuazione prospettate (*la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema*), e i diritti e libertà delle persone interessate.

In linea con l'attenuamento e la posticipazione della necessità di interlocuzione con l'Autorità giudiziaria, che si riscontra, in generale, nella procedimentalizzazione delle attività che devono compiersi nell'immediato, il **comma 6** contempla anche un **procedimento d'urgenza** che elimina la preventiva interlocuzione con il pubblico ministero che viene posticipata: "Nei casi d'urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare un **pregiudizio grave e irreparabile** per le finalità di cui al comma 1, l'utilizzo del sistema di IA può essere avviato, su disposizione del questore, dei comandanti o dei responsabili indicati al comma 4, dall'organo di polizia procedente, previa comunicazione, anche **in forma orale**, al procuratore della Repubblica, e a condizione che sia limitato a quanto strettamente necessario, in ogni caso con delimitazione dell'area interessata e indicazione delle persone ricercate".

In tale ipotesi, prosegue il **comma 7,** la richiesta di autorizzazione è solo posticipata e viene "trasmessa al procuratore della Repubblica **senza ritardo** e in ogni caso entro ventiquattro ore dall'inizio delle operazioni. Il procuratore della Repubblica, ove ritenga sussistenti le condizioni di cui al medesimo comma 6, provvede nelle successive ventiquattro ore".

La sanzione in caso di uso dei sistemi al di fuori delle condizioni e dei termini previsti dai commi 4, 5, 6 e 7 dell'art. 8, ovvero in caso di mancata autorizzazione, è che l'utilizzo del sistema di intelligenza artificiale oggetto dell'autorizzazione deve essere immediatamente interrotto e tutti i dati personali, i risultati e gli output acquisiti e prodotti devono essere **cancellati**, *fatti salvi gli elementi acquisiti legittimamente sotto altra base giuridica conforme al d.lgs. n. 51 del 2018*, con **divieto di utilizzazione** dei risultati forniti dai sistemi di intelligenza artificiale anche a fini preventivi "puri".

Si consolida dunque il principio cardine secondo cui, all'interno di ordinamenti fondati sul costituzionalismo che intendano preservare la propria fisionomia democratica e pluralista, le pur legittime istanze di prevenzione e di tutela della sicurezza pubblica non possono in alcun modo farsi scudo per giustificare un ricorso indiscriminato o massivo a strumenti di identificazione biometrica remota in tempo reale.

L'ultimo comma dell'art. 8 stabilisce, infine, come si è anticipato, che si applichino le disposizioni di cui all'articolo 226, comma 5, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui all'allegato al d.lgs. 28 luglio 1989, n. 271.

È una norma di chiusura fondamentale che, a scanso di equivoci (che potrebbero ingenerarsi per la presenza della interlocuzione con il pubblico ministero), determina la

definitiva ed esclusiva collocazione sistematica del procedimento nell'ambito delle attività di prevenzione.

Il richiamato **art. 226, comma 5**, in tema di intercettazioni (sarà necessario un adeguato coordinamento), stabilisce il principio generale **di divieto di utilizzo delle attività preventive nel procedimento penale** se non a fini investigativi: "In ogni caso gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel procedimento penale, fatti salvi i fini investigativi. In ogni caso le attività di *intercettazion*e preventiva di cui ai commi precedenti, e le notizie acquisite a seguito delle attività medesime, non possono essere menzionate in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgate".

In linea con il procedimento individuato, che coinvolge l'autorità giudiziaria esclusivamente nella persona del pubblico ministero (a differenza di quanto si vedrà è previsto per la localizzazione o l'identificazione di un soggetto che abbia commesso un illecito penale nell'ambito di attività di indagine vera e propria ove è prevista l'interlocuzione con il GIP), il decreto ribadisce così il carattere meramente *preventivo* dell'attività svolta dalle forze di polizia, rafforzando la cesura già tracciata con la distinzione procedimentale fra il perseguimento degli obiettivi di cui ai punti (i) e (ii) delineati dall'art. 5, paragrafo 1 lett. h del regolamento IA, e gli obiettivi di cui al successivo punto (iii).

Non può non rilevarsi, tuttavia, che l'obbligo di procedimentalizzazione introdotto manifesta la piena consapevolezza da parte del legislatore del carattere estremamente invasivo che contraddistingue tali attività e del loro forte impatto sui diritti della persona.

Va aggiunto che la distinzione fra attività di prevenzione e attività repressiva, chiara da un punto di vista teorico, risulta complicata agli effetti pratici poiché spesso l'attività di polizia giudiziaria si configura alla stregua di una progressione dell'attività di polizia amministrativa e di sicurezza, qualora la notizia di reato emerga proprio dalle operazioni di vigilanza e osservazione derivanti dallo svolgimento di quest'ultima[35].

Così come già è stato messo in evidenza a proposito delle intercettazioni[36], tali attività preventive sono formalmente estranee agli scopi tipici dell'accertamento penale ma la linea di confine rispetto alle procedure di identificazione che si svolgono nel corso delle indagini (disciplinate dal nuovo art. 359-*ter* c.p.p.), non può dirsi netta[37], dal momento che la polizia di sicurezza spesso indossa anche le vesti di polizia giudiziaria.

Sarà demandato al pubblico ministero, dunque, non solo il compito di controllare le iniziative delle forze di polizia ma anche di determinare la cessazione delle attività preventive non appena sia stata acquisita una *notizia criminis* [38]. Da quel momento in poi, si deve ritenere che i risultati delle attività non potranno più essere utilizzati se non azionando le garanzie procedimentali di cui all'art. 359-*ter* c.p.p. nelle ipotesi tassative in esso previste.

---

[35] D. MANZIONE, *Polizia giudiziaria*, in *Enc. dir., Agg*., VI, p. 857.
[36] W. NOCERINO, *Le intercettazioni e i controlli preventivi,* Cedam, 2019, p. 91
[37] P. BALDUCCI, *Le garanzie nelle intercettazioni fra costituzione e legge ordinaria,* Giuffré, 2002, p. 87 ss..
[38] Così, per le intercettazioni, G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Giuffré, 1983, pp. 176 ss..

L'art. 9 del d.lgs., rubricato "**Valutazione d'impatto sui diritti fondamentali, conservazione delle registrazioni e notifica dell'utilizzo dei sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale**", predispone una serie di cautele e di regole programmatiche per l'utilizzazione di un sistema di intelligenza artificiale per il riconoscimento biometrico a distanza in tempo reale per scopi di polizia o di indagine penale.

Il testo fa riferimento al "responsabile del trattamento dei dati"[39] che, nel linguaggio del regolamento IA, coincide con il *deployer*[40], il quale, prima di attivare il sistema, deve obbligatoriamente completare due valutazioni: una per analizzare l'impatto sui diritti fondamentali delle[41] e una specifica sulla tutela della privacy e dei dati personali.

È prevista, inoltre, la **registrazione obbligatoria** delle attività: ogni qual volta venga utilizzata l'intelligenza artificiale allo scopo indicato, il sistema deve registrare l'operazione in automatico all'interno di file di cronologia (log) blindati e non modificabili. Questi file devono contenere tutte le informazioni minime richieste dalla legge europea, vanno custoditi **per cinque anni**[42] dal momento dell'uso e possono essere consultati solo dalle autorità competenti per finalità di verifica della liceità del trattamento, di controllo interno e nell'ambito di un procedimento penale.

Il comma 4 prevede la necessità che il titolare del trattamento, dopo l'utilizzo dei sistemi di cui al comma 1, effettui **una notifica al Garante**, in conformità a quanto previsto dall'articolo 5, paragrafo 4, del regolamento IA[43].

Nel procedimento di notifica interviene **l'autorità giudiziaria** competente (il **pubblico ministero**), che deve rilasciare un apposito **nulla osta** (che può essere differito per un periodo non superiore a tre mesi, rinnovabile per una sola volta, in presenza di specifiche esigenze di segretezza), contenente le informazioni essenziali sull'autorizzazione rilasciata e sul risultato conseguito con l'utilizzo del sistema e che non include dati operativi sensibili. Nel

---

[39]Per le forze di polizia, il titolare del trattamento dei dati personali ai fini della legge sulla *privacy* viene individuato nell'ambito delle rispettive strutture di competenza. Si veda il "Modello organizzativo privacy dell'Arma dei carabinieri", reperibile *on line*, che individua il titolare del trattamento nell' "Arma dei Carabinieri"; per la Polizia di Stato è il Ministero dell'Interno, per la Guardia di Finanza è il Corpo della Guardia di Finanza.

[40]In base all'art. 3 n. 4) del regolamento IA per «*deployer*» si intende: una persona fisica o giuridica, **un'autorità pubblica**, un'agenzia o un altro organismo che utilizza un sistema di IA **sotto la propria autorità**, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

[41]L'art. 27 del regolamento IA prevede la **valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio**, secondo cui: "1.Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad **alto rischio** destinati a essere usati nel settore elencati nell'allegato III, punto 2, i ***deployer* che sono organismi di diritto pubblico** o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione **dell'impatto sui diritti fondamentali** che l'uso di tale sistema può produrre. A tal fine, i *deployer* effettuano una valutazione che comprende gli elementi seguenti: una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo".

[42] Il comma 3 dell'art. 9 del d.lgs. stabilisce: "Restano fermi i termini di conservazione dei dati personali previsti, per finalità di polizia, dall'articolo 10 del regolamento, di cui al d.P.R. 15 gennaio 2018, n. 15."

[43] L'art. 5 paragrafo 4 del regolamento IA prevede che ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto sia notificato alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati conformemente alle regole nazionali.

caso di più attivazioni del sistema di IA per l'identificazione biometrica remota in tempo reale nello stesso contesto operativo ovvero di più utilizzi omogenei del predetto sistema, la notifica può essere effettuata in modo periodico e cumulativo, secondo i termini previsti dal decreto di cui al comma 5, ferma restando la necessità del nulla osta preventivo dell'autorità giudiziaria.

Ad un successivo **DPCM**, di concerto con il Ministro della giustizia[44], sentiti il Garante e le Autorità nazionali per l'intelligenza artificiale, il comma 5 demanda l'individuazione dei requisiti necessari in relazione all'uso dei sistemi di IA per l'identificazione biometrica remota in tempo reale per le finalità di cui all'art. 8 o di cui all'art. 359-*ter* c.p.p. introdotto dall'art. 13 del decreto (v. infra).

Il DPCM dovrà prevedere elementi essenziali per la sicurezza, quali:

a) i requisiti tecnici minimi di affidabilità e accuratezza dei sistemi di IA per l'identificazione biometrica remota in tempo reale;

b) le modalità di monitoraggio periodico delle prestazioni dei sistemi, con particolare riguardo alla rilevazione e alla mitigazione di eventuali *bias* o effetti discriminatori;

c) i requisiti tecnici minimi delle banche dati di riferimento impiegate per il confronto biometrico, anche con riferimento alle relative misure di sicurezza, ai tempi e alle modalità di cancellazione dei dati e alle garanzie di non incrementalità del set di confronto per ogni singolo utilizzo autorizzato;

d) le misure tecniche e organizzative necessarie a garantire un adeguato livello di sicurezza del trattamento;

e) le misure tecniche e organizzative necessarie a impedire accessi illeciti ai dati;

f) le informazioni che il titolare del trattamento è tenuto ad allegare alla richiesta di autorizzazione ai sensi dell'articolo 8 del presente decreto o dell'articolo 359-*ter* del codice di procedura penale, introdotto dall'articolo 13 del presente decreto, in ordine alle caratteristiche tecniche del sistema, ai risultati delle verifiche di accuratezza e ai meccanismi di gestione degli errori;

g) le modalità di esecuzione della notifica di cui al comma 4;

h) gli ulteriori adempimenti cui il titolare del trattamento è tenuto in conformità a quanto previsto dal regolamento IA.

2.5. La videosorveglianza integrata con componenti di IA e il riconoscimento facciale "a posteriori" di un indiziato di reato.

Qualora il trattamento avvenga su materiale già registrato (es. telecamere a circuito chiuso analizzate ore o giorni dopo l'evento), la fattispecie trasmuta tecnicamente in un

[44] Sulla problematica mancanza di interlocuzione con il CSM nelle questioni di gestione della intelligenza artificiale anche nei procedimenti in cui sono coinvolti i magistrati si veda F. DAL CANTO-S. ROVELLI, *Il modello costituzionale di ordinamento giudiziario e la sfida della digitalizzazione della giurisdizione: il ruolo del Ministero della Giustizia e del Consiglio Superiore della Magistratura prima e dopo la legge italiana sull'intelligenza artificiale*, in *Quest. giust*., 9/12/2025.

sistema di **identificazione biometrica remota «a posteriori»** (*post-remote biometric identification*), la cui disciplina è regolata dall'art. 10 del testo.

L'art. 10 introduce un procedimento complesso, diversamente articolato, a seconda che:

1) si riferisca a una **persona oggetto di ricerca mirata** in quanto **indiziata** della commissione di un reato;

2) abbia quale finalità esclusiva, **dopo la commissione di un reato**, **l'identificazione iniziale di una persona** potenzialmente indiziata della commissione del reato sulla base di elementi oggettivi e verificabili direttamente connessi al fatto reato[45].

[45] **L'art. 10 del d.lgs.** recita: "1. In tutti i casi in cui specifiche disposizioni di legge consentono l'installazione di sistemi di videosorveglianza, tali sistemi possono essere integrati con componenti di intelligenza artificiale, nel rispetto della normativa in materia di protezione dei dati personali e del regolamento IA. Le componenti di intelligenza artificiale, destinate al riconoscimento facciale, non possono essere attivate se non nei casi, alle condizioni e con le modalità previste dai commi 2 e 3. L'attivazione è effettuata successivamente all'acquisizione delle immagini, con un intervallo di tempo tale da non configurare un'identificazione biometrica remota in tempo reale ai sensi del regolamento IA.
2. Per procedere al riconoscimento facciale a posteriori, mediante i sistemi integrati di cui al comma 1 di una persona oggetto di ricerca mirata in quanto indiziata della commissione di un reato, il pubblico ministero, su istanza degli ufficiali di polizia giudiziaria che hanno avviato i predetti sistemi, chiede al giudice per le indagini preliminari l'autorizzazione all'utilizzo dei medesimi sistemi senza ritardo e comunque entro quarantotto ore dal loro avvio. Il giudice, qualora ne ricorrano i presupposti, autorizza l'utilizzo con decreto motivato entro le successive quarantotto ore. Se non sono osservati i termini previsti dal primo periodo ovvero in caso di mancata autorizzazione, l'uso delle tecnologie di riconoscimento facciale collegato alla richiesta di autorizzazione è immediatamente interrotto e tutti i dati personali, i risultati e gli output acquisiti e prodotti sono cancellati, salvo che costituiscano corpo del reato.
3. In conformità all'articolo 26, paragrafo 10, primo comma, del regolamento IA, l'autorizzazione di cui al comma 2 non è richiesta quando le tecnologie di riconoscimento facciale di cui al comma 1 sono utilizzate esclusivamente dopo la commissione di un reato al solo fine dell'identificazione iniziale di una persona potenzialmente indiziata della commissione del reato, sulla base di elementi oggettivi e verificabili direttamente connessi al fatto di reato. Nei casi di cui al primo periodo, l'utilizzo delle tecnologie è effettuato sotto la diretta ed esclusiva responsabilità dell'ufficiale di pubblica sicurezza designato dal questore per la gestione dell'ordine e della sicurezza pubblica ovvero, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria di cui all'articolo 57, comma 1, lettere a) e b), del codice di procedura penale che procede in relazione al reato. Se non è osservato quanto previsto dal presente comma, i risultati ottenuti mediante le tecnologie di riconoscimento facciale di cui al comma 1 non possono essere utilizzati e tutti i dati personali, i risultati e gli output acquisiti o prodotti sono cancellati, salvo che costituiscano corpo del reato.
4. Sulla base dei criteri di cui al comma 12, lettera a), l'utilizzo dei sistemi di videosorveglianza previsti dal comma 1, nei casi ivi contemplati, comporta il trattamento automatizzato, delle immagini del volto delle persone che accedono a luoghi o a eventi per i quali sussistono particolari esigenze di ordine e sicurezza pubblica, senza elaborazione dei relativi dati biometrici. Le immagini sono memorizzate, a livello locale, nella base dati di riferimento di cui al comma 12, lettera b). Nella medesima base dati sono altresì memorizzati, senza ricorrere a tecnologie di riconoscimento biometrico, i corrispondenti dati anagrafici e, ove previsto un posto assegnato, il relativo identificativo, acquisiti mediante la scansione elettronica dei titoli di accesso. Successivamente alla commissione di un fatto di reato, l'attivazione delle tecnologie di riconoscimento facciale comporta l'elaborazione dei dati biometrici delle immagini presenti nella base dati locale di cui al primo periodo, cui sono associati i dati memorizzati ai sensi del secondo periodo, per l'effettuazione del confronto a posteriori con i dati biometrici estratti dalle immagini del volto della persona indiziata del reato.
5. Il titolare del trattamento dei dati personali effettuato con l'utilizzo dei sistemi integrati dalle componenti di IA e dalle tecnologie di cui al comma 1 è il Ministero dell'interno - Dipartimento della pubblica sicurezza.
6. Per i trattamenti di dati personali svolti con i sistemi integrati di cui al comma 1, il titolare del trattamento di cui al comma 5 effettua in via preventiva la valutazione d'impatto sulla protezione dei dati e consulta il Garante ai sensi degli articoli 23 e 24 del d.lgs. 18 maggio 2018, n. 51. È possibile effettuare un'unica valutazione d'impatto sulla protezione dei dati valida per tutti i sistemi analoghi.
7. I dati personali trattati con i sistemi integrati ai sensi del comma 1 sono conservati nella base di dati di riferimento individuata ai sensi del comma 12, lettera b), per sette giorni dalla raccolta e sono cancellati automaticamente decorso tale termine.
8. Gli accessi e le operazioni di trattamento sui sistemi di cui al presente articolo devono essere effettuati esclusivamente dalle persone autorizzate e registrati automaticamente in appositi file di log, non modificabili, conformemente a quanto previsto dall'articolo 12, paragrafo 3, del regolamento IA. I file di log sono conservati per cinque anni dall'accesso e dall'operazione, e resi accessibili per finalità di verifica della liceità del trattamento, di controllo interno e nell'ambito di un procedimento penale.
9. Restano fermi i termini di conservazione dei dati personali previsti, per finalità di polizia, dall'articolo 10 del regolamento di cui al d.P.R. 15 gennaio 2018, n. 15.
10. Nessuna decisione che produca effetti giuridici negativi sulla persona cui si riferiscono i dati oggetto del trattamento può essere basata unicamente sui risultati forniti dall'applicazione di riconoscimento facciale. Si osservano, altresì, le garanzie e i limiti di cui all'articolo 8 del d.lgs. n. 51 del 2018.
11. I sistemi di cui al comma 1 non possono essere in alcun caso utilizzati con l'attivazione delle tecnologie di riconoscimento facciale in modo non mirato, senza alcun collegamento con un reato o con un procedimento penale, ovvero a fini di controllo e di identificazione biometrica generalizzati o indiscriminati delle persone.

Nel primo caso, il procedimento prevede l'interlocuzione fra il **pubblico ministero** (investito, a sua volta, dagli ufficiali di polizia giudiziaria che hanno avviato i sistemi di IA) e il **giudice per le indagini preliminari** che deve autorizzare l'utilizzo.

In sostanza, se l'indagato è già noto e il sistema viene impiegato per tracciarne i movimenti passati o localizzarlo nei filmati d'archivio, scatta la riserva di giurisdizione, trattandosi di attività di indagine in senso proprio.

Nel secondo caso, considerato ricadere nelle attività di mera prevenzione, l'utilizzo è effettuato sotto la diretta ed esclusiva responsabilità **dell'ufficiale di pubblica sicurezza** designato dal questore per la gestione dell'ordine e della sicurezza pubblica ovvero, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria che procede in relazione al reato.

La previsione ricalca il disposto dell'art.26, comma 1 del regolamento IA che prevede che "nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato", il *deployer* di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori non sia tenuto a chiedere un'autorizzazione all'autorità giudiziaria quando il sistema è utilizzato per **l'identificazione iniziale di un potenziale sospetto** sulla base di fatti oggettivi e verificabili direttamente connessi al reato.

Anche in relazione a tale fattispecie va segnalata la difficoltà di distinzione fra gli ambiti di intervento a cui la disposizione di riferisce, spesso interferenti fra loro. Si segnala in particolare che, a differenza di quanto accade nel procedimento delineato all'art. 8 del decreto legislativo, nell'ipotesi sub 2), non è previsto neanche l'intervento autorizzatorio del pubblico ministero, ricadendo l'intero procedimento nella competenza delle forze di polizia.

Il mancato rispetto del procedimento e della tempistica in esso prevista comportano la cancellazione dei dati acquisiti, salvo che costituiscano corpo del reato.

Si noti che anche in tali ipotesi di riconoscimento facciale "a posteriori", nessuna decisione che produca effetti giuridici negativi sulla persona cui si riferiscono i dati oggetto del trattamento può essere basata *unicamente* sui risultati forniti dall'applicazione (ed è necessario il rispetto della normativa in materia di protezione dei dati personali).

---

12. Con decreto del Ministro dell'interno, sentito il Garante, sono indicati:
a) i criteri per l'individuazione dei luoghi e degli eventi di cui al comma 4;
b) le modalità del trattamento automatizzato delle immagini del volto, senza elaborazione dei dati biometrici, delle persone che accedono ai luoghi o agli eventi di cui al comma 4, e della loro memorizzazione a livello locale, ai sensi del primo e del secondo periodo del comma anzidetto, in una base dati di riferimento, per l'elaborazione e il confronto, esclusivamente a posteriori rispetto alla commissione di un fatto di reato, dei dati biometrici;
c) le misure tecniche e organizzative necessarie a garantire un adeguato livello di sicurezza del trattamento;
d) gli adempimenti cui il titolare del trattamento è tenuto in conformità a quanto previsto dal regolamento IA.
13. All'installazione e alla manutenzione delle componenti di IA e delle tecnologie biometriche di cui al comma 1 possono provvedere, senza nuovi o maggiori oneri per la finanza pubblica, i gestori dei luoghi di cui al comma 4, gli organizzatori o promotori degli eventi di cui al medesimo comma, ovvero chi ha la disponibilità delle strutture ove tali eventi si svolgono, in accordo con i proprietari degli stessi luoghi o strutture, con particolare riferimento agli enti locali per le rispettive piattaforme di videosorveglianza, nonché, fermo quanto previsto al comma 5, in relazione ai ruoli svolti nel trattamento dei dati personali, nel rispetto del d.lgs. n. 51 del 2018. Nelle ipotesi di cui al primo periodo, i predetti sistemi sono concessi in comodato gratuito alla questura, che ne acquisisce la completa ed esclusiva disponibilità.
14. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri per la finanza pubblica".

Le immagini raccolte nei luoghi o eventi pubblici sono memorizzate localmente senza elaborazione biometrica e vengono cancellate automaticamente se non sono di utilità per lo scopo investigativo previsto.

Il confronto biometrico è dunque possibile solo *ex post* e limitatamente alle immagini della persona indiziata, nel rispetto del divieto assoluto di sorveglianza generalizzata e dell'obbligo di registrare ogni operazione in *log* non modificabili conservati per cinque anni.

La disciplina mira a impedire la creazione di banche dati cumulative, vietando l'alimentazione incrementale e l'uso di *dataset* ottenuti tramite *scraping* non mirato, e garantisce che gli *output* illegittimamente acquisiti siano inutilizzabili.

L'acquisizione dei dati con tale tecnica di riconoscimento "a posteriori" è stata oggetto di attenzione da parte del Garante per la protezione dei dati personali[46] che aveva segnalato criticità relative ad una raccolta automatica e indiscriminata di dati biometrici.

Nel parere è stato evidenziato il rischio di profilazione massiva di tutti i presenti in contesti eterogenei e affollati come stadi, concerti, stazioni e grandi eventi, dovendosi richiamare sul punto le garanzie antidiscriminatorie previste dall'art. 8 del d.lgs. n. 51/2018.

La circostanza che sia stata demandata al Ministro dell'Interno (comma 12), l'adozione di un decreto che regola aspetti decisivi dell'utilizzo, tra cui i criteri per l'individuazione dei luoghi e degli eventi connotati da esigenze di ordine e sicurezza pubblica, le modalità del primo trattamento automatizzato e della memorizzazione delle immagini dei volti di quanti accedono ai luoghi o partecipano agli eventi, nonché le misure di sicurezza e gli adempimenti dovuti dei titolari del trattamento, è sembrata, in sede di primo commento, un'opzione discutibile nella misura in cui affida ad un atto amministrativo profili particolarmente rilevanti per il complessivo equilibrio della disciplina[47].

Va altresì evidenziato che, in base al considerando 39 del regolamento IA, qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica, diverso da quello connesso all'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto disciplinato dal regolamento, dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 10 della direttiva (UE) 2016/680[48], ossia il criterio di *stretta necessità* laddove possa involgere aspetti sensibili della persona.

[46] Con il parere del 14 luglio 2026, reso pubblico il 29 luglio, il Garante per la protezione dei dati personali ha dato il via libera – con condizioni – "ai Titoli I e III dello schema di decreto legislativo (Atto del Governo n. 418) che adegua l'ordinamento italiano all'AI Act".

[47] N. ROSSI, *L'intelligenza artificiale*, *cit*.

[48] L'art. 10 della Direttiva (UE) 2016/680 disciplina il trattamento di categorie particolari di dati personali, disponendo: "Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato".

3. Disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiali.

3.1. Definizioni utilizzate dal testo.

All'evidente fine di armonizzare le pratiche di utilizzo dei sistemi di intelligenza artificiale nello spazio europeo e di non creare o – quanto meno – limitare il rischio di equivoci interpretativi in una materia nuova ed estremamente tecnica, l'**art. 11** del d.lgs. in commento richiama per intero l'apparato definitorio dell'art. 3 del regolamento IA con riferimento a tutte le disposizioni del titolo II relativo alle disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale, nonché alle disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi.

L'unico comma dell'articolo 11 stabilisce che si applicano le definizioni di cui all'**art. 3** del regolamento IA.

Secondo quanto si legge nella *Relazione illustrativa*, la scelta del rinvio dinamico è volta a evitare duplicazioni definitorie e ad assicurare la piena uniformità terminologica con il quadro eurounitario, in coerenza con le indicazioni del § 3 della circolare della Presidenza del Consiglio dei ministri 2 maggio 2001 (recante *«Guida alla redazione dei testi normativi»*), in tema di rapporti fra atti normativi.

Rinviando, dunque, all'art. 3 del regolamento IA per l'elenco dettagliato delle definizioni, si evidenzia che, ai fini delle materie disciplinate nel titolo II, ossia delle disposizioni penali e di quelle sulla responsabilità civile, assumono particolare rilievo le seguenti in esso contenute:

«**sistema di IA**» (articolo 3, punto 1): 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;

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

«***deployer***» (articolo 3, punto 4): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;

«**importatore**» (articolo 3, punto 6): una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona stabilita in un paese terzo;

«**distributore**» (articolo 3, punto 7): una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione;

«**operatore**» (articolo 3, punto 8): un fornitore, un fabbricante del prodotto, un *deployer*, un rappresentante autorizzato, un importatore o un distributore.

Con riguardo alle disposizioni processuali penali, e in particolare all'articolo 359-*ter* del codice di procedura penale (introdotto dall'articolo 13), rilevano le definizioni di:

«**dati biometrici**» (articolo 3, punto 34): i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici;

«**identificazione biometrica**» (articolo 3, punto 35): il riconoscimento automatizzato di caratteristiche umane di tipo fisico, fisiologico, comportamentale o psicologico, allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di persone memorizzati in una banca dati;

«**categorie particolari di dati personali**» (articolo 3, punto 37): le categorie di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725;

«**dati operativi sensibili**» (articolo 3, punto 38): dati operativi relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali;

«**sistema di identificazione biometrica remota**» (articolo 3, punto 41): un sistema di IA finalizzato a identificare persone fisiche, senza il loro coinvolgimento attivo e in genere a distanza, mediante il confronto dei loro dati biometrici con quelli contenuti in una banca dati di riferimento;

«**sistema di identificazione biometrica remota "in tempo reale"**» (articolo 3, punto 42): un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, comprendendo non solo l'identificazione istantanea ma anche quella con ritardi limitati, così da evitare l'elusione delle norme;

«**modello di IA per finalità generali**» (articolo 3, punto 63): un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato.

3.2. Modifiche al c.p.

L'unica norma di rilievo penale (sostanziale) contenuta nel decreto è quella prevista dall'**art. 12**, che introduce, all'**art. 437-*bis* c.p.**, il reato di "**Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi**".

Va ricordato, peraltro, che già la legge IA ha introdotto autonomamente due fattispecie di reato[49].

La prima, di cui al nuovo **art. 612-*quater* c.p.**, rubricato "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale", punisce 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. Il delitto è punibile a querela della persona offesa, con talune eccezioni di procedibilità *ex* officio[50].

La seconda ha incrementato la normativa penale della disciplina del **diritto d'autore**, aggiungendo la **lett. a-*ter* all'art. 171, comma 1, l. 22 aprile 1941, n. 633,** che punisce la riproduzione senza diritto di materiali disponibili in rete, inclusi quelli effettuati o mediati attraverso sistemi di intelligenza artificiale[51].

È stata aggiunta, inoltre, (art. 26, comma 1, lett. a) **nell'art. 61 c.p.** la nuova **aggravante comune** di cui al n. **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", nonché alcune aggravanti specifiche per il delitto di cui all'art. **294 c.p.** (attentati contro i diritti politici del cittadino), per l'art. **2637 cod. civ**. (aggiotaggio) e per l'**art. 185**, d.lgs. 24 febbraio 1998, n. 58 (manipolazione del mercato) [52].

La legge IA (**art. 24 comma 3**), aveva delegato altresì il Governo ad adottare uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale, secondo specifici princìpi e criteri direttivi contemplanti l'introduzione di autonome fattispecie di reato (comma 5 lett. b), punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'omesso adeguamento di misure di

---

[49] Per un primo commento B. FRAGASSO, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, in *Sist. pen*., 2025, fasc. 10, p.157.

[50] L'art. **612-*quater* c.p.**, rubricato "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale, è stato introdotto nel codice penale dall'art. 26, comma 1, lett. c della "legge IA", e punisce "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".

[51] **L'art. 171** cit. dispone: "Salvo quanto previsto dall'art. 171-*bis* e dall'articolo 171-*ter* è punito con la multa da L. 500 a L. 20.000 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: (omissis); 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. Si veda N.M. TRITTO, *Novità normative in materia di intelligenza artificiale e diritto penale*, in *Riv. pen*., 2025, 10, p. 825.; L. SCOLLO, *L'intelligenza artificiale entra nel codice penale*, in *Dir. pen. proc*., 2025, 6, p. 693.; G. BARONE, *La regolamentazione italiana dell'intelligenza artificiale: dove eravamo rimasti?*, in *Dir. pen. proc.,* 2025, 6, in particolare pagg. 709 ss..

[52] Vedi L. PICOTTI, *I contenuti penali della legge sull'intelligenza artificiale*, in *Sist. pen*., 2/12/2025.

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[53].

Il Governo ha dato attuazione alla delega con l'art. 12 del d.lgs., che introduce nel codice penale l'**art. 437-*bis* cod. pen**[54].

Dal punto di vista sistematico, la disposizione si colloca tra i delitti di comune pericolo mediante violenza, di cui al capo I del titolo VI (dei **delitti contro l'incolumità pubblica**) del codice, che hanno la caratteristica di esporre a pericolo la vita e l'integrità fisica di un numero indeterminato di persone, pregiudicando in tal modo la sicurezza sociale.

Come si vedrà nel paragrafo successivo, la configurazione del reato si distingue propriamente da tale scelta in senso stretto, atteso che – in conformità con la delega - le due condotte previste ai commi 1 e 2 si realizzano *anche* solo con la messa in pericolo della vita e dell'incolumità individuali.

Ciò non toglie che, in armonia con la collocazione nel codice, sembra prevalere negli interessi protetti dalla nuova fattispecie incriminatrice un aspetto di pericolo diffuso, la possibilità di una potenza espansiva del rischio fatale e una indeterminatezza della potenziale vittima, elementi che distinguono il nuovo delitto rispetto ai delitti contro la persona, pur proteggendo anche interessi individuali che vengono posti in pericolo dai singoli fatti illeciti.

D'altra parte, la dottrina tradizionale e parte della giurisprudenza, anche con riferimento agli altri delitti contro l'incolumità pubblica, all'interno dei quali l'art. 437-*bis* c.p. è stato inserito, ne ha ampiamente sottolineato la caratteristica di reati plurioffensivi che hanno quale oggetto giuridico, da un lato, l'interesse generale all'incolumità pubblica, dall'altro, gli interessi particolari che sono lesi o posti in pericolo dalle varie azioni criminose[55].

Ugualmente, così come altri delitti previsti nello stesso capo (come, ad es., gli artt. 435 e 437 c.p.), non si addice al reato introdotto la caratteristica della commissione tramite "violenza" tenuto conto, per di più, che il primo comma, tratteggia una condotta di tipo omissivo[56].

L'inserimento dopo il reato di cui all'art. 437 c.p. si giustifica per l'adozione di un modello strutturale ad esso omogeneo, quanto meno nella configurazione del comma 1, ideato come delitto di comune pericolo mediante omissione di cautele.

---

[53] Evidenzia una "direttrice espansiva" nell'art. 24, comma 5, della legge IA, volta cioè ad estendere l'area del penalmente rilevante "che attesta che il legislatore è ben consapevole che le fattispecie che puniscono eventi di danno potrebbero risultare inadeguate a sanzionare la condotta dei produttori e degli utilizzatori professionali dei sistemi di I.A. e che, di conseguenza, potrebbe essere necessaria l'introduzione di reati che anticipino la tutela penale allo stadio della creazione del pericolo", B. FRAGASSO*, Diritto penale e rischio da intelligenza artificiale: brevi note sulle deleghe contenute nella legge 132/2025*, in *Riv. it. dir. proc. pen*., 2026, 1, p. 307.

[54] Per una prima lettura si veda B. FRAGASSO, *Disposizioni attuative in materia di intelligenza artificiale: il reato di omessa adozione di misure di sicurezza nei sistemi di I.A. e altre novità in materia di autorità di vigilanza, identificazione biometrica, responsabilità da reato degli enti e responsabilità civile*, in *Sist. pen*., 12/06/2026.

[55] Per il reato di cui all'art. 437 c.p. "*ciò implica che il referente di valore non possa ritenersi circoscritto alla difesa dell'incolumità pubblica": esso si estende, infatti, anche alla salvaguardia dell'incolumità del singolo lavoratore avverso il rischio di infortuni sul lavoro*", così A. GARGANI, *Reati contro l'incolumità pubblica*, in *Trattato di diritto penale* diretto da C.F. GROSSO-T. PADOVANI- A. PAGLIARO, Giuffrè, 2008, p. 533. V. anche F. ANTOLISEI, *Manuale di diritto penale, Parte speciale*, II, Giuffrè, 2022, p. 7. In giurisprudenza nel senso indicato: Sez. 4, 24/11/2017, n. 57673, Rv. 271693-01; Sez. 1, 21/02/2007, n. 12464, Rv. 236431-01 (anche se, difformi, Sez. 1, 20/01/2016, n. 18168, Rv. 266881-01 e Sez. 4, 25/11/20, n. 7939, Rv. 280928-01).

[56] V. F. ANTOLISEI, *Manuale*, cit., p. 8

La collocazione sistematica indica in maniera chiara come il legislatore configuri la produzione, gestione e di utilizzo professionale dell'intelligenza artificiale come un'attività con un potenziale minaccioso per l'incolumità degli individui, in relazione alla quale è necessario evitare un completo affidamento alla tecnica, dovendo restare la stessa sotto il controllo vigile dell'uomo, nella visione antropocentrica che permea la normativa di cui al regolamento IA.

Il reato è previsto solo per i sistemi di intelligenza artificiale "**ad alto rischio".**

In tale quadro **le organizzazioni** sono destinate ad assumere un ruolo da protagonista.

Di tale centralità è espressione l'inserimento dell' art. 437-*bis* c.p. - accanto al già citato art. 612-*quater* c.p. - nell'**elenco dei reati presupposto della responsabilità da reato degli enti** (v., di seguito al paragrafo 3.6.).

Tale scelta riflette la consapevolezza di come siano, in concreto, proprio le organizzazioni a governare la prevenzione e la gestione dei rischi da intelligenza artificiale[57].

3.3. Art. 437-*bis* c.p. (Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi).

Il nuovo delitto di cui all'**art. 437-*bis***, introdotto nel c.p. dall'articolo 12 del d.lgs., è rubricato "***Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi***" e dispone:

"Chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana è punito con la reclusione da uno a cinque anni, quando da tali omissioni derivi pericolo per la vita o l'incolumità pubblica o individuale. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da due a otto anni.

Salvo che il fatto costituisca più grave reato, chiunque, al di fuori dei casi indicati al primo comma, altera sistemi di intelligenza artificiale ad alto rischio è punito, qualora dal fatto derivi un pericolo per la vita o l'incolumità pubblica o individuale, con la reclusione da due a sei anni. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da tre a dieci anni.

Se taluno dei fatti previsti dal comma primo è commesso per colpa grave, la pena è ridotta da un terzo a un sesto.

L'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio che omette intenzionalmente di adottare misure di sorveglianza umana è punito con le pene previste dal primo comma, primo e secondo periodo, qualora da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure un pericolo per la sicurezza dello Stato".

[57] Così B. FRAGASSO, *Art. 437- bis c.p.: il nuovo reato di pericolo concreto in materia di i*.a., in *Altalex*, 23/09/2026.

All'interno della norma, che ha una struttura complessa, si rinvengono quattro differenti fattispecie che hanno come oggetto i sistemi di IA ad alto rischio:
- la prima (comma 1), in forma omissiva, punisce la mancata predisposizione delle misure di sicurezza nella fase di progettazione, addestramento, produzione e immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio;
- la seconda (comma 2), in forma commissiva, sanziona l'alterazione illecita dei medesimi sistemi;
- la terza contempla la stessa condotta delineata nel primo comma, nella previsione colposa "grave" (comma 3);
- la quarta è una fattispecie omissiva propria dell'utilizzatore professionale che sanziona il mancato obbligo di adottare misure di sorveglianza umana (comma 4).

3.3.1. Il delitto di omessa adozione di misure di sicurezza.

Riprendendo il criterio di delega stabilito dalla legge IA all'art. 24, comma 5, lett. b), il delitto di omessa adozione di misure di sicurezza di cui al comma 1 si configura come un'ipotesi di **reato omissivo proprio**[58].

Soggetto attivo del reato può essere "**chiunque**". La norma costruisce il delitto opportunamente come un reato comune (per evitare il rischio di smagliature nel sistema delle responsabilità), anche se finisce necessariamente per individuare la figura dell'agente in un soggetto che abbia avuto un ruolo individuabile nella catena di produzione e messa sul mercato del sistema di intelligenza artificiale.

Verosimilmente, dunque, il "chiunque" utilizzato dal legislatore deve essere modellato sulla funzione che l'agente svolge, dal momento che colui il quale *progetta, addestra, produce o immette sul mercato* un sistema di intelligenza artificiale assume per lo più carattere professionale, specie trattandosi di sistemi di intelligenza artificiale esclusivamente "ad alto rischio".

Stante la configurazione del reato come omissivo occorre, inoltre, che il soggetto che (*non*) interviene nella catena produttiva-circolatoria del sistema di intelligenza artificiale ad alto rischio, abbia mancato ad un dovere giuridico di fare allo stesso imposto, ossia si possa configurare una sua specifica **posizione di garanzia** rispetto alle fasi di interesse descritte dal legislatore[59].

La fattispecie pone dunque la necessità di individuare le fonti normative dell'obbligo giuridico violato dal soggetto attivo del reato, di natura extrapenale e permeate dalle conoscenze tecniche più recenti, secondo un criterio evolutivo permanente, "*dalle quali desumere le informazioni su quali soggetti, quali obblighi, quali eventi rilevano nel fondare una posizione di garanzia penalmente rilevante*" [60].

---

[58] F. MANTOVANI-G. FLORA, *Diritto penale*, Cedam, 2025, p. 113 ss..
[59] Vedi sulle posizioni di garanzia ricavabili dal regolamento IA, L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi?*, in *Sist. pen*., 31/07/2024, p. 15; S. DE FLAMMINEIS, *Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del D.L.L. 1146/2024*, in *Sist. pen*., 2024, fasc. 9, p. 12 ss..
[60] Così M. DONINI, *Diritto penale, Parte generale*, Giuffrè, 2026, p. 785 e p. 807.

Le posizioni di garanzia vanno individuate fra coloro cui è deputato il controllo delle fonti di pericolo, in relazione alle attività consentite nei sistemi definiti di per sé "ad alto rischio".

Il ruolo dell'agente dovrà dunque essere ricercato, non solo nel soggetto a capo dell'eventuale società/impresa/organismo che direttamente agisca, ma anche in quel soggetto - "chiunque" - che ricopra un ruolo decisivo (eventualmente delegato), all'interno del sistema organizzativo formale e sostanziale del soggetto che agisce nelle fasi individuate dal legislatore (che spesso, considerati i costi legati ai sistemi di intelligenza artificiale, assumerà le apparenze di una struttura complessa)[61].

La formulazione del legislatore appare genericamente descrittiva nella elencazione della tipologia di attività in cui si deve inserire la condotta del soggetto attivo del delitto, dovendosi ritenere compresi, al suo interno, tutte quelle accezioni di "operatore" proprie dell'apparato definitorio del regolamento IA che il decreto, all'art. 11, ha inteso integralmente recepire: **fornitore**, ***deployer*, importatore** e **distributore,** soggetti che possono dirsi *tutti* rientrare nel circuito di chi "immette sul mercato" un sistema di intelligenza artificiale.

Anche nella *Relazione illustrativa*, viene precisato che la condotta è imputata a chi opera in una delle fasi del ciclo di vita rilevanti (progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale) e che l'elenco è funzionale a coprire tutte le posizioni di garanzia individuate dal regolamento IA.

A stretto rigore, "l'immissione sul mercato" secondo la definizione dell'art. 3 n. 9) del regolamento IA, riguarderebbe invece solo "la prima messa a disposizione" di un sistema di intelligenza artificiale sul mercato dell'Unione, il che rende poco coerente la terminologia utilizzata nell'art. 437-*bis* c.p., introdotto dall'art. 12 del d.lgs. con l'espresso richiamo alla tassonomia del regolamento effettuata dal precedente art. 11.

La condotta di inerzia può concretizzarsi:

- nel mancato inserimento di quei presidi tecnici di sicurezza che, ritenuti idonei a evitare difetti di funzionamento, devono accompagnare il sistema di IA ad alto rischio lungo tutto il suo ciclo di vita (partendo dalle fasi iniziali di progettazione, produzione e addestramento, fino all'immissione sul mercato).
- nella mancata applicazione di misure di sorveglianza umana.

Pur muovendosi secondo una logica precauzionale, coerente con l'approccio al rischio del regolamento IA, l'orientamento del legislatore delegato viene temperato dalla necessità che i beni giuridici protetti corrano un pericolo affinché il delitto si realizzi.

In linea con le elaborazioni ormai consolidate sul principio di offensività e del suo fondamento costituzionale[62], il **pericolo** è "**concreto**": per la sua sussistenza, dunque, la

[61] Sulle posizioni di garanzia e sulla colpa di organizzazione e responsabilità punitiva delle persone giuridiche si veda L. PICOTTI., *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. proc.,* 2024, 3, p. 299. Si veda anche B. FRAGASSO*, Intelligenza artificiale e crisi del diritto penale d'evento: profili di responsabilità penale del produttore di sistemi di i.a*., in *Riv. it. dir. proc. pen.,* 2024, 1, p. 287 ss. che individua "l'elefante nella stanza" nella discrasia tra carattere intrinsecamente plurisoggettivo della criminalità d'impresa e conformazione personalistica della responsabilità penale.

[62] V. F. MANTOVANI-G. FLORA, *Diritto penale*, Cedam, 2025, p. 168 ss..

minaccia per l'incolumità deve effettivamente esistere, ossia dovrà formare oggetto di specifica prova nell'eventuale giudizio volto all'accertamento della sussistenza del reato[63].

La concreta minaccia al bene giuridico protetto dalla norma andrà ricostruita alla luce delle conoscenze della tecnica, tenendo presente che il legislatore non fa riferimento a specifiche "misure di sicurezza" destinate alla prevenzione del pericolo concreto paventato, bensì ha riguardo a misure di sicurezza generiche ma *strutturalmente funzionali* alla prevenzione di "malfunzionamenti" o "alterazioni".

Ai fini della realizzazione del delitto, non occorre che si verifichi alcun evento lesivo, essendo sufficiente che si ponga in essere la condotta omissiva.

Tuttavia, l'omissione sarà penalmente rilevante solo se i *malfunzionamenti* o le *alterazioni* al sistema siano potenzialmente tali da dare concretezza al rischio per l'incolumità. La **messa in pericolo** del bene giuridico protetto, che è **elemento costitutivo** della fattispecie, dovrà dunque formare oggetto di specifico e puntuale accertamento[64].

Come si è detto, l'oggetto della tutela penale sono solo i sistemi di intelligenza artificiale "**ad alto rischio**" (per tale nozione v. paragrafo 2.2.).

Per quanto riguarda l'elemento soggettivo del reato, il **dolo** richiesto è generico e consiste nella volontà cosciente e libera di violare il proprio obbligo giuridico omettendo di adottare le misure di sicurezza.

Oltre alla volontà del fatto, sembra necessaria anche la coscienza che le misure di sicurezza non predisposte siano destinate alla prevenzione di possibili malfunzionamenti o alterazioni del funzionamento dei sistemi.

La fattispecie individua, infatti, la condotta omissiva non in astratto (mancata adozione di misure di sicurezza *tout court*), ma correla la violazione di un obbligo giuridico come direttamente funzionale alla prevenzione dei danneggiamenti *pericolosi.*

Incertezze possono permanere, invece, sulla questione se il dolo debba abbracciare anche il pericolo per l'incolumità.

La dottrina e la giurisprudenza prevalenti, con riferimento alle fattispecie di reato costruite in maniera analoga, sono per la soluzione affermativa[65].

---

[63] V. F. ANTOLISEI, *Manuale*, u. cit., p. 7; G. FIANDACA–E. MUSCO, *Diritto penale, Parte speciale*, I, Zanichelli, 2025, p. 538 il quale evidenzia, per tali tipi di reati, la completa delega all'organo giudicante della individuazione della condotta pericolosa incriminata, criticabile anche sotto il profilo del principio di tassatività della norma incriminatrice.

[64] Nel parere che la Commissione dell'ANM "Innovazione Tecnologica e Organizzativa, Transizione Digitale, Informatica e Intelligenza Artificiale" ha reso *su Atto del Governo n. 418 (Schema decreto legislativo recante "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024,* (il cui contenuto è raggiungibile al link https://lamagistratura.it/attualita/il-parere-della-commissione-innovazione-sul-decreto-ia-del-governo/), si pone l'accento sulla difficoltà potenziale di un tale accertamento: "*L'introduzione di tale disposizione va positivamente valutata, nella parte in cui estende l'intervento penale ad omissioni inerenti misure tecniche di sicurezza relative ad un sistema IA classificato come ad alto rischio. Il potenziale assai esteso ambito di operatività della previsione, per come sopra delineato, è contemperato proprio dalla previsione, quale elemento costitutivo della fattispecie, della necessità circa la verificazione di un pericolo concreto, tenuto conto della natura dei beni tutelati, quali vita, l'incolumità individuale o la sicurezza dello Stato. Pur tuttavia, può ipotizzarsi che la fattispecie, per come prevista, porterà a difficoltà di accertamento, in considerazione del nesso richiesto, ma sostanzialmente indeterminato, tra le omissioni tipizzate id il pericolo concreto dei beni oggetto di tutela*".

[65] Si veda, Sez. 1, 1/01/2008, n. 17214, Rv. 240002-01; Sez. 1, 20/11/1996, n. 11161, Rv. 206428-01; Sez. 2, 1/09/1994, n. 11699, Rv. 199760-01.

Secondo tale impostazione, nel fuoco del dolo deve rientrare dunque, quanto meno, anche la **previsione del pericolo** ricollegabile alla omissione, senza che tale evento di pericolo debba essere tuttavia specificamente perseguito in funzione dell'obiettivo di incidere effettivamente sulla incolumità individuale o pubblica, determinandosi altrimenti una configurazione criminosa più grave (per quanto il legislatore, contrariamente a quanto previsto per l'ipotesi commissiva, non ne faccia espressa riserva), essendo sufficiente solo la consapevolezza del rischio potenziale[66].

La pericolosità deve essere investita dal dolo poiché non è condizione obiettiva di punibilità ma elemento costitutivo della fattispecie[67].

Ove l'omissione abbia riguardato la predisposizione delle **misure di sorveglianza umana**, il dolo copre la coscienza e volontà della mancata adozione e la consapevolezza del pericolo per l'incolumità.

Anche sotto il profilo dell'accertamento, il delitto omissivo che si configura come omissione delle misure di sorveglianza umana appare più agevole dal momento che la mancata previsione di tali misure comporta in sé, ove ne consegua il pericolo, l'integrazione del reato.

Può dunque affermarsi che tale specifica omissione, legata alla mancata previsione di un intervento dell'uomo nel sistema, determini a priori il rischio più rilevante ravvisato dal legislatore, nell'ottica antropocentrica che connota l'intero regolamento IA.

La configurabilità o meno del **tentativo**, va ricostruita in relazione all'elaborazione dell'applicazione dell'istituto nei reati omissivi propri, tradizionalmente esclusa[68], ma oggetto di un mutamento di prospettiva, ormai neanche tanto recente, che collega la configurabilità del tentativo al termine per l'adempimento, ritenendo che, ove il termine per adempiere non sia decorso, ci si troverà di fronte ad un'ipotesi di tentativo tutte le volte che un soggetto obbligato precostituisca una situazione tale da rendere impossibile l'ottemperanza alla pretesa normativa, di modo che "*i requisiti dell'idoneità e dell'univocità previsti dall'art. 56 risulteranno in linea di massima meglio apprezzabili a misura che gli atti del reo si avvicinano alla soglia dell'impossibilità di adempiere*"[69].

Le pene edittali variano in base alla natura del pericolo generato dall'omissione:

- la reclusione **da 1 a 5 anni** qualora sia minacciata la vita o l'incolumità individuale o pubblica;
- la reclusione **da 2 a 8 anni** nel caso in cui il pericolo riguardi la sicurezza dello Stato.

L'aggravamento di pena previsto nel caso in cui il fatto metta in pericolo la sicurezza dello Stato dà luogo ad **aggravante**[70], dunque suscettibile di essere posta in bilanciamento con eventuali attenuanti.

---

[66] V., per il reato di cui all'art. 437 c.p., P. CIPOLLA, *I delitti contro l'incolumità pubblica*, in G. LATTANZI-E. LUPO, *Rassegna di giurisprudenza e dottrina al codice penale*, Giuffrè, 2016, p. 835; F. ANTOLISEI, u. cit. p. 42 G. FIANDACA–E. MUSCO, *Diritto penale*, u. cit., 564.
[67] R. NITTI, *I delitti contro l'incolumità pubblica*, cit., p. 882.
[68] V. Sez. 2, 6/02/2007, n. 9551, Rv. 235834-01; Sez. 6, 3/12/1999, n. 705, Rv. 215321-01.
[69] Così G. FIANDACA – E. MUSCO, *Diritto penale (parte generale*), Zanichelli, 2025, pagg. 669
[70] Vedi Sez. 4, 13/05/2016, n. 52511, Rv. 269571-01 per il delitto di cui all'art. 437 c.p. nella previsione aggravata, in tal caso, dalla verificazione dell'evento.

3.3.2. Il delitto omissivo colposo.

In base a quanto disposto dal **terzo comma**, il delitto è punibile anche in caso di **colpa grave**: per tale fattispecie è prevista una **riduzione della pena, compresa tra un terzo e un sesto** a seconda della distinzione del bene giuridico posto in pericolo.

La *Relazione illustrativa* chiarisce che la scelta di limitare la punibilità colposa alla sola "colpa grave" risponde a un principio di proporzionalità.

Si è voluto cioè circoscrivere la sanzione penale alle sole macroscopiche violazioni dei doveri di diligenza, evitando di criminalizzare qualsiasi difformità dagli standard tecnici in un settore che evolve rapidamente e in cui coesistono regole tecniche nazionali, europee e internazionali[71].

Si legge una sorta di implicita consapevolezza della scivolosità del terreno in cui opera la responsabilità penale nel campo in esame che, per il vero, non sembra mancare anche a fronte della ipotesi dolosa de comma 1, laddove, pur adottando il soggetto misure di sicurezza, queste si dovessero rivelare non adeguate in concreto – ad esempio perché non aggiornate– ad evitare il pericolo paventato dal legislatore.

Le fattispecie di cui al primo e al terzo comma sono entrambe di natura preventivo-cautelare, prescindendo dalla verifica di eventi lesivi.

Sul piano applicativo, si preannunciano quindi non poche difficoltà per la distinzione in concreto della fattispecie dolosa da quella colposa "grave", tenuto presente che il dolo richiesto per il delitto di cui al primo comma potrebbe assumere anche la forma di **dolo indiretto** o **eventuale** e che entrambe le condotte attengono alla mancata predisposizione di misure precauzionali[72].

In tale ultimo elemento, ossia l'individuazione delle *misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi* va individuato un ulteriore aspetto di difficoltà applicativa della fattispecie, sia dolosa che colposa.

L'evoluzione della tecnica e della regolamentazione adeguata a tale rango renderà certamente non impossibile ricavare un corpo di interventi di tipo protocollare, tali da costituire un riferimento per la valutazione in concreto di tali misure e della loro idoneità alla prevenzione.

Allo stato, il panorama appare tuttavia incerto, specie tenuto conto dei molteplici settori di intervento che sono contemplati nei sistemi ad "alto rischio" e soprattutto *in fieri* (con

[71] V. G. CIVELLO, *Il nuovo articolo 437-bis, co. 3, c.p.: verso la depenalizzazione della colpa lieve?,* in *Sist. pen.,* 5/11/2026 il quale, muovendo dalla scelta del legislatore di prevedere la sola colpa "grave" per il reato in esame riflette sulle ragioni di una tendenza ad espungere dall'area penale le ipotesi di colpa – oggettivamente e/o soggettivamente – lieve.

[72] Si vedano le problematiche emerse per le fattispecie assimilabili di cui all'art. 437 c.p. e 451 c.p. in A. GARGANI, *Reati contro l'incolumità pubblica*, in *Trattato di diritto penale, cit.* p. 538. Anche M. DONINI, *Diritto penale*, cit., p. 794: "*Le cose si complicano quando l'obbligo di agire ha una funzione essa stessa preventivo-cautelare, e pertanto interferisce con le cautele che servono a identificare la colpa, quella forma di colpa che si definisce colpa specifica, o per inosservanza di leggi, regolamenti, ordini o discipline, di fonti scritte in particolare*."

modalità progressiva e incessante), determinando problemi di determinatezza della fattispecie.

Non vi è dubbio che il campo di elezione della fattispecie colposa è quella della corretta applicazione delle misure che assicurino la conformità ai requisiti che sono previsti per i sistemi ad alto rischio dal regolamento IA (artt. 8 ss.) consacrati nella documentazione a corredo.

Sia per la collocazione sistematica all'interno del codice penale, sia per l'assonanza delle previsioni tecniche previste per i sistemi, riecheggiano in tali disposizioni le elaborazioni culturali e giuridiche proprie della normativa in materia di sicurezza sul lavoro.

Il delitto appare assimilabile, sotto il profilo della struttura della condotta nella forma omissiva al delitto di cui all'art. 437 cod. pen"[73].

Rispetto al sistema tratteggiato dal d.lgs. 9 aprile 2008, n. 81, nella formulazione attualmente vigente, maggiori incertezze si ravvisano nella individuazione della catena delle responsabilità connesse alle azioni contemplate dal legislatore che le individua nella *progettazione, addestramento, produzione e immissione sul mercato.*

Resta da verificare inoltre se, accanto al campo di elezione della colpa *grave* specifica, rimangano margini per condotte colpose generiche per omissione.

Il paradigma classico della responsabilità giuridica, fondato sui presupposti del controllo e della prevedibilità della condotta, appare presentare una strutturale inadeguatezza di fronte ai sistemi di intelligenza artificiale, pur a fronte degli specifici obblighi di prevenzione sanciti dalle fonti europee e interne.

L'assenza di un controllo assoluto e di una totale prevedibilità *ex ante* sulle evoluzioni del sistema, unitamente al difetto di trasparenza dei suoi processi cognitivi (la cosiddetta *black box*), potrebbe scardinare il tradizionale nesso di imputazione. Diventa infatti estremamente complesso distinguere se l'evento lesivo sia l'effetto di un vizio nativo dell'algoritmo, di un deficit nella fase di *training*, di un'erronea interazione da parte dell'utilizzatore o, infine, di variabili esogene e imprevedibili.

L'IA potrebbe instaurare una condizione di indeterminatezza sistemica di difficile governo attraverso un semplice inasprimento dei precetti normativi o un'iper-regolamentazione.

Un apparato di regole, per quanto dettagliato e pervasivo, difficilmente può essere in grado di mappare e anticipare l'intera gamma di rischi scaturenti dalla mutua interazione tra i modelli algoritmici, l'elemento umano e l'eterogeneità dei contesti operativi.

Anche per tale ipotesi colposa la finalità tipica delle misure tecniche deve essere incentrata nella loro strumentalità rispetto alla prevenzione di malfunzionamenti o alterazioni, dunque con profili di ricostruzione causale prettamente tecnici.

---

[73] Sez. 4, 14/11/2017, n. 16715, Rv. 273098-01; anche Sez. 4, 4/02/2020, n. 7564, Rv. 278580-01 secondo cui: "*Il reato di cui all'art. 437, primo comma, c.p., ove la condotta consista nell'omissione di cautele contro infortuni sul lavoro, ha natura permanente sicché, nel caso in cui l'imputazione indichi il "tempus commissi delicti" con l'indicazione della data della cessazione della condotta illecita, il termine di prescrizione decorre da tale data, e non da quella di emissione della sentenza di primo grado, ferma la necessità di verificare se la permanenza sia cessata in epoca anteriore perché il dispositivo omesso sia stato collocato o non più utilmente collocabile ovvero, trattandosi di reato proprio, perché sia stata dismessa la posizione di garanzia*".

3.3.3. Il delitto di alterazione illecita dei sistemi.

Il secondo comma dell'art. 437-*bis* c.p. disciplina il **reato di alterazione illecita dei sistemi**. Questa norma mira a colpire chiunque modifichi un sistema di IA ad alto rischio senza essere coinvolto nelle attività descritte dal primo comma (addestramento, produzione, progettazione, immissione sul mercato) e, di conseguenza, senza avere la legittimazione ad agire su di esso. Per la consumazione del reato occorre, anche in questo caso, la determinazione di un pericolo per la incolumità pubblica o individuale.

Rispetto alla fattispecie del primo comma, la condotta tipica è qui concepita in forma **commissiva** e consiste nell'alterare di un sistema di intelligenza artificiale ad alto rischio con il conseguente pericolo concreto individuato nelle due fattispecie, di base ed aggravata.

In questo caso, dunque, il soggetto attivo "**chiunque**" si colloca effettivamente nell'ambito di una cerchia potenzialmente illimitata di agenti che intervengono dall'esterno, compiendo una sorta di sabotaggio al sistema.

La *Relazione illustrativa* descrive la fattispecie in esame come una norma di chiusura indispensabile per scongiurare vuoti di tutela laddove il pericolo effettivo derivi da interventi attivi ed esterni sul sistema.

Questo ruolo è ribadito dalla clausola di riserva inserita nel testo, la quale prevede l'applicabilità della norma solo se il fatto non costituisce un reato più grave[74].

Viene inoltre evidenziato come la disposizione si colleghi logicamente alla natura omissiva del primo comma, completando e razionalizzando l'intero impianto normativo: sarebbe infatti contraddittorio lasciare impunito il soggetto esterno che pone in essere l'alterazione attiva, condotta che risulta ancora più grave e che giustifica, di conseguenza, sanzioni più severe.

La clausola di riserva vale anche in relazione alla condotta omissiva di cui al primo comma, a significare che l'alterazione "commissiva" richiede una condotta che può compiersi anche al di fuori delle fasi di attività ivi individuate e anche dalla tipologia di intervento sabotatore, che non necessariamente deve avere ad oggetto le specifiche misure di sicurezza predisposte per evitare malfunzionamenti, ma incide sulla materialità complessiva del sistema, pur dovendosi sempre accertare la messa in pericolo del bene protetto.

Anche per l'ipotesi commissiva è previsto il solo dolo generico per la cui configurazione valgono le considerazioni già esposte.

Non vi sono dubbi sulla configurabilità del **tentativo**.

Le pene edittali variano in base alla natura del pericolo generato dall'alterazione:

- la reclusione **da 2 a 6 anni** qualora sia minacciata la vita o l'incolumità individuale o pubblica;
- la reclusione **da 3 a 10 anni** nel caso in cui il pericolo riguardi la sicurezza dello Stato.

[74] Si possono ipotizzare fattispecie più gravi già all'interno dello stesso capo I del titolo IV del codice penale, come nel caso dei delitti di strage art. 422 c.p., di disastro aviatorio art. 428 c.p., di attentato alla sicurezza delle installazioni nucleari art. 433-*bis* c.p., etc., commessi attraverso l'alterazione di un sistema di intelligenza artificiale ad alto rischio.

3.3.4. Il delitto di omessa adozione delle misure di sorveglianza umana.

Infine, il comma 4 prevede una ulteriore fattispecie in cui soggetto attivo è **l'utilizzatore professionale** di sistemi di intelligenza artificiale ad alto rischio che omette intenzionalmente di adottare misure di sorveglianza umana. L'agente è punito con le pene previste dal primo comma, primo e secondo periodo, qualora da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure un pericolo per la sicurezza dello Stato.

Si tratta di un reato proprio dell'"utilizzatore professionale", a dolo intenzionale, limitato alla mancata adozione di **misure di sorveglianza umana** nel sistema.

La norma non indica chi sia "l'utilizzatore professionale", ma tale espressione altro non risulta che la trasposizione del termine ***deployer***, definito nel regolamento IA come una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, *tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.*

Il dolo "rafforzato" intenzionale richiede la rappresentazione e volizione dell'omissione della sorveglianza umana nel sistema di intelligenza artificiale come obiettivo primario dell'agente, con la cosciente previsione del pericolo concreto per la incolumità. Le pene sono le stesse del primo comma.

Sebbene né la fattispecie prevista al comma 1, né quelle previste ai commi 3 e 4 contengano clausole di riserva, non è escluso che, attraverso l'utilizzo di sistemi di intelligenza artificiale, le omissioni dolose o colpose dell'agente possano integrare anche (o solo) reati diversi rispetto a quelli contemplati dall'art. 437-*bis* c.p., in tutti i casi in cui, a titolo di esempio, in luogo della mera messa in pericolo del bene giuridico protetto se ne determini la lesione.

Specie in relazione ai sistemi di intelligenza artificiale ad alto rischio, destinati a essere utilizzati come *componenti di sicurezza di un prodotto* (ai sensi dell'art. 6 del regolamento IA), è ben possibile, infatti, che le omissioni, dolose o colpose, delle misure tecniche di sicurezza possano provocare gravi eventi di danno per l'incolumità pubblica o individuale[75].

[75] Si pensi, a titolo esemplificativo, ai delitti di strage art. 422 c.p., epidemia art. 438 c.p., morte o lesioni come conseguenza di altro delitto art. 586 c.p. (in cui "altro delitto" è quello di cui al comma 1 o al comma 4 dell'art. 437-*bis* c.p.).

3.4. Le modifiche al codice di procedura penale. L'impiego investigativo dei sistemi di identificazione biometrica remota *in tempo reale* nel nuovo art. 359-*ter* c.p.p.[76]

L'impianto normativo delineato dall'art. 8 del d.lgs. n. 160/2026, concernente le attribuzioni di pubblica sicurezza e l'attività preventiva delle forze di polizia, trova una simmetrica estensione sul versante del vero e proprio procedimento penale.

I sistemi di intelligenza artificiale orientati all'identificazione biometrica remota *in tempo reale* fanno il loro esordio nella fase delle indagini preliminari e per il perseguimento di finalità strettamente investigative[77].

---

[76] L'art. 13 introduce **Modifiche al codice di procedura penale**: "1. Al codice di procedura penale, dopo l'articolo 359-*bis* è inserito il seguente: «**Art. 359-*ter* (Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale**) - 1. Quando occorre **confermare l'identificazione** di una persona nei confronti della quale vi sono sufficienti indizi della commissione di uno dei delitti di cui all'**allegato II al** regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, puniti con la pena della reclusione **non inferiore nel massimo a quattro anni**, ovvero procedere alla **ricerca mirata**, ivi compresa la **localizzazione**, di una persona **indiziata** dei medesimi delitti, può essere autorizzato l'impiego di sistemi di intelligenza artificiale per **l'identificazione biometrica remota in tempo reale**.2. Quando occorre procedere alla ricerca di **un latitante** ai fini dell'esecuzione di un'ordinanza che dispone una **misura cautelare coercitiva** per uno dei delitti indicati al comma 1, ovvero di un **ordine di esecuzione** non sospeso che dispone la carcerazione per i medesimi delitti, può essere autorizzata la localizzazione della persona ricercata tramite identificazione biometrica remota in tempo reale con l'uso di sistemi di intelligenza artificiale, procedendo al **confronto** dei suoi dati biometrici con quelli di individui memorizzati in una banca dati di riferimento.3. Nei casi di cui ai commi 1 e 2, il confronto biometrico avviene esclusivamente con **una banca dati di riferimento adeguata** per ciascuna delle finalità di cui ai medesimi commi, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate, di cui ai medesimi commi 1 e 2. La banca dati di cui al primo periodo può essere derivata da dati contenuti in banche dati in uso alla polizia giudiziaria o tenute da altre pubbliche amministrazioni e accessibili alla stessa o all'autorità giudiziaria, ovvero da immagini, filmati o altri elementi biometrici acquisiti legalmente nell'ambito delle indagini. **Il contenuto della banca dati di cui al primo periodo è formato appositamente per ciascun utilizzo, con i soli dati biometrici pertinenti alla specifica finalità**, che sono cancellati al termine della validità dell'autorizzazione, in modo da garantire che il set di confronto sia specifico per ciascuna autorizzazione e non sia suscettibile di alimentazione incrementale rispetto alle autorizzazioni pregresse. È in ogni caso **vietato** l'uso di banche dati biometriche alimentate, in tutto o in parte, mediante tecniche di **scraping non mirato**, ovvero costituite in violazione delle disposizioni vigenti in materia di protezione dei dati personali.4. Con le stesse modalità di cui ai commi 1, 2 e 3 può essere autorizzata la ricerca mirata, nell'ambito di un procedimento penale, di **specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale** di esseri umani.5. Nei casi di cui ai commi da 1 a 4 **il pubblico ministero** richiede l'autorizzazione all'impiego del sistema di intelligenza artificiale per l'identificazione biometrica remota in tempo reale al giudice per le indagini preliminari.6. Il **giudice per le indagini preliminari autorizza l'impiego** del sistema di intelligenza artificiale di cui al comma 5 con decreto motivato. Nel provvedimento di autorizzazione è delimitata **l'area geografica** di applicazione, sono indicate le **persone** specificamente ricercate ed è determinato **il tempo strettamente necessario**, che non può in ogni caso superare i quindici giorni, prorogabili dal giudice, con decreto motivato, su richiesta del pubblico ministero, per periodi successivi di quindici giorni, qualora permangano le condizioni. L'autorizzazione può essere concessa soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento (UE) 2024/1689. 7. **Quando ricorrono ragioni di urgenza** e vi è fondato motivo di ritenere che dal ritardo possa derivare pregiudizio grave e irreparabile per le finalità di cui ai commi da 1 a 4, **il pubblico ministero**, con provvedimento adottato nel rispetto delle indicazioni di cui al comma 6, secondo periodo, dispone l'utilizzo del sistema di intelligenza artificiale per l'identificazione biometrica remota in tempo reale **con decreto motivato.** Il decreto è comunicato immediatamente e comunque non oltre ventiquattro ore al giudice per le indagini preliminari, il quale, se ne ricorrono i presupposti, nelle successive quarantotto ore, convalida il provvedimento e autorizza la prosecuzione. Negli stessi casi di cui al primo periodo, se non sia possibile, per la situazione di urgenza, attendere il provvedimento del pubblico ministero, all'attivazione del sistema di identificazione biometrica remota in tempo reale provvedono gli ufficiali di polizia giudiziaria, i quali, senza ritardo e comunque entro le successive dodici ore, trasmettono la richiesta di autorizzazione al pubblico ministero, il quale, se ne ricorrono i presupposti, richiede al giudice la convalida entro ventiquattro ore dall'avvio del sistema. Il giudice, se ne ricorrono i presupposti, nelle successive quarantotto ore, convalida il provvedimento e autorizza la prosecuzione dell'attività, con le indicazioni di cui al comma 6.8. I risultati forniti dai sistemi di intelligenza artificiale non possono essere utilizzati qualora gli stessi siano stati impiegati fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dai commi 6 e 7. In questi casi, tutti i dati personali, i risultati e gli *output* acquisiti e prodotti sono **cancellati**, salvo che costituiscano corpo del reato.».

[77] N. CANESTRINI, *Riconoscimento facciale e intelligenza artificiale nelle indagini: regole, limiti e diritti della difesa***,** in *CanestriniLex,* 10/10/2026 osserva come la materia finora non avesse una disciplina tipica: "*l'identificazione biometrica veniva ricondotta, di volta in volta, ai rilievi di polizia giudiziaria, all'identificazione o agli accertamenti tecnici*". Il tentativo di introdurre un sistema in tempo reale si era fermato davanti al **parere negativo del Garante** sul sistema **SARI *Real Time*** del 25 marzo 2021. L'Autorità garante ha espresso parere negativo in quanto il trattamento dei dati biometrici tramite il sistema SARI Real Time non risulta conforme alla disciplina di cui al decreto legislativo del 30 giugno 2003, n. 196, integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101, in assenza di un'adeguata e specifica normativa che legittimi il riconoscimento facciale in tempo reale,

La norma si inserisce in un delicato quadro di equilibri fra sicurezza e rispetto dei diritti fondamentali[78].

L'art. 13 del d.lgs. introduce l'art. **359-*ter* c.p.p**., norma di stretto diritto processuale deputata a disciplinare i presupposti e le forme dei provvedimenti di «identificazione» e «localizzazione» mediante i predetti applicativi tecnologici[79].

3.4.1. Oggetto e presupposti del procedimento.

Il procedimento si colloca nell'ambito delle attività investigative proprie del pubblico ministero, nel contesto dell'utilizzo di ausili di carattere tecnico (inserito dopo gli artt. 359 che prevede l'utilizzo di consulenti tecnici del p.m. e 359-*bis* che disciplina il procedimento relativo al prelievo coattivo di campioni biologici su persone viventi di cui ricalca sommariamente le fasi), sotto la rubrica «**Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale**».

Il ricorso a tali strumenti di indagine è rigorosamente subordinato a un duplice vincolo selettivo, sia sotto il profilo edittale sia in ordine al *fumus* di reato.

Il catalogo dei reati presupposto è mutuato dall'Allegato II del Regolamento IA, *limitatamente* alle fattispecie punite con la pena della reclusione non inferiore nel massimo a quattro anni.

L'allegato II del Regolamento elenca i seguenti reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii): **terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale** coinvolta in uno o più dei reati elencati sopra.

---

essendovi il rischio di una sorveglianza universale allo scopo di identificare alcuni individui in violazione della loro vita privata. Critico anche E. BELVINI, *La disciplina dei software di riconoscimento facciale: rischi e prospettive,* in *Proc. pen. giust*., 1, 2026 il quale osserva: "*La diffusione del tutto informale del S.A.R.I., senza specificare limiti rigorosi d'impiego e regole chiare sui requisiti per poterlo adoperare, produce numerose incognite: sono ignote le modalità con le quali sono alimentate le banche dati utilizzate per il raffronto automatizzato; non è affatto chiaro il destino delle immagini catturate dalla macchina ma di cui l'operatore ha escluso il match nel caso concreto, palesando così l'insidia di raccolte indiscriminate dei dati biometrici da utilizzare per ulteriori riconoscimenti; non sono note le metodologie con le quali è testata l'accuratezza del software; si concretizza, con il S.A.R.I. Real Time, il pericolo di monitoraggi clandestini su ampie fette della popolazione; non è dato sapere se vi sono accorgimenti per limitare gli accessi al tool né, tanto meno, se essi sono annotati in un apposito registro*".

[78] Per l'identificazione biometrica remota *in tempo reale* v. **Corte EDU,** Sez. III, 4 luglio 2023, Glulikh c. Russia in cui si sottolinea come l'uso indiscriminato di strumenti di riconoscimento facciale per l'individuazione di un sospettato sia uno strumento fortemente intrusivo che necessita di un alto livello di giustificazione in una società democratica in quanto lesivo degli artt. 8 (Libertà di espressione) e 10 (Vita privata) della Carta. Il caso riguardava un soggetto che manifestava da solo e pacificamente, sanzionato solo per un mero illecito amministrativo (per non aver preavvisato la sua protesta), che era stato identificato attraverso immagini diffuse in rete, poi individuato e arrestato in metropolitana grazie alle telecamere a riconoscimento facciale in tempo reale.

[79] Per un primo commento si veda N. ROSSI, *L'intelligenza artificiale*, cit.

Si tratta di un'elencazione tassativa di delitti, insuscettibile di analogia, espressione di un criterio di proporzione in senso stretto.

La platea delle fattispecie a cui lo strumento di indagine è applicabile è di fatto piuttosto vasta, tenuto conto che, in relazione al limite edittale individuato, vi rientrano pressocché tutti i delitti che appartengono alle categorie elencate dal regolamento IA, compresi molti dei reati ambientali (laddove siano caratterizzati quali delitti e non come contravvenzioni).

Nel caso della rapina, tuttavia, è necessario che sia "organizzata[80]" o "a mano armata", non bastando la fattispecie semplice, pur avendo limiti edittali superiori a quello individuato.

All'interno di tale perimetro, l'impiego della tecnologia è legittimato per le seguenti esigenze tassative:

- conferma dell'identificazione di un soggetto nei cui confronti emergano sufficienti indizi in ordine alla commissione di uno dei delitti summenzionati;

- ricerca mirata e **localizzazione** del soggetto indiziato dei medesimi titoli di reato;

- localizzazione di soggetti **latitanti o evasi**, destinatari di una misura cautelare coercitiva ovvero di un ordine di esecuzione della pena detentiva[81];

- ricerca mirata, nell'ambito di un pendente procedimento penale, di **specifiche vittime** dei delitti di sottrazione, tratta di persone o sfruttamento sessuale.

Il confronto biometrico può avvenire esclusivamente con **una banca dati di riferimento adeguata** per ciascuna delle finalità indicate, che deve contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone menzionate, anche non identificate.

3.4.2. Il procedimento autorizzativo.

In ossequio al principio della riserva di giurisdizione a tutela dei diritti costituzionali e convenzionali, l'*attivazione* dei sistemi biometrici in tempo reale[82] è subordinata alla preventiva autorizzazione del **giudice per le indagini preliminari**, il quale provvede con **decreto motivato** su istanza del pubblico ministero[83].

---

[80] Il requisito dell'organizzazione sembra richiedere, per il diritto interno, una rapina quantomeno aggravata dalla più persone riunite, *ex* art. 628, comma 3, n. 1) c.p..

[81] Nel parere che la Commissione dell'ANM "Innovazione Tecnologica e Organizzativa, Transizione Digitale, Informatica e Intelligenza Artificiale" ha reso *su Atto del Governo n. 418 (Schema decreto legislativo recante "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024,* (il cui contenuto è raggiungibile al link https://lamagistratura.it/attualita/il-parere-della-commissione-innovazione-sul-decreto-ia-del-governo/), viene formulato sul punto uno specifico rilievo in materia di competenza: "*Tenuto conto che il comma 2 consente l'impiego di sistemi IA di rilevazione biometrica per ricercare un latitante nei confronti del quale bisogna eseguire una misura cautelare coercitiva ovvero un ordine di esecuzione della pena della reclusione e che la misura cautelare può essere applicata anche al di fuori delle indagini preliminari, problemi possono ravvisarsi nella parte in cui viene stabilita la competenza all'autorizzazione all'impiego di sistemi di IA per l'identificazione biometrica remota in tempo reale unicamente in capo al GIP, anche nella parte in cui egli non è più competente con riferimento al procedimento al quale la misura coercitiva o l'ordine di esecuzione si riferiscono*".

[82] Si vedano, per la corretta comprensione dell'attività di "riconoscimento biometrico" le linee-guida in materia di riconoscimento biometrico e firma grafometrica di cui all'Allegato A al Provvedimento del Garante del 12 novembre 2014, cit.

[83] G.M. RICCIO, *d.lgs. 160/2026, cit.,* osserva: "*La scelta di riservare al g.i.p. (e non al solo p.m.) l'autorizzazione all'identificazione biometrica remota in tempo reale nell'ambito di un procedimento penale già pendente, a differenza di quanto previsto in via amministrativa dall'art. 8 per le finalità di mera prevenzione, disegna un sistema "a doppio binario" le cui differenze di garanzia (giudice v. pubblico ministero) trovano una qualche giustificazione nella diversità*

Il provvedimento giurisdizionale deve assolvere a precisi oneri di specificazione e contenimento, determinando espressamente:

1. l'estensione e i confini dell'area geografica di applicazione;
2. i dati identificativi o gli elementi selettivi delle persone specificamente ricercate;
3. il limite temporale dell'attività, circoscritto alla stretta necessità investigativa e comunque non superiore a quindici giorni, fatta salva la facoltà di proroga con successivo decreto su richiesta motivata del pubblico ministero.

Sotto il profilo motivazionale, il giudice per le indagini preliminari è investito, dunque, del dovere di compiere il giudizio di bilanciamento e di **proporzionalità**[84] prescritto dall'art. 5, paragrafo 2, del Regolamento IA.

Tale vaglio impone la valutazione comparativa tra il pregiudizio derivante dal mancato impiego del sistema e le ricadute concrete della misura sui diritti e sulle libertà fondamentali dei terzi e dei soggetti interessati (*data protection impact assessment* e rispetto dei diritti fondamentali).

La codificazione normativa della necessità di una simile valutazione costituisce una novità nel contenuto della motivazione richiesta all'autorità giudiziaria, richiedendo un **giudizio di impatto** dell'uso del sistema per le strette finalità consentite dal legislatore che funge da presupposto di legittimazione dell'adozione del decreto autorizzativo e che consiste in un espresso giudizio di comparazione e di bilanciamento che mira alla salvaguardia del principio di proporzionalità, precludendo l'adozione di motivazioni prive della esplicitazione di tale espresso bilanciamento che chiarisca la ragione della prevalenza della necessità dell'utilizzo del sistema di intelligenza artificiale sui diritti fondamentali.

Nel caso in cui il decreto del giudice per le indagini preliminari non sia motivato o non adeguatamente motivato rispetto allo specifico contenuto richiesto dal modello procedimentale, secondo uno schema assimilabile a quello delle intercettazioni (art. 271 c.p.p.), il legislatore ne fa conseguire l'**inutilizzabilità** dei risultati forniti dai sistemi di intelligenza artificiale (per mancata osservazione delle disposizioni previste dal **comma 6** dell'art. 359-*ter* c.p.p.).

Proprio perché la sanzione è quella della inutilizzabilità, ampie indicazioni circa le conseguenze di una motivazione mancante, insufficiente o incongrua si possano forse trarre dalle elaborazioni giurisprudenziali in materia di intercettazioni[85], così come avuto riguardo

---

delle finalità perseguite, ma che imporranno un attento coordinamento interpretativo, specie nei casi di sovrapposizione fattuale tra prevenzione e repressione dei reati".

[84] Per il rilievo che assume il **principio di proporzionalità nel processo penale** si veda l'analisi di L. GIORDANO, *Principio di proporzionalità e diritto processuale penale: una panoramica giurisprudenziale*, in *Dir. giust. cost.*, 28/04/2025. In giurisprudenza, fra le molte, v. *Sez.* U, 28/04/2016, *n.* 27620, Rv. 267486-01; S.U, 19/04/2018, n. 36072, Rv. 273548-01.

[85] V., in particolare, Sez. U, 21/06/2000, n. 17, Rv. 216665-01: "*La mancanza di motivazione dei decreti che autorizzano o prorogano le operazioni di intercettazioni telefoniche o tra presenti, di quelli che convalidano i decreti emessi in caso d'urgenza dal pubblico ministero, nonché di questi ultimi, comporta l'inutilizzabilità dei risultati delle operazioni captative. (Nell'occasione, la S.C. ha avuto modo di precisare che si ha **mancanza della motivazione** non solo quando l'apparato giustificativo manchi in senso fisico-testuale, ma anche quando la motivazione sia apparente, semplicemente ripetitiva della formula normativa, del tutto incongrua rispetto al provvedimento che dovrebbe giustificare; mentre si ha **difetto della motivazione** - emendabile dal giudice cui la doglianza venga prospettata, sia esso il giudice del merito che deve utilizzare i risultati delle intercettazioni, sia esso quello dell'impugnazione nella fase di merito o in quella di legittimità - allorché quest'ultima sia incompleta, insufficiente,*

alle conseguenze della inutilizzabilità rispetto ai risultati ottenuti[86]. Va peraltro evidenziato che la norma è ancora più incisiva laddove impone non solo un divieto di utilizzo ma anche la **cancellazione** di tutti i dati personali, i risultati e gli output acquisiti e prodotti, a meno che non costituiscano corpo del reato.

Il legislatore ha previsto due sub-procedimenti derogatori, attivabili qualora il *periculum in mora* e il rischio di un danno grave e irreparabile non consentano il rispetto dei tempi della procedura ordinaria:

- procedura **d'urgenza**: il pubblico ministero assume la titolarità del potere autorizzatorio, adottando un proprio decreto motivato che deve essere trasmesso, senza ritardo, al giudice per le indagini preliminari per la necessaria convalida[87].
- procedura di **estrema urgenza**: qualora la situazione emergenziale precluda finanche la tempestiva adozione del provvedimento del magistrato inquirente, l'attivazione dei sistemi è demandata direttamente agli ufficiali di polizia giudiziaria. Sorge in capo a questi ultimi l'obbligo di trasmettere gli atti al pubblico ministero entro il termine perentorio di dodici ore; il pubblico ministero, valutata la sussistenza dei presupposti, formulerà la successiva richiesta di convalida al giudice**.**

A garanzia dell'effettività del tessuto precettivo, l'ultimo comma riproduce il medesimo regime sanzionatorio già stabilito dall'art. 8 del d.lgs. n. 160/2026: l'inosservanza delle procedure autorizzative stabilite dalla legge, così come l'eventuale **diniego di convalida** da parte del giudice per le indagini preliminari, determina una duplice conseguenza: l'obbligo di immediata cancellazione dei dati biometrici acquisiti e la totale inutilizzabilità processuale dei risultati medio tempore ottenuti.

La *Relazione illustrativa* qualifica la previsione come formulata «secondo il paradigma dell'art. 191 c.p.p.» e la descrive quale «strumento di chiusura del sistema di garanzie».

La collocazione sistematica, l'assetto del procedimento autorizzativo e i poteri riconosciuti alla polizia giudiziaria nei casi di urgenza sono stati oggetto di critiche a una prima lettura della norma.

In primo luogo, la norma è stata ritenuta fuori posto, in quanto l'attività in essa prevista non sarebbe equiparabile a un accertamento tecnico ma piuttosto assimilabile a un'intercettazione, nella misura in cui vi è una sorveglianza in tempo reale che consente di acquisire dei dati biometrici.

---

non perfettamente adeguata, affetta da vizi che non negano, ne' compromettono la giustificazione, ma la rendono non puntuale).

[86] Da ultimo Sez. 6, 25/11/2025, n. 41152, Rv. 289047: "*L'inutilizzabilità degli esiti di intercettazioni telefoniche non preclude la possibilità che essi siano apprezzati alla stregua di una "notitia criminis", cui può seguire l'iscrizione di un nuovo procedimento penale e l'adozione, in forza di ulteriori elementi indiziari, di un provvedimento di sequestro probatorio, non operando, nella materia dell'inutilizzabilità, il principio sancito dall'art. 185 c.p.p. per le nullità, secondo cui il vizio si trasmette agli atti consecutivi a quello dichiarato nullo".*

[87] Si veda Sez. 6, 13/12/2021, n. 8885, Rv. 283010-01 che, per l'omologa procedura in materia di prelievo urgente di campioni biologici di cui all'art. 359-*bis* c.p.p., fa decorrere il termine di 48 ore per la convalida non dall'emissione del decreto del pubblico ministero ma dall'effettuazione del prelievo. *Mutatis mutandis* il termine di 48 ore dovrebbe dunque decorrere dal momento dell'attivazione effettiva del sistema biometrico in tempo reale e non dall'adozione del decreto da parte del pubblico ministero.

Non pare del tutto in fuoco tale critica atteso che il procedimento tipizzato introdotto dal legislatore ha essenzialmente una finalità di ricerca di un soggetto in vista della sua identificazione e localizzazione, senza che vengano in rilievo condotte poste in essere durante l'attivazione del sistema di riconoscimento.

Sotto questo profilo, va considerato che sussiste una assonanza con il prelievo coattivo di campioni biologici che, allo stesso modo, può essere utilizzato per la identificazione dell'indagato.

Anzi, l'identificazione con intelligenza artificiale di elementi biometrici dovrebbe essere preferita al prelievo coattivo di materiale biologico, essendo uno strumento meno invasivo nella sfera personale dell'indagato[88].

L'inserimento dell'art. 359-*ter* c.p.p. in questo contesto indica che l'aspetto di interesse per il legislatore è soprattutto negli aspetti tecnici che governano simili procedimenti di riconoscimento biometrico.

Una grave criticità è stata individuata anche nella disciplina d'urgenza, contemplata dal comma 7, ove si affida la competenza al pubblico ministero e, in caso di estrema urgenza, agli ufficiali di polizia giudiziaria. Pur ritenendo tale disposizione possa essere conforme al regolamento (che prevede un'eccezione all'art. 5 par. 3), viene individuato un rischio di illegittimità costituzionale per violazione dell'art. 3 Cost. in quanto l'omologa disciplina sulle intercettazioni, strumento quanto meno equiparabile sotto il profilo della intrusività, non prevede (e non potrebbe prevedere, data la riserva di giurisdizione di cui all'art. 15 Cost.), neppure per i casi di urgenza, poteri autonomi della polizia giudiziaria[89].

3.4.3. Rilevanza indiziaria e probatoria.

Il sistema prevede che l'autorizzazione all'impiego del sistema sia funzionale ad una mera funzione di *conferma* di identità o di ricerca di un soggetto.

Non si affronta, attraverso il procedimento individuato, il problema della rilevanza indiziaria o probatoria dei risultati forniti dal sistema per l'adozione di provvedimenti conseguenti (ai fini, ad es., dell'adozione misure cautelari o in ordine alla rilevanza probatoria di una identificazione siffatta in un successivo giudizio).

Va di per sé che il modulo procedimentale utilizzato non incide sull'attendibilità del risultato, ma garantisce solo il rispetto delle regole per il bilanciamento degli interessi in gioco[90].

---

[88] Così A. VELE, *Identificazione, intelligenza artificiale e riconoscimento facciale ai sensi dell'art. 349 c.p.p.*, in *Arch. pen*., 1, 2026.

[89] Si veda V. GIALUZ, *Riconoscimento biometrico e garanzie necessarie nello Stato democratico*, in *Sist. pen*. 30 luglio 2026, secondo cui ne conseguirebbe il paradosso per cui, per un atto meno intrusivo, si finirebbe per escludere la facoltà di attivarsi della polizia, mentre lo si consentirebbe per un atto molto più intrusivo per il singolo e per la collettività, qual è il riconoscimento biometrico *real time*.

[90] Si legge in L. BELVINI, *La disciplina, cit.*: *"Dalla disamina dei profili tecnici sono emerse diverse incognite da affrontare nel vaglio sulla compatibilità dei sistemi automatizzati di riconoscimento facciale con i valori che governano la procedura giudiziaria. Un primo consistente ostacolo è rappresentato dall'**opacità** che contraddistingue l'algoritmo di I.A. alla base del software: le metodiche di «autoapprendimento» e la complessità delle reti neurali artificiali, che garantiscono il funzionamento dei tools di identificazione biometrica, rendono inaccessibile l'operato dell'apparato informatico; la qual cosa impedisce di comprendere come la macchina "riconosce" i volti umani, essendo, in sostanza, possibile soltanto osservare gli input e il «match» restituito dall'algoritmo senza conoscere il quomodo dell'operazione*

Va evidenziato in proposito che, per i risultati acquisiti all'esito del procedimento autorizzatorio delineato dall'art. 359-*ter* c.p.p. non è replicata dal legislatore una formula analoga a quella utilizzata nell'art. 7 comma 1 lett c)[91], né vengono date indicazioni sul valore probatorio dei risultati acquisiti alla luce dei principi generali contenuti nell'art. 192 c.p.p..

Il problema dell'attendibilità di tali risultati resta dunque in una zona di opacità, affidata ad una valutazione del giudice che dovrà basarsi o sugli elementi di contesto (nei quali si inserisca la *conferma* ottenuta dal sistema), o sul grado di affidabilità dello specifico sistema di intelligenza artificiale che è stato utilizzato.

Va ricordato allora che l'art. 13 del regolamento IA impone a chi progetta e sviluppa i sistemi di IA ad alto rischio di garantire un tipo e un livello di trasparenza adeguati, che consenta ai *deployer* (in questo caso le forze di polizia), di avere istruzioni corrette sul funzionamento.

Nel settore che ci occupa, appaiono particolarmente rilevanti i dati previsti nel paragrafo 3 lett. b) ossia quelli attinenti a "le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio", tra cui spicca il **livello di accuratezza** che ci si può attendere in relazione agli usi che ne vengano effettuati.

Deve necessariamente emergere, dunque, in fase di utilizzo e di interpretazione dei dati estratti dal sistema, un grado di probabilità scientifica apprezzabile che possa rassicurare circa l'affidabilità del sistema e in che misura.

Di tali aspetti il decreto legislativo non si occupa ma si ritiene che dovranno necessariamente connotare la comunicazione informativa fra polizia giudiziaria, che è il *deployer* che utilizza il sistema autorizzato, e autorità giudiziaria che acquisisce e valuta il risultato[92].

D'altra parte, la legge IA, all'art. 15 stabilisce che nei casi di utilizzo dei sistemi di intelligenza artificiale nell'ambito dell'attività giudiziaria sia sempre riservata al magistrato ogni decisione sull'interpretazione, sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti.

Si tratta di individuare, con l'ausilio dell'esperienza tecnica, quali siano gli strumenti di cui il giudice possa disporre per compiere le sue valutazioni con riferimento al grado di approssimazione o di certezza offerto dal sistema.

---

automatizzata. In questo modo, il sistema assume le sembianze di una vera e propria «black box», pregiudicando qualsiasi possibilità di controllare, ex post, il percorso decisionale seguito dall'automated facial recognition system. Si tratta di un aspetto che complica, in maniera considerevole, la fruibilità dei frutti dell'I.A. nel procedimento penale. L'opacità è fatalmente in antitesi con la costellazione di valori fondamentali, interni (artt. 24, 27, co. 2, 111 Cost.) e sovranazionali (artt. 6 Cedu, 47 e 48 C.D.F.U.E.) che, nel presidiare la funzione epistemica dell'accertamento penale, esigono la piena trasparenza e governabilità dei processi automatizzati capaci di condizionare la decisione giudiziaria. In effetti, servirsi di mezzi che, a causa della loro imperscrutabilità, non sono sorvegliabili appieno dall'uomo, rischia di mettere a repentaglio l'autonomia della magistratura, producendo decisioni appiattite acriticamente sul «cogito artificiale»[70], e, al contempo, mortifica i diritti difensivi (art. 24, co. 2, Cost.), impedendo ai soggetti destinatari dei provvedimenti basati sui risultati «automatizzati» di poterne contestare i contenuti".

[91] Che prevede la possibilità di operazioni di catalogazione dei dati acquisiti attraverso i sistemi di i.a. per le forze di polizia sempre che esse non costituiscano "l'unico fondamento di decisioni che producono effetti giuridici nei confronti di persone fisiche".

[92] A. VELE, *Identificazione, cit.,* segnala: "*l'intelligenza artificiale deve essere in grado di «spiegare» come è giunta alle proprie conclusioni, ove determinati software – oggi o domani – siano in grado di evidenziare i passaggi logici del risultato prodotti*".

3.5. Modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale: il sequestro preventivo sui contenuti generati con intelligenza artificiale.

L'art. 14 del d.lgs. modifica **l'art. 104, comma 1**, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui all'allegato al d.lgs. 28 luglio 1989, n. 271, alla **lettera e-*bis***).

L'art. 104 citato è rubricato "Esecuzione del **sequestro preventivo**" e disciplina, in relazione alle diverse tipologie di beni oggetto del sequestro (beni mobili, immobili, crediti, etc.), le modalità esecutive attraverso le quali il sequestro viene in concreto posto in essere.

L'art. 2, comma 2-*bis* del d.l. 24 febbraio 2026, n. 23, convertito con modificazioni, con legge 24 aprile 2026, n. 54[93], ha aggiunto alla disposizione la lettera e-*bis*) che ha regolato le modalità di attuazione del sequestro preventivo "sui contenuti online *del profilo personale* e sui relativi dati".

Il sequestro si realizza "mediante **ordine** ai prestatori di servizi di hosting, ai fornitori di piattaforme online o di motori di ricerca o ai prestatori di servizi intermediari della società dell'informazione quali definiti all'art. 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015[94], **di rimuovere i contenuti e i dati o disabilitare l'accesso al profilo,** garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite".

L'art. 14 del d.lgs. ha **sostituito** le parole «del profilo personale», con le seguenti: **«generati anche con sistemi di intelligenza artificiale»,** introducendo una specifica modalità di attuazione del sequestro preventivo di tipo impeditivo nelle procedure investigative sui contenuti generati con i sistemi di intelligenza artificiale, non più necessariamente afferenti al profilo personale.

Nella *Relazione introduttiva* a tal proposito si legge che "con specifico riguardo alla modifica dell'articolo 104 del d.lgs. 28 luglio 1989, n. 271, non si può omettere un riferimento agli ambiti interessati dal regolamento (UE) 2021/784 relativo al contrasto della diffusione di

---

[93] Si tratta del cd. "**decreto sicurezza**" per l'analisi del quale si rinvia alla **Relazione su novità normativa dell'Ufficio del Massimario** n. 39 del 13/05/2026. A p. 85 di detta relazione si legge: "*la novità introdotta dal «decreto sicurezza» si limita a fornire un referente normativo a una modalità esecutiva già, invero, praticata in relazione al sequestro preventivo di contenuti digitali, misura anch'essa già scrutinata dalla giurisprudenza. Infatti, come chiarito da Sez. U, n. 31022 del 29/01/2015, Fazzo, Rv. 264089-01, nella moderna società digitale, di fronte a illeciti penali commessi in uno spazio caratterizzato da nuovi modelli comunicativi e da innovative modalità di fruizione dei beni immateriali, il sequestro preventivo non può essere inteso come limitato alla sola adprehensio in senso fisico della «cosa», potendosi anche concretizzare «in una vera e propria **inibitoria**» rivolta al fornitore di connettività, che deve impedire agli utenti l'accesso al sito o alla singola pagina web incriminati ovvero rimuovere il file che viene in rilievo, con l'effetto di arrestare l'attività criminosa in atto o scongiurare la commissione di ulteriori condotte illecite. Infine, l'inciso, presente nell'ultima parte della nuova disposizione, teso a salvaguardare, nell'esecuzione del sequestro preventivo dei dati del profilodigitale della persona, la fruizione dei contenuti estranei alle condotte illecite, si pone in linea con la giurisprudenza di legittimità, secondo la quale anche il sequestro preventivo deve essere governato dai medesimi principi di proporzionalità, adeguatezza e gradualità, dettati dall'art. 275 c.p.p. per le misure cautelari personali (cfr. Sez. 3, n. 21271 del 7/05/2014, Konovalov, Rv. 261509-01; Sez. 5, n. 11895 del 30/10/2013, Belviso, Rv. 258333-01)."*

[94] La Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015 prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione). L'art. 1, paragrafo 1., lett. b) definisce "servizio" qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

contenuti terroristici online e del regolamento (UE) 2022/2065 (Digital Services Act), rispetto ai quali assume rilievo il tema della rimozione e del sequestro di contenuti digitali generati anche mediante sistemi di intelligenza artificiale".

Il riferimento normativo evidenzia l'intersezione tra la sicurezza dei contenuti digitali, la tutela dei diritti fondamentali e l'impatto delle tecnologie emergenti, in quanto i due regolamenti menzionati rappresentano i pilastri europei per la moderazione e la rimozione dei contenuti illeciti in rete, con implicazioni dirette sul materiale generato da intelligenze artificiali.

Il Regolamento (UE) 2021/784 (Contrasto ai contenuti terroristici online) si concentra, in particolare, sulla **rimozione** tempestiva del materiale di propaganda, istigazione o apologia del terrorismo. Su ordine dell'autorità nazionale competente[95], i prestatori di servizi di hosting devono rimuovere il contenuto terroristico o disabilitarne l'accesso entro 60 minuti dalla ricezione dell'ordine. Sono previste, inoltre, una serie di **misure preventive** delle quali sono onerate le piattaforme esposte a tali rischi che devono implementare i sistemi automatizzati di filtraggio in grado di riconoscere la reiterazione di contenuti già identificati come illeciti.

Il Regolamento (UE) 2022/2065 (Digital Services Act - DSA), definisce il quadro generale di responsabilità per tutti i servizi intermediari digitali in Europa prevedendo **meccanismi di segnalazione e azione,** obbligando le piattaforme a istituire procedure chiare per consentire agli utenti di segnalare contenuti illegali e a decidere sulla loro rimozione in modo tempestivo, diligente e non arbitrario. Introduce inoltre tutele contro le rimozioni ingiustificate, richiedendo motivazioni trasparenti per la moderazione e offrendo agli utenti vie di ricorso accessibili.

Il tema della rimozione e del sequestro di contenuti generati da IA (come *deepfake*, testi sintetici di propaganda o immagini manipolate), amplifica la complessità tecnica e giuridica di queste norme, tenuto conto che i sistemi di IA generativa consentono la produzione massiva, rapida e realistica di contenuti illeciti o terroristici dissimulati, rendendo obsoleti i vecchi sistemi di rilevamento basati solo su firme digitali note.

Si tenga peraltro presente che entrambi i regolamenti stabiliscono che, nonostante la rimozione o la disabilitazione dell'accesso pubblico, i fornitori di servizi devono conservare i contenuti rimossi e i relativi dati di traffico per un periodo specifico (es. 6 mesi per il regolamento terroristico), rendendoli disponibili per finalità investigative e per l'eventuale formale sequestro *probatorio* da parte dell'autorità giudiziaria[96].

---

[95] L'art. 3 del d.lgs. 24 luglio 2023, n. 107, che contiene adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2021/784, individua nel **pubblico ministero** l'autorità competente a emettere un ordine di rimozione nei confronti di un prestatore di servizi di hosting quando i contenuti terroristici sono riconducibili a un delitto con finalità terroristiche. Diversa, dunque, si pone la scansione procedurale per questi ordini immediati nel settore specifico del contenuto "terroristico" e la previsione dell'ordine quale modalità attuativa del sequestro preventivo, che ricade nel procedimento ordinario di competenza del giudice per le indagini preliminari ex art. 321 c.p.p.

[96] L'art. 6 del Regolamento (UE) 2021/784. stabilisce che i prestatori di servizi di hosting devono conservare i contenuti terroristici che sono stati rimossi o il cui accesso è stato disabilitato (insieme ai relativi dati di traffico) per un periodo di 6 mesi. La norma specifica che tale conservazione serve esclusivamente per finalità di ricorso amministrativo o giudiziario, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Per quanto riguarda invece il Digital Services Act (Regolamento UE 2022/2065), l'obbligo di conservazione dei dati legata alle rimozioni e alle decisioni di moderazione si ravvisa in diverse disposizioni come l'art. 20 (relativo al sistema

3.6. La responsabilità amministrativa degli enti per reati commessi con l'uso dell'intelligenza artificiale.

L'**art. 15** del d.lgs. così dispone: "1. Al **d.lgs. 8 giugno 2001, n. 231,** dopo l'articolo 25-undevicies**, è inserito il seguente: «Art. 25-vicies** (Reati commessi con l'uso di sistemi di intelligenza artificiale). - 1. In relazione al delitto di cui all'articolo 437-*bis* del codice penale, si applica all'ente la sanzione pecuniaria da seicento a mille quote. 2. In relazione al delitto di cui all'articolo 612-*quater* del codice penale, si applica all'ente la sanzione pecuniaria da duecento a settecento quote. 3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b), c), d) ed e).».

L'**art. 15 del decreto** amplia dunque i reati-presupposto della responsabilità amministrativa degli enti, introducendo il nuovo (e allo stato ultimo del lungo elenco che prevede le sanzioni all'ente in relazione alle fattispecie di reato individuate), **art. 25-*vicies* d.lgs. n. 231/2001**.

La responsabilità dell'ente scatta esclusivamente per due fattispecie:

- Art. 437-*bis* c.p.: Sanzione pecuniaria da **600 a 1000 quote**.

- Art. 612-*quater* c.p., introdotto dalla legge IA: Sanzione pecuniaria da **200 a 700 quote**.

Per entrambi i reati si applicano solo le **sanzioni interdittive** dell'art. 9, comma 2, lett. b), c), d) ed e) del decreto: sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito (art. 9, comma 2, lett. b) d.lgs. n. 231 de 2001); divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio (art. 9, comma 2, lett. c) d.lgs. n. 231 de 2001); esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi (art. 9, comma 2, lett. d) d.lgs. n. 231 de 2001); divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. e) d.lgs. n. 231 de 2001).

Resta **esclusa** la sanzione dell'**interdizione dall'esercizio dell'attività**. La scelta di escludere l'interdizione dall'esercizio dell'attività rispetta il principio di proporzionalità, collocando di fatto i reati legati all'IA in una fascia di gravità moderata, inferiore rispetto ai reati contro la PA o alla criminalità organizzata.

L'art. **612-*quater* c.p.** è generalmente procedibile a querela della persona offesa. Di conseguenza, la responsabilità dell'ente *ex* art. 25-vicies dipenderà dall'iniziativa del singolo danneggiato. Secondo i primi commentatori, ciò rischia di creare un fenomeno di *under-enforcement* (mancata applicazione della norma), specialmente nei casi in cui i contenuti sintetici o i deepfake non autorizzati vengano diffusi da soggetti collettivi in campagne pubblicitarie senza che la vittima sporga formale querela[97].

interno di gestione dei reclami, che richiede di mantenere i dati necessari a gestire i ricorsi degli utenti), e l'art. 39 (per le piattaforme online di dimensioni molto grandi <VLOP> e ai motori di ricerca di dimensioni molto grandi <VLOSE> i quali devono conservare per finalità ispettive e di audit i dati relativi ai propri sistemi di moderazione).

[97] Vedi G.M. RICCIO, *d.lgs. 160/2026, cit*..

L'articolo 612-*quater* c.p. non punisce la semplice creazione di contenuti *fake*: richiede diffusione senza consenso, capacità di ingannare sulla genuinità e danno ingiusto.[98]

L'ente che si avvale dei sistemi di intelligenza artificiale dovrà dunque gestire il consenso e verificare i contenuti in fase di produzione o diffusione.

Con riferimento al reato di cui all'art. **437-*bis* c.p.**, chi sviluppa o utilizza sistemi di IA ad alto rischio deve invece introdurre protocolli specifici per verificare periodicamente le misure di sicurezza tecnica dei sistemi, al fine di scongiurare i rischi paventati dalla fattispecie, nonché per tracciare la **sorveglianza umana qualificata.**

Deve osservarsi, peraltro, che, mentre il reato di cui all'art. 612 -*quater* c.p. può assumere tipicamente una connotazione soggettiva personale, il reato di cui all'art. **437-*bis* c.p.** (con particolare riferimento alla fattispecie omissiva di cui al primo comma), offre immediate correlazioni con la struttura organizzativa complessa dell'ente responsabile, all'interno della quale può rilevare la specifica **posizione di garanzia** che si assume violata.

Come si evince dal testo normativo e come evidenziato dalla giurisprudenza di legittimità: "*Ai fini della configurabilità della responsabilità amministrativa per fatto proprio dell'ente per i reati commessi nel suo interesse o a suo vantaggio, deve sussistere un rapporto qualificato tra l'autore del reato presupposto e l'ente. (In motivazione la Corte ha precisato che tra l'autore del reato presupposto e la società è necessario che sussista una relazione funzionale a norma dell'art. 5, comma 1, lett. a) e b), del d.lgs. 8 giugno 2001, n. 231, e che la condotta della persona fisica sia conseguenza non tanto di un suo atteggiamento soggettivo, quanto di un preciso assetto organizzativo "negligente" dell'ente da intendersi in senso normativo, ossia non rispondente ai modelli di organizzazione e di gestione previsti dagli artt. 6 e 7 del citato d.lgs.*)"[99].

L'illecito dell'ente si struttura su una fattispecie complessa costituita sul piano oggettivo da tre elementi essenziali: la realizzazione di un reato, integrato nei suoi estremi oggettivi e soggettivi, la sua riferibilità a una persona che abbia un rapporto qualificato con l'ente e la sua commissione nell'interesse o a vantaggio dell'ente stesso (art. 5 d.lgs. n. 231/2001).

A questi elementi si aggiunge l'elemento soggettivo della colpa di organizzazione, diversamente connotato a seconda che il reato presupposto sia stato commesso da un soggetto in posizione apicale o sottoposto all'altrui vigilanza e direzione (artt. 6 e 7 d.lgs. n. 231/2001)[100].

Il sistema che configura la responsabilità amministrativa dell'ente (art. 5, d.lgs. n. 231 del 2001), richiede, infatti, che il reato debba essere stato commesso da persone che «rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso» (art. 5, lett. a, d.lgs. n. 231

[98] "Per l'impresa", osserva dal lato manageriale, V. D'IMPERIO, *Intelligenza artificiale e Modello 231: responsabilità, controlli ed evidenze*, in *Altalex*, 30/9/2026: "*il punto di attenzione è nei processi di comunicazione, marketing, gestione del personale e nei rapporti con chi pubblica per suo conto*. *Consenso, provenienza, approvazione e controllo prima della diffusione devono essere verificabili*".

[99] *Sez.* 5, 18/02/2025, n. 19096, Rv. 288138-01.

[100] Così in motivazione *Sez.* 4, 20/01/2026, n. 5357, Rv. 289479-01.

del 2001), oppure da persone «sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a» (art. 5, lett. b, d.lgs. n. 231 del 2001).

Occorre, inoltre, la rilevanza dell'interesse o del vantaggio dell'ente: "*La responsabilità da reato degli enti non può essere inferita dalla sola prova del reato presupposto, postulando invece, sul piano oggettivo, la realizzazione di un reato, integrato nei suoi estremi oggettivi e soggettivi, commesso nell'interesse o a vantaggio dell'ente da parte di una persona che abbia un rapporto qualificato con quest'ultimo, nonché, sul piano soggettivo, la colpa di organizzazione, diversamente connotata a seconda che il reato presupposto sia stato perpetrato da un soggetto in posizione apicale o sottoposto all'altrui vigilanza e direzione*"[101].

In sostanza, solo in presenza del legame soggettivo tra reo ed ente e quello teleologico tra reato ed ente è possibile configurare la responsabilità amministrativa, in quanto solo in presenza di tali legami si può ritenere che l'ente risponda per un fatto proprio e non per un fatto altrui.

La giurisprudenza di legittimità ha chiarito che la struttura dell'illecito addebitato all'ente risulta incentrata sul reato presupposto, rispetto al quale "*la relazione funzionale sussistente tra reo ed ente e quella teleologica tra reato ed ente hanno la funzione di irrobustire il rapporto di immedesimazione organica, escludendo che possa essere attribuito all'ente un reato commesso sì da un soggetto incardinato nell'organizzazione ma per fini estranei agli scopi di questo"*[102].

Muovendo da tali premesse, va dunque evidenziato come il rispetto dei requisiti di tracciabilità, *logging* e supervisione umana prescritti dal regolamento IA diventi il parametro fondamentale per valutare se l'ente sia incorso o meno una "**colpa di organizzazione**"[103].

Le aziende sono tenute a procedere ad un aggiornamento mirato del *risk assessment*, a mappare i sistemi utilizzati e a formalizzare protocolli stringenti per dimostrare chi eserciti la sorveglianza umana e se tale figura possieda il tempo e l'effettiva autorità per arrestare la macchina.

Come si è visto, l'art. 437-*bis* c.p. punisce anche la condotta colposa (in caso di *colpa grave*): l'inclusione di questa fattispecie nell'elenco dei reati presupposto (senza distinzioni tra dolo e colpa, a differenza di quanto avviene per la sicurezza sul lavoro o l'ambiente), estende il rischio per la responsabilità amministrativa alle condotte omissive colpose nella *governance* del rischio tecnologico[104].

---

[101] *Sez.* 6, 29/01/2025, n. 17664, Rv. 288143-01.
[102] Così *Sez.* 5, 18/02/2025, n. 19096, Rv. 288138–01 che richiama Sez. IV, 15 febbraio 2022, n. 18413, Rv. 283247-01 e Sez. IV, 8 gennaio 2021, n. 32899, Rv. 281997-02.
[103] Osserva M. FUMO, *Norme (para-)penali "in grigio" nella proposta riforma della 231,* in *Giust. ins*., 20/10/2026, criticando l'erronea collocazione della colpa di organizzazione quale elemento dell'illecito, che "*A ben vedere la «colpa di organizzazione», altro non è che una invenzione semantica, o se si vuole, una immaginifica concettualizzazione della colpa degli organizzatori, i quali, per negligenza, imprudenza, imperizia, inosservanza di leggi o regolamenti, hanno malamente organizzato l'ente e, per quel che qui interessa, hanno mal costruito (o addirittura omesso di costruire) il MOGC, ovvero non lo hanno correttamente applicato*", trattandosi dunque sempre di un "rimprovero" derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione dei reati previsti tra quelli idonei a fondare la responsabilità del soggetto collettivo, dovendo tali accorgimenti essere consacrati in un documento che individua i rischi e delinea le misure atte a contrastarli, come ricostruito da SU 24/04/2014, n. 38343, Rv. 261113-01.
[104] Vedi G.M. RICCIO, *d.lgs. 160/2026, cit*..

Ciò si allinea al concetto di "colpa di organizzazione" e obbliga le imprese a dimostrare di aver adottato modelli efficaci sia contro le alterazioni dolose, sia contro le carenze colpose di vigilanza: "*In tema di responsabilità da reato degli enti, la colpa di organizzazione ex art. 25-septies d.lgs. 8 giugno 2001, n. 231, riveste funzione analoga a quella della colpa afferente al reato commesso dalla persona fisica, risultando elemento costitutivo del fatto tipico, integrato dalla violazione rimproverabile della regola cautelare, la soddisfazione del cui onere probatorio grava sull'accusa, mediante la prova dell'immedesimazione organica rafforzata prevista dalla norma e della carenza del modello organizzativo, oltre che del reato presupposto e del nesso causale tra reato e comportamento dell'ente… proprio nel caso di responsabilità degli enti ritenuta in relazione a reati colposi di evento in violazione della normativa antinfortunistica, il S.C. ha precisato che la "colpa di organizzazione" deve intendersi in senso normativo ed è fondata sul rimprovero derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione dei reati previsti tra quelli idonei a fondare la responsabilità del soggetto collettivo, dovendo tali accorgimenti essere consacrati in un documento che individui i rischi e delinei le misure atte a contrastarli* »."[105].

Si ripropongono le problematiche già evidenziate a proposito della fattispecie colposa introdotta dal legislatore, dovendosi rilevare che nelle organizzazioni complesse rilevano i profili della programmazione e della corretta distribuzione delle competenze ma, non ultimo, quello degli obblighi formativi rispetto ai rischi derivanti dall'utilizzo dei sistemi.

4. Modifiche alla legislazione processuale per i profili risarcitori civili.

4.1. Introduzione agli artt. 16-20 del Capo II del Titolo II. Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale.

Il Capo II del Titolo II, rubricato «Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale», si compone di cinque articoli, gli artt. da 16 a 20, e contiene la parte del decreto legislativo specificamente dedicata alla tutela civile del soggetto danneggiato dall'utilizzo di un sistema di intelligenza artificiale.

Le disposizioni danno attuazione all'art. 24, comma 5, lett. d), della legge 23 settembre 2025, n. 132, che ha delegato il Governo a prevedere, nei casi di responsabilità civile, strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenendo conto della classificazione dei sistemi di intelligenza artificiale e degli obblighi individuati dal regolamento (UE) 2024/1689.

Il legislatore delegato non ha introdotto una fattispecie autonoma e unitaria di «responsabilità civile da intelligenza artificiale», né ha attribuito al sistema artificiale una soggettività giuridica o la qualità di autonomo centro di imputazione del danno. La responsabilità continua a essere riferita alle persone fisiche e agli enti coinvolti nella

[105] Sez. 4, *del* 25/06/2024, n. 31665, Rv. 286871–02; Sez. U, n. 38343 del 2014 cit., Rv. 261109-01

progettazione, nello sviluppo, nella produzione, nell'immissione sul mercato, nell'integrazione e nell'utilizzazione del sistema, secondo i diversi criteri di imputazione previsti dall'ordinamento. Le nuove disposizioni si innestano, pertanto, sulle fattispecie generali e speciali di responsabilità contrattuale ed extracontrattuale, incidendo soprattutto sul piano dell'accesso alle informazioni, della prova del nesso causale e dell'effettività della tutela risarcitoria.

La scelta legislativa muove dalla considerazione che le controversie relative all'intelligenza artificiale presentano difficoltà probatorie peculiari. La complessità tecnica dei sistemi, la possibile opacità dei processi che conducono dall'*input* all'*output*, la capacità di adattamento successiva alla messa in servizio e la distribuzione delle funzioni tra una pluralità di operatori (cd. "filiera tecnologica") possono rendere estremamente difficile individuare la causa del danno. A ciò si aggiunge che la documentazione tecnica, i registri delle operazioni, i dati di addestramento, le informazioni sul sistema di gestione dei rischi e quelle relative alla sorveglianza umana si trovano normalmente nella disponibilità del fornitore, del produttore, del *deployer* o di altri soggetti della filiera tecnologica, e non del danneggiato.

Il Capo II intende correggere questa asimmetria informativa senza trasformare ogni danno verificatosi in occasione dell'impiego di un sistema di intelligenza artificiale in una forma di responsabilità oggettiva. Il suo impianto è costruito attraverso una sequenza coordinata di strumenti: la delimitazione dell'ambito applicativo della disciplina; l'accesso agli elementi di prova detenuti dalla controparte o da terzi; la presunzione relativa del nesso causale; l'esclusione di qualsiasi efficacia automaticamente liberatoria della certificazione di conformità; infine, l'azione diretta del danneggiato nei confronti dell'impresa di assicurazione.

L'art. 16, rubricato «Ambito di applicazione e foro del consumatore», costituisce la disposizione generale del Capo II. Esso stabilisce che le norme sull'accesso alle prove contenute nell'art. 17 trovano applicazione nelle azioni di risarcimento del danno, tanto contrattuale quanto extracontrattuale, cagionato nell'utilizzo di un sistema di intelligenza artificiale. La formulazione adottata consente di ricomprendere non soltanto il danno direttamente prodotto da un *output* erroneo, ma anche quello derivante dall'integrazione del sistema in un processo decisionale od organizzativo, dall'omessa supervisione umana, dall'impiego di dati inadeguati, dalla configurazione non corretta del sistema o da un suo utilizzo difforme rispetto alla destinazione prevista.

La disposizione non individua uno specifico titolo di responsabilità. Restano quindi applicabili, secondo le caratteristiche della singola fattispecie, le regole in materia di responsabilità contrattuale, illecito aquiliano, esercizio di attività pericolose, danno cagionato da cose in custodia, responsabilità per fatto degli ausiliari e responsabilità da prodotto difettoso. L'ampiezza del riferimento alle azioni contrattuali ed extracontrattuali conferma che il legislatore ha inteso predisporre strumenti processuali trasversali, destinati a operare indipendentemente dalla qualificazione sostanziale della domanda.

Il comma 2 dell'art. 16 circoscrive, tuttavia, l'applicazione degli artt. 18 e 19 alle azioni nelle quali il danno sia derivato dalla violazione di uno o più obblighi previsti dal regolamento

(UE) 2024/1689. Ne deriva una differenza tra l'ambito dell'accesso alle prove e quello della presunzione causale: l'accesso previsto dall'art. 17 può essere richiesto in tutte le controversie risarcitorie relative all'utilizzo di un sistema di IA, mentre la presunzione dell'art. 18 presuppone la violazione di uno specifico obbligo regolatorio.

Il comma 3 reca una clausola di salvezza dei regimi speciali di derivazione eurounitaria. Restano ferme, in particolare, la disciplina dell'art. 82 del regolamento (UE) 2016/679, relativa al risarcimento del danno cagionato dal trattamento illecito dei dati personali, e la normativa nazionale di recepimento della direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi. La disposizione è diretta a evitare che il nuovo intervento determini una riduzione delle tutele già riconosciute o introduca un rapporto di specialità non espressamente previsto.

Il comma 4 completa la disposizione generale introducendo, in favore del danneggiato persona fisica che abbia agito per scopi estranei alla propria attività imprenditoriale, commerciale, artigianale o professionale, un foro territoriale "aggiuntivo", individuato nel luogo della residenza o del domicilio del danneggiato. Diversamente dal foro previsto dall'art. 66-*bis* del codice del consumo, il criterio non ha carattere esclusivo, ma si aggiunge ai fori competenti secondo i criteri ordinari, rafforzando la prossimità della tutela in controversie caratterizzate da particolare complessità tecnica.

L'art. 17, rubricato «Accesso alle prove», introduce lo strumento destinato a operare più direttamente sullo squilibrio informativo tra le parti. Su istanza del soggetto che allega di avere subito un danno, il giudice può ordinare alla controparte o al terzo che ne abbia la disponibilità l'esibizione degli elementi di prova specificamente pertinenti al funzionamento del sistema di intelligenza artificiale. L'ordine presuppone che l'istante abbia presentato fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche con riferimento al collegamento tra il risultato prodotto dal sistema e il danno lamentato.

Tra gli elementi probatori suscettibili di esibizione la norma indica, in via esemplificativa, i registri di registrazione automatica degli eventi, la documentazione relativa al sistema di gestione dei rischi, le informazioni contenute nella documentazione tecnica e quelle concernenti i parametri e le modalità della sorveglianza umana. Il legislatore valorizza così, in funzione probatoria, la documentazione che il regolamento IA impone agli operatori di formare e conservare per finalità di conformità, sicurezza e tracciabilità.

L'accesso non è, tuttavia, indiscriminato. L'ordine deve rispettare i principi di necessità e proporzionalità e deve tenere conto degli interessi delle parti e dei terzi, con particolare riguardo alla protezione dei segreti commerciali e delle informazioni riservate. Quando l'esibizione comporta il rischio di divulgazione di tali informazioni, il giudice è tenuto ad adottare le misure di tutela previste dall'art. 121-*ter* del codice della proprietà industriale, potendo circoscrivere l'accesso, oscurare parti dei documenti o adottare altre cautele idonee.

La norma attribuisce particolare rilevanza alle conseguenze derivanti dall'inadempimento dell'ordine. Dall'inosservanza ingiustificata il giudice può desumere argomenti di prova ai sensi dell'art. 116 c.p.c.; qualora l'inadempimento riguardi la documentazione regolatoria

specificamente indicata dal comma 2, il giudice può, previa valutazione degli altri elementi acquisiti, ritenere ammessi i fatti allegati dalla parte istante. Per il terzo che non ottemperi all'ordine è inoltre prevista una sanzione pecuniaria da euro 1.500 a euro 10.000.

L'art. 18, rubricato «Presunzione del nesso di causalità», interviene sul principale ostacolo probatorio delle controversie algoritmiche. Quando il danno deriva dalla violazione di uno o più obblighi previsti dal regolamento IA, il nesso causale tra la violazione e il danno è presunto, salva la prova contraria del convenuto. La presunzione ha quindi carattere relativo e incide soltanto sulla causalità: non esonera il danneggiato dalla prova dell'esistenza del danno e dell'obbligo violato, né introduce, in termini generali, una presunzione della colpa.

La disposizione intende evitare che l'opacità del funzionamento interno del sistema renda sostanzialmente impossibile la tutela risarcitoria. La presunzione non dovrebbe, tuttavia, operare in modo automatico per qualsiasi inosservanza del regolamento IA. Sarà necessario verificare che l'obbligo fosse applicabile al soggetto convenuto e al sistema utilizzato e, soprattutto, che fosse diretto a prevenire o ridurre il tipo di rischio concretizzatosi nell'evento dannoso. Soltanto tale correlazione consente di mantenere la presunzione entro una funzione propriamente eziologica, impedendo che una violazione meramente formale si trasformi in un'automatica imputazione del danno.

L'art. 19, rubricato «Rilevanza della conformità del sistema di intelligenza artificiale», precisa che la conformità del sistema agli obblighi del regolamento (UE) 2024/1689, anche quando attestata attraverso le procedure di certificazione previste dal medesimo regolamento, non esclude di per sé la responsabilità del danneggiante. La norma distingue pertanto il piano della conformità amministrativa e regolatoria da quello della responsabilità civile: la certificazione non costituisce una causa automatica di esonero, perché il danno può dipendere dalle modalità concrete di configurazione, integrazione, aggiornamento, sorveglianza o utilizzazione del sistema.

La conformità conserva, nondimeno, valore nel complessivo accertamento giudiziale. Essa potrà concorrere alla valutazione della diligenza osservata dall'operatore e delle cautele adottate, senza precludere al giudice di verificare se, nelle specifiche circostanze del caso, fossero esigibili misure ulteriori o se il sistema, pur formalmente conforme, sia stato impiegato in modo negligente, improprio o non coerente con la propria destinazione.

L'art. 20, infine, introduce l'«Azione diretta nei confronti dell'impresa di assicurazione». La disposizione consente al danneggiato di agire direttamente contro l'impresa che assicura la responsabilità civile per i danni cagionati nell'utilizzo di sistemi di intelligenza artificiale, nei limiti delle somme per le quali è stata stipulata la copertura. Il modello è quello già sperimentato nella responsabilità civile derivante dalla circolazione dei veicoli, ma viene qui esteso alle controversie risarcitorie relative all'utilizzo dei sistemi di IA.

Prima dell'instaurazione del giudizio, il danneggiato può chiedere al soggetto che intende convenire di comunicare l'esistenza di una copertura assicurativa, gli estremi del contratto e la denominazione dell'impresa assicuratrice. La comunicazione deve intervenire entro trenta giorni; la sua omissione o incompletezza può essere valutata dal giudice come argomento di

prova ai sensi dell'art. 116 c.p.c. La richiesta preventiva non costituisce, tuttavia, condizione di procedibilità della domanda.

L'impresa assicuratrice può opporre al danneggiato le eccezioni derivanti dal contratto antecedenti al sinistro e conserva il diritto di rivalsa nei confronti dell'assicurato nei casi in cui avrebbe avuto titolo per rifiutare o ridurre la prestazione. Nel giudizio promosso direttamente contro l'assicuratore deve essere chiamato anche il soggetto individuato come responsabile del danno, in qualità di litisconsorte necessario. Il termine di prescrizione dell'azione diretta coincide con quello applicabile all'azione esercitabile nei confronti del responsabile.

Nel loro insieme, gli artt. 16-20 delineano dunque una disciplina prevalentemente processuale, destinata a rendere effettiva la tutela risarcitoria senza sostituire i tradizionali criteri sostanziali di responsabilità. Il sistema di tutele introdotto dal legislatore si fonda sulla complementarità tra accesso alle prove, agevolazione della prova del nesso eziologico, piena valutabilità della condotta nonostante la certificazione di conformità e rafforzamento della garanzia patrimoniale attraverso l'azione diretta contro l'assicuratore.

Il punto di equilibrio perseguito dal legislatore consiste nell'impedire che la complessità e l'opacità tecnologica rendano impossibile l'accertamento del danno, senza per questo costruire una responsabilità indifferenziata di tutti gli operatori della filiera. Rimangono pertanto centrali l'individuazione del titolo sostanziale azionato, la riferibilità degli obblighi al singolo operatore, l'accertamento del contributo causale delle diverse condotte e, nell'ipotesi di concorso di più responsabili, l'eventuale applicazione dell'art. 2055 c.c..

Su tali aspetti è prevedibile che assuma particolare rilievo l'elaborazione della giurisprudenza di legittimità, chiamata a precisare il rapporto tra la disciplina speciale e le categorie generali della responsabilità civile, la soglia di verosimiglianza necessaria per accedere alle prove, l'ambito della presunzione causale, il valore della conformità regolatoria e le condizioni per imputare unitariamente un danno che costituisca l'esito dell'interazione tra difetto tecnologico, carenza organizzativa, insufficienza della sorveglianza umana e condotta dell'utilizzatore.

4.1.1. Il d.lgs. 9 settembre 2026, n. 160. Premessa.

Come già evidenziato, il d.lgs. n.160 del 2026 è stato adottato in attuazione delle deleghe conferite dall'**art. 24** della **legge IA**. Con specifico riguardo alla **responsabilità civile**, la legge delega ha previsto l'introduzione di strumenti di tutela del danneggiato, anche mediante una regolamentazione dei criteri di ripartizione dell'onere della prova, che tenga conto della classificazione dei sistemi di intelligenza artificiale e degli obblighi stabiliti dal regolamento europeo.

In questa parte la presente relazione, incentrata sugli aspetti civilistici, prende in esame tanto gli interventi che incidono sui criteri sostanziali di imputazione della responsabilità quanto le disposizioni che, sul piano processuale, introducono strumenti diretti ad agevolare l'accertamento dei fatti, l'accesso alle informazioni nella disponibilità degli operatori della

filiera tecnologica e la prova del rapporto causale tra l'utilizzo del sistema di intelligenza artificiale e il danno lamentato.

L'intervento normativo si colloca all'interno di un quadro regolatorio composito, nel quale convergono fonti europee e nazionali aventi oggetto e funzioni differenti. Vengono anzitutto in rilievo il **regolamento (UE) 2024/1689**, che stabilisce regole armonizzate in materia di intelligenza artificiale secondo un modello fondato sulla classificazione e sulla prevenzione dei rischi, e la **direttiva (UE) 2024/2853**, relativa alla responsabilità per danno da prodotti difettosi. A tali fonti si affiancano **la legge n**. **132** del **2025** e, per effetto del decreto legislativo in esame, le disposizioni specificamente destinate a regolare le conseguenze civili della realizzazione e dell'impiego illecito dei sistemi di intelligenza artificiale. Il preambolo del decreto richiama espressamente, oltre al regolamento sull'intelligenza artificiale e alla direttiva sui prodotti difettosi, l'**art. 116 c.p.c.** e gli **artt. 2050** e **2051** c.c., così evidenziando la necessità di coordinare la nuova disciplina con le regole generali in materia di valutazione della prova, e di responsabilità da esercizio di attività pericolose e da cose in custodia.

Il **d.lgs. n. 160 del 2026** muove dalla considerazione che l'impiego dei sistemi di intelligenza artificiale può determinare difficoltà di accertamento non pienamente riconducibili a quelle proprie delle "ordinarie controversie risarcitorie". La complessità tecnica dei sistemi, la distribuzione delle funzioni tra una pluralità di operatori, la possibile opacità dei processi attraverso i quali il sistema produce un determinato risultato e la concentrazione delle informazioni rilevanti nella sfera di disponibilità dei soggetti che progettano, forniscono o utilizzano professionalmente il sistema possono, infatti, determinare una significativa asimmetria informativa tra le parti del giudizio.

In tale prospettiva, la disciplina introdotta dal decreto non configura il sistema di intelligenza artificiale come **autonomo centro di imputazione giuridica**. La responsabilità continua a essere riferita alle persone fisiche e agli enti coinvolti nella realizzazione, nella messa in circolazione e nell'utilizzazione del sistema, secondo i criteri di imputazione stabiliti dall'ordinamento. L'autonomia tecnica od operativa del sistema non vale, pertanto, a interrompere necessariamente la relazione tra il danno e le condotte umane od organizzative che hanno concorso alla sua produzione, ma rende più complessa l'individuazione delle condotte giuridicamente rilevanti e la ricostruzione del relativo apporto causale. La portata innovativa dell'intervento deve essere apprezzata, in primo luogo, sul piano del raccordo tra la disciplina preventiva posta dal regolamento europeo e le regole della responsabilità civile. Gli obblighi concernenti la gestione del rischio, la qualità e la governance dei dati, la documentazione tecnica, la registrazione degli eventi, la trasparenza e la sorveglianza umana sono dettati dal regolamento in funzione della sicurezza e della conformità dei sistemi. La loro osservanza o violazione può, tuttavia, assumere rilievo anche nel giudizio risarcitorio, concorrendo alla definizione della condotta esigibile, alla ricostruzione del rischio prevedibile e all'individuazione dei fatti rilevanti ai fini dell'imputazione del danno.

Il decreto legislativo, con la sua disciplina, impone la necessità del **coordinamento** tra le nuove disposizioni e le fattispecie di responsabilità disciplinate dal codice civile. Il

riferimento, nel preambolo del d.lgs., agli **artt. 2050 e 2051 c.c.** rende necessario verificare, da un lato, a quali condizioni la produzione, la messa in circolazione o l'impiego professionale di un sistema di intelligenza artificiale possano essere ricondotti all'esercizio di un'attività pericolosa e, dall'altro, se e in quale misura la crescente autonomia operativa del sistema sia compatibile con la relazione di custodia presupposta dall'art. 2051 c.c..

Si pone altresì la questione problematica del rapporto tra la disciplina generale dell'illecito aquiliano e quella della responsabilità per danno da prodotto difettoso, rispetto alla quale la **direttiva (UE) 2024/2853** assume specifica rilevanza per i prodotti caratterizzati da componenti digitali e per il software. Uno dei principali nuclei problematici della nuova disciplina attiene al rapporto tra la violazione degli obblighi imposti agli operatori e l'accertamento del nesso causale. La non conformità del sistema o l'inosservanza degli obblighi di gestione, controllo, documentazione e trasparenza non possono confondersi con la prova del danno né con quella della sua derivazione causale. Occorre, pertanto, distinguere la violazione della regola di condotta, quale possibile presupposto della responsabilità, dall'accertamento che il danno lamentato costituisca conseguenza dell'impiego del sistema o della specifica inosservanza contestata. Analogo rilievo assume la disciplina dell'onere della prova. Gli strumenti introdotti dal legislatore sono diretti a correggere lo squilibrio informativo esistente tra il danneggiato e i soggetti che dispongono della documentazione tecnica e dei dati necessari alla comprensione del funzionamento del sistema. Essi non esimono, tuttavia, il giudice dall'individuare i fatti costitutivi della pretesa e dal verificare, in relazione alla concreta fattispecie, i presupposti applicativi delle regole di agevolazione probatoria. Dovrà, in particolare, essere chiarito se tali regole incidano soltanto sulla prova del rapporto eziologico ovvero anche sulla dimostrazione della condotta, della colpa e della riferibilità del sistema al soggetto convenuto. Sotto il profilo processuale, assumono rilievo l'accesso alla documentazione tecnica e agli altri elementi conoscitivi nella disponibilità degli operatori, il rapporto tra ordine di esibizione e tutela delle informazioni riservate, gli effetti processuali dell'inosservanza dei provvedimenti giudiziali e il ruolo della consulenza tecnica. Quest'ultima, avuto riguardo alla particolare complessità delle controversie, potrà risultare frequentemente necessaria per la ricostruzione del funzionamento del sistema e delle condizioni nelle quali esso è stato utilizzato. Resta, tuttavia, ferma la distinzione tra l'accertamento tecnico dei fattori che hanno concorso alla produzione del risultato e la valutazione giuridica della loro rilevanza causale, riservata al giudice.

Le disposizioni civilistiche del d.lgs. n. 160 del 2026 verranno, dunque, esaminate secondo una duplice direttrice. Saranno dapprima analizzate le norme sostanziali e il loro coordinamento con i modelli di responsabilità previsti dal codice civile e dalla disciplina europea del prodotto difettoso. Verranno poi esaminati gli strumenti processuali predisposti a tutela del danneggiato, con particolare riguardo all'accesso alla prova, alle regole di ripartizione dell'onere probatorio, all'accertamento del nesso causale e alle misure dirette ad assicurare l'effettività della tutela risarcitoria. L'indagine sarà condotta con specifica attenzione alle questioni suscettibili di assumere rilievo nell'attività nomofilattica: la

delimitazione dell'ambito applicativo delle nuove disposizioni; l'individuazione dei soggetti responsabili lungo la filiera tecnologica; la qualificazione delle attività connesse alla realizzazione e all'impiego dei sistemi; il rapporto tra conformità regolatoria e responsabilità civile; l'operatività delle presunzioni; il coordinamento tra le regole speciali e i principi generali in materia di prova e causalità; la tutela della riservatezza e dei segreti commerciali nell'acquisizione della documentazione tecnica.

La novità dell'intervento e la mancanza, allo stato, di un'elaborazione giurisprudenziale consolidata impongono un esame che, muovendo dal dato testuale e dal sistema delle fonti, individui le prime opzioni interpretative senza anticipare soluzioni non ancora "verificate" nella prassi applicativa. In questa prospettiva, la relazione intende offrire una prima ricognizione ragionata della disciplina e dei suoi possibili riflessi sul contenzioso civile, segnalando le questioni sulle quali potrà rendersi necessario l'intervento chiarificatore della giurisprudenza di legittimità.

4.2. Il quadro normativo europeo ed interno.

4.2.1. La dichiarazione comune sui diritti e i principi digitali e la Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto, adottata il 13 maggio 2026.

Il 5.12.2022 il Parlamento europeo, il Consiglio e la Commissione hanno proclamato solennemente **la Dichiarazione comune sui diritti e i principi digitali per il decennio digitale**. L'obiettivo della dichiarazione è definire i diritti dei cittadini nello spazio digitale ed elaborare un quadro di principi che l'UE e gli Stati membri convengono di sostenere nel processo di trasformazione digitale. Nel **considerando n.4** della Dichiarazione si afferma che "*Il Parlamento ha invitato più volte a definire principi etici che guidino l'approccio dell'UE alla trasformazione digitale e garantiscano il pieno rispetto dei diritti fondamentali quali la protezione dei dati, il diritto al rispetto della vita privata, la non discriminazione e la parità di genere, nonché di principi quali la protezione dei consumatori, la neutralità tecnologica e della rete, l'affidabilità e l'inclusività. Ha inoltre chiesto una maggiore protezione dei diritti degli utenti nell'ambiente digitale, nonché dei diritti dei lavoratori e del diritto alla disconnessione*" mentre nel **capitolo I**, **art. 1** della Dichiarazione, si afferma che "*Le persone sono al centro della trasformazione digitale nell'Unione europea.* ***La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali***". Le Istituzioni europee si impegnano nella dichiarazione [106] a: "*a) rafforzare il quadro democratico per una trasformazione digitale che vada a beneficio di ogni persona e migliori la vita tutte le persone che vivono nell'UE; b) adottare le misure necessarie per garantire che i valori dell'UE e i diritti delle persone riconosciuti dal diritto dell'Unione siano rispettati online così come offline; c) promuovere e garantire un'azione*

[106] Capitolo I "Mettere le persone al centro della trasformazione digitale".

responsabile e diligente da parte di tutti gli attori, pubblici e privati, nell'ambiente digitale; d) promuovere attivamente questa visione della trasformazione digitale, anche nelle relazioni internazionali.".

Come già in precedenza evidenziato, l'impegno dell'UE è, quindi, a favore di una trasformazione digitale "**sicura, sostenibile e protetta che ponga le persone al centro**" e che sia in linea con i valori e i diritti fondamentali posti alla base dell'Unione Europea. La dichiarazione impegna altresì gli Stati Membri a garantire una trasformazione digitale che miri all'inclusione, all'accessibilità, all'uguaglianza, alla sostenibilità, alla resilienza, alla sicurezza, al miglioramento della qualità della vita, alla disponibilità di servizi e al rispetto dei diritti e delle aspirazioni di ognuno. La Dichiarazione fa prendere specifici impegni alle Istituzioni comunitarie anche con riguardo all'utilizzo delle intelligenze artificiali. Gli **artt. 8** e **9** del **Capitolo III** prevedono che "*L'intelligenza artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano*" e che "*Ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dai sistemi algoritmici e di intelligenza artificiale, anche compiendo le proprie scelte informate nell'ambiente digitale, e* ***rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali***.". Le Istituzioni europee si impegnano[107] di conseguenza a: "*a) promuovere sistemi di intelligenza artificiale antropocentrici, affidabili ed etici nell'intero corso del loro sviluppo, della loro diffusione e del loro utilizzo, in linea con i valori dell'UE; b) garantire un livello adeguato di trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e fare in modo che le persone siano autonome e responsabili quando li utilizzano e informate quando interagiscono con essi; c) garantire che i sistemi algoritmici siano basati su insiemi di dati adeguati al fine di evitare discriminazioni e consentano la supervisione umana di tutti i risultati che interessano la sicurezza e i diritti fondamentali delle persone; d) garantire che le tecnologie come l'intelligenza artificiale non siano utilizzate per pregiudicare le scelte delle persone, ad esempio per quanto riguarda la salute, l'istruzione, l'occupazione e la vita privata;* ***e) prevedere garanzie e adottare misure adeguate, anche promuovendo norme affidabili, al fine di assicurare che, in ogni momento, l'intelligenza artificiale e i sistemi digitali siano sicuri e vengano utilizzati nel pieno rispetto dei diritti fondamentali****; f) adottare misure per garantire che la ricerca sull'intelligenza artificiale rispetti i più elevati principi etici e il diritto pertinente dell'UE.*".

La **Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto**, adottata il 13 maggio 2026, mira a garantire, attraverso la cooperazione tra gli Stati aderenti, che le attività svolte durante il ciclo di vita dei sistemi di intelligenza artificiale siano compatibili con i diritti umani, la democrazia e lo Stato di diritto. L'adozione della Convenzione segna una tappa fondamentale nel processo di costruzione di un diritto internazionale dell'intelligenza artificiale. Per la prima volta, infatti, il Consiglio d'Europa ha elaborato uno strumento giuridicamente vincolante

[107] Capitolo III Libertà di scelta, Interazioni con algoritmi e sistemi di intelligenza artificiale.

destinato a porre principi comuni per la regolazione dell'**intero ciclo di vita dei sistemi di IA**, non limitandosi agli aspetti economici o tecnologici della loro utilizzazione, ma assumendo come punto di riferimento la tutela della persona, la salvaguardia delle istituzioni democratiche e la protezione dello Stato di diritto. Tale scelta metodologica appare particolarmente significativa perché colloca il fenomeno dell'intelligenza artificiale all'interno della tradizione giuridica europea dei diritti fondamentali. Mentre il dibattito pubblico è stato spesso caratterizzato dall'alternativa tra promozione dell'innovazione e contenimento dei rischi tecnologici, la Convenzione sceglie una strada differente: l'intelligenza artificiale non viene considerata come un semplice prodotto da regolare né come una minaccia da contenere, ma come una tecnologia che deve essere sviluppata e utilizzata secondo parametri compatibili con la dignità della persona e con i valori democratici. All' **art. 9**[108] della Convenzione le parti si impegnano, infatti, ad adottare o mantenere in vigore misure volte a garantire la "*responsabilizzazione*" e la "*responsabilità*" per gli impatti negativi sui diritti umani, sulla democrazia e sullo Stato di diritto derivanti dalle attività che rientrano nel ciclo di vita dei sistemi di intelligenza artificiale, nonché ad adottare, all'**art.12**[109], le misure più adeguate per promuovere l'affidabilità dei sistemi di intelligenza artificiale e "*la fiducia negli output da essi prodotti, che potrebbero includere requisiti relativi a una qualità e una sicurezza adeguate durante l'intero ciclo di vita dei sistemi di intelligenza artificiale*.". La Convenzione impone poi, all'**art. 20**[110], agli Stati di implementare **l'alfabetizzazione** e **le competenze digitali** di ogni segmento della popolazione nonché le "*competenze specialistiche specifiche per i responsabili dell'individuazione, della valutazione, della prevenzione e dell'attenuazione dei rischi presentati dai sistemi di intelligenza artificiale*". È compito poi degli Stati prevedere misure che mirino a prevenire ed attenuare i rischi derivanti dall'utilizzo di sistemi di intelligenza artificiale (**art. 16**[111]) quando questi ultimi possono mettere a repentaglio i diritti fondamentali della persona e la vita democratica di ogni Paese firmatario.

---

[108] Art. 9: "Ciascuna parte adotta o mantiene in vigore misure volte a garantire la responsabilizzazione e la responsabilità per gli impatti negativi sui diritti umani, sulla democrazia e sullo Stato di diritto derivanti dalle attività che rientrano nel ciclo di vita dei sistemi di intelligenza artificiale.

[109] Art. 12 della Convenzione: "Ciascuna parte adotta, se del caso, misure volte a promuovere l'affidabilità dei sistemi di intelligenza artificiale e la fiducia negli output da essi prodotti, che potrebbero includere requisiti relativi a una qualità e una sicurezza adeguate durante l'intero ciclo di vita dei sistemi di intelligenza artificiale.".

[110] Art. 20 della Convenzione: "Ciascuna parte incoraggia e promuove un'alfabetizzazione e delle competenze digitali adeguate per tutti i segmenti della popolazione, comprese competenze specialistiche specifiche per i responsabili dell'individuazione, della valutazione, della prevenzione e dell'attenuazione dei rischi presentati dai sistemi di intelligenza artificiale.".

[111] Art. 16 della Convenzione: "Ciascuna parte, tenendo conto dei principi di cui al capo III, adotta o mantiene in vigore misure volte all'individuazione, alla valutazione, alla prevenzione e all'attenuazione dei rischi posti dai sistemi di intelligenza artificiale, prendendo in considerazione gli impatti effettivi e potenziali sui diritti umani, sulla democrazia e sullo Stato di diritto. 2.Tali misure sono graduate e differenziate, se del caso, e: a) tengono debitamente conto del contesto e dell'uso previsto dei sistemi di intelligenza artificiale, in particolare per quanto riguarda i rischi per i diritti umani, la democrazia e lo Stato di diritto; b) tengono debitamente conto della probabilità che si verifichino potenziali impatti e della relativa gravità; c) prendono in considerazione, se del caso, i punti di vista dei pertinenti portatori di interessi, in particolare delle persone i cui diritti possono essere colpiti; d) si applicano iterativamente a tutte le attività che rientrano nel ciclo di vita del sistema di intelligenza artificiale; e) comprendono il monitoraggio dei rischi e degli impatti negativi per i diritti umani, la democrazia e lo Stato di diritto; f) comprendono la documentazione dei rischi, degli impatti effettivi e potenziali e dell'approccio alla gestione dei rischi; e g) richiedono, se del caso, che i sistemi di intelligenza artificiale siano sottoposti a prova prima di essere messi a disposizione per il primo utilizzo e qualora siano modificati in modo significativo. 3.Ciascuna parte adotta o mantiene in vigore misure volte a garantire che gli impatti negativi dei sistemi di intelligenza artificiale sui diritti umani, sulla democrazia e sullo Stato di diritto siano affrontati in modo adeguato. Tali impatti negativi e le misure per affrontarli dovrebbero essere documentati e orientare le pertinenti misure di gestione dei rischi di cui al paragrafo 2.4. Ciascuna parte valuta la

Questa Convenzione costituisce, quindi, il primo strumento internazionale giuridicamente vincolante volto a disciplinare l'uso dell'intelligenza artificiale mediante una prospettiva incentrata sui diritti fondamentali, sulla tutela delle istituzioni democratiche e sulla salvaguardia dello Stato di diritto. La Convenzione assume particolare rilievo perché, pur non introducendo una disciplina uniforme della responsabilità civile né un autonomo regime risarcitorio, individua una serie di principi destinati a fungere da criteri interpretativi e parametri di conformazione delle future legislazioni nazionali e sovranazionali.

I principi stabiliti dalla **Dichiarazione** e dalla **Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto** stanno "guidando" il legislatore europeo e gli Stati membri nella preparazione e successiva emanazione dei regolamenti e delle direttive nei settori interessati dalla trasformazione digitale nonché le leggi interne di adeguamento a queste ultime.

Per quel concerne, più specificamente, la regolamentazione dei sistemi di intelligenza artificiale è entrato in vigore il **Regolamento UE 2024/1689** («**Regolamento IA**»), da ultimo modificato dal **Regolamento (UE) 2026/1744** (il c.d. «**Digital Omnibus sull'IA**»), ed è stata approvata la **legge 23 settembre 2025, n. 132**, recante «*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*», cui ha fatto seguito il primo decreto attuativo di rilievo processuale e sostanziale nel settore civile, il d.lgs. n. 160, vigente dal 30 settembre 2026.

4.2.2. Il Regolamento (UE) 2024/1689.

Il **Regolamento (UE) 2024/1689,** Regolamento IA, del Parlamento europeo e del Consiglio, del 13 giugno 2024, ha istituito il primo quadro giuridico organico sull'intelligenza artificiale a livello sovranazionale (il c.d. AI Act)[112], promuovendo un'IA **antropocentrica** e **affidabile**[113]. Il Regolamento sull'IA definisce, all'**art. 3, comma 1, n. 1**, l'Intelligenza Artificiale come "*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*".

necessità di una moratoria, di un divieto o di altre misure appropriate in relazione a determinati usi dei sistemi di intelligenza artificiale qualora ritenga che tali usi siano incompatibili con il rispetto dei diritti umani, il funzionamento della democrazia o lo Stato di diritto.

[112] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (*AI Act*), in particolare artt. 4, 5, 6, 8-15, 26, 27, 50, 57, 59, 86, 113 e All. II e III (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689).

[113] Articolo 1, Oggetto, del regolamento IA cit.: " 1. Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione. 2. Il presente regolamento stabilisce: a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione; b) divieti di talune pratiche di IA; c) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi; d) regole di trasparenza armonizzate per determinati sistemi di IA; e) regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali; f) regole in materia di monitoraggio del mercato, vigilanza del mercato, governance ed esecuzione; g) misure a sostegno dell'innovazione, con particolare attenzione alle PMI, comprese le start-up.".

Date le avanzate capacità che tali sistemi presentano, e che li rendono capaci di funzionare in maniera autonoma elaborando simultaneamente ingenti quantità di dati e producendo diversi tipi di *output* a seconda della richiesta effettuata dall'utilizzatore, il provvedimento unionale sceglie di adoperare una definizione volutamente ampia, accompagnata da un approccio orizzontale basato sul rischio, al fine di ricomprendere all'interno delle sue maglie più tipologie possibili di sistemi di IA. Il regolamento IA adotta un approccio basato sul rischio, distinguendo tra **pratiche vietate**, **sistemi ad alto rischio**, **sistemi soggetti a obblighi di trasparenza e sistemi a rischio minimo**[114]. Si vuole garantire un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, inclusi democrazia, Stato di diritto e ambiente, e favorire l'innovazione e la libera circolazione dei prodotti e servizi basati su sistemi di intelligenza artificiale. Il regolamento si fonda sui valori dell'Unione sanciti dalla **Carta dei diritti fondamentali**[115], promuovendo la protezione delle persone, delle imprese, della democrazia, dello Stato di diritto e dell'ambiente. L'IA, secondo il regolamento, deve essere antropocentrica, cioè al servizio delle persone, e sviluppata nel rispetto dei diritti e delle libertà fondamentali. Il regolamento, in particolare, prevede che alcune pratiche di IA sono vietate (rischio inaccettabile), altre sono soggette a requisiti stringenti (alto rischio), come il settore giudiziario, altre ancora sono soggette solo ad obblighi di trasparenza. I sistemi di IA ad alto rischio sono quelli che possono avere un impatto significativo su salute, sicurezza o diritti fondamentali delle persone. Sono vietati[116]

---

[114] E. Borghetto, *Utilizzo dei sistemi di IA: conseguenze processuali e regimi di responsabilità*, in Danno e Responsabilità, n. 5, 1° settembre 2026, p. 555.

[115] Considerando 1 del regolamento IA cit.: "Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno 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) nell'Unione, in conformità dei valori dell'Unione, 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 («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento".

[116] Art.5, paragrafo 1, sono vietate le seguenti pratiche di IA: a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo;
b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo; c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: - un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; - un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;
d) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa; e) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping*

sistemi di IA che manipolano il comportamento umano in modo subliminale o ingannevole, che sfruttano la vulnerabilità di persone o gruppi, che attribuiscono punteggi sociali, che fanno *scraping* di dati biometrici per il riconoscimento facciale, che inferiscono emozioni in contesti lavorativi o scolastici, o che usano identificazione biometrica remota in tempo reale salvo eccezioni rigorose. Sono considerati ad alto rischio[117], ancora, i sistemi di IA usati in ambiti come: biometria, infrastrutture critiche, istruzione, occupazione, accesso a servizi essenziali, attività di contrasto, migrazione, giustizia, processi democratici, ecc. Tali sistemi devono rispettare requisiti di gestione del rischio, qualità dei dati, documentazione tecnica, trasparenza, sorveglianza umana, accuratezza, robustezza e cibersicurezza. Il regolamento sottolinea la centralità della tutela dei diritti fondamentali, inclusi la non discriminazione, la protezione dei dati personali, la libertà di espressione, la presunzione di innocenza, la protezione dei minori e la parità di genere. Viene richiesto dal regolamento IA che i sistemi di IA ad alto rischio siano progettati e utilizzati in modo da prevenire rischi per i diritti fondamentali e che siano previste valutazioni d'impatto specifiche. Viene istituito un sistema di governance multilivello: autorità nazionali, un Ufficio europeo per l'IA, un Consiglio europeo per l'IA, un forum consultivo e un gruppo di esperti scientifici. Sono previste sanzioni severe per le violazioni, fino al 7% del fatturato mondiale per le pratiche vietate. Il regolamento promuove l'innovazione responsabile, prevede spazi di sperimentazione normativa (*sandbox*) e misure di sostegno specifiche per PMI e start-up. Sono introdotte regole specifiche per i modelli di IA per finalità generali (come i grandi modelli linguistici), con obblighi di trasparenza, documentazione tecnica, gestione dei rischi sistemici e rispetto del diritto d'autore. La Commissione europea dovrà monitorare e aggiornare periodicamente l'elenco dei

non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso; f) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza; g) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di *set* di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto; h) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti: - la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; - 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; - la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

[117] L'articolo 6 del regolamento IA cit. stabilisce che un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: - il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; - il prodotto, il cui componente di sicurezza di cui sopra è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.
Il medesimo articolo, al paragrafo 2, include tra i sistemi di IA ad alto rischio anche quelli indicati nell'Allegato III. Nel rinviare a tale allegato, si segnala che i settori in cui rientrano tali sistemi sono quelli riguardanti: la biometria; le infrastrutture critiche; l'istruzione e la formazione professionale; l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo; l'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e la fruizione degli stessi; le attività di contrasto; la migrazione, l'asilo e la gestione del controllo delle frontiere; l'amministrazione della giustizia e i processi democratici.

sistemi ad alto rischio e delle pratiche vietate, tenendo conto dell'evoluzione tecnologica e sociale.

La definizione delle attività in base al rischio discende direttamente dalla scelta legislativa di fondo di definire gli obblighi in materia di intelligenza artificiale mediante l'approccio basato sul rischio (*Risk based approach- RBA*). Il *risk-based approach* è la tecnica regolatoria trasversale per cui la conformità è graduata in funzione della probabilità, gravità e prevedibilità del pregiudizio, imponendo al destinatario una valutazione preventiva, documentata e aggiornata dei rischi e delle misure di mitigazione. Esso trae la sua origine in altri settori dell'ordinamento unionale, ed in particolare nei settori dell'antiriciclaggio e nel GDPR. Nel regolamento IA il RBA assume, come si è visto, forma strutturata: i sistemi di IA sono classificati in vietati, ad alto rischio, a trasparenza specifica e a rischio minimo, e per quelli ad alto rischio è richiesto un sistema di gestione del rischio che identifichi e analizzi i rischi noti e ragionevolmente prevedibili, anche da usi impropri, stimi e valuti tali rischi, adotti misure adeguate di trattamento e utilizzi il monitoraggio post-commercializzazione per aggiornare l'analisi. La verifica di conformità non si esaurisce nella qualificazione formale, ma richiede documentazione tecnica, qualità dei dati, supervisione umana, accuratezza, robustezza, *cybersecurity*, valutazione di conformità e, per i *deployer* interessati, valutazione d'impatto sui diritti fondamentali. In questa prospettiva, il RBA si configura come un principio di *accountability*: l'organizzazione deve dimostrare di aver adottato misure ragionevolmente esigibili, coerenti con il rischio residuo e controllate nel tempo. L'approccio basato sul rischio si va pertanto sempre più configurando come un istituto di carattere generale, dell'ordinamento unionale e nazionale[118].

Fatte queste premesse in ordine alle novità introdotte dal regolamento in tema di impiego dei sistemi di IA va rilevato che esso non introduce una disciplina europea unitaria della responsabilità civile ma si limita a regolare, come già accennato, **l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA attraverso un sistema di obblighi pubblicistici e di gestione del rischio**. La responsabilità civile resta in larga misura affidata agli ordinamenti nazionali. Il **considerando 9**[119] del regolamento afferma che quest'ultimo è

---

[118] P. FALLETTA - A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di informatica e diritto, 1/2024*, https://irinsubria.uninsubria.it/bitstream/11383/2173251/1/0155_RIID_2024_01Falletta.pdf. Oltre all'AI Act, il RBA opera nel GDPR (misure adeguate, privacy by design/by default, DPIA (Garante per la protezione dei dati personali, Relazione annuale 2024. [garanteprivacy](https://www.garanteprivacy.it/garante/document?ID=10149391), nel d.lgs. n. 231/2001 (modelli organizzativi calibrati sui reati-presupposto e sulle aree sensibili), nel d.lgs. n. 81/2008 (valutazione dei rischi per la salute e sicurezza), nel DSA (Data Servicies Act), nelle normative antiriciclaggio (adeguata verifica e controlli graduati) e nelle discipline di *cybersecurity* e sicurezza dei prodotti. La giurisprudenza declina il RBA (che raramente è preso in considerazione autonomamente al di fuori della disciplina antiriciclaggio ed in parte del GDPR) soprattutto attraverso i principi di *accountability*, proporzionalità ed effettività:
Corte Giustizia UE Sez. III, 14 dicembre 2023, n. 340, https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=576757. Cfr. anche Cass. civ., Sez. I, 7 maggio 2025, n. 12034; Cass. civ., Sez. I, 11 ottobre 2023, n. 28385. La giurisprudenza si concentra sulla valutazione dell'idoneità delle misure adottate per valutare la responsabilità ed il suo grado. È chiaro che si tratta di uno dei casi in cui la principale difficoltà deriva dalla valutazione a posteriori, rispetto al verificarsi del danno, e dalla misurazione della proporzionalità.

[119] Considerando 9 del regolamento IA cit.: "È opportuno che le norme armonizzate applicabili all'immissione sul mercato, alla messa in servizio e all'uso di sistemi di IA ad alto rischio siano stabilite conformemente al regolamento (CE) n, 765/2008 del Parlamento europeo e del Consiglio (…), alla decisione n, 768/2008/CE del Parlamento europeo e del Consiglio ((UE) 2019/1020 del Parlamento europeo e del Consiglio e al regolamento («nuovo quadro legislativo»). Le norme armonizzate stabilite nel presente regolamento dovrebbero applicarsi in tutti i settori e, in

complementare rispetto alle discipline esistenti in materia di tutela dei consumatori, sicurezza dei prodotti, diritti fondamentali e protezione dei dati; lascia impregiudicati ("*remain unaffected and fully applicable*") tutti i rimedi già previsti dal diritto dell'Unione, compreso il risarcimento del danno; precisa, poi, che gli obblighi posti dal regolamento IA operano" *without prejudice to national law*", purché compatibile con il diritto dell'Unione. Deve ritenersi, quindi, che il legislatore unionale non ha voluto armonizzare le regole risarcitorie, lasciando spazio alla legislazione dei singoli Stati. Questa scelta appare ragionevole considerata la persistenza della diversità degli ordinamenti giuridici dei singoli Stati (basti pensare alla notoria divisione tra paesi di *common law* e paesi di *civil law*). Del resto, l'**art. 2** del regolamento delimita il proprio ambito applicativo esclusivamente ai profili regolatori della immissione nel mercato delle Intelligenze artificiali[120] salvaguardando la disciplina interna dei

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

[120] Articolo 2, Ambito di applicazione, del regolamento IA cit.: "1. Il presente regolamento si applica: a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo; b) ai *deployer* dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione; c) ai fornitori e ai *deployer* di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione; d) agli importatori e ai distributori di sistemi di IA; e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio; f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione; g) alle persone interessate che si trovano nell'Unione. 2. Ai sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, relativo a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, si applicano unicamente l'articolo 6, paragrafo 1, gli articoli da 102 a 109 e l'articolo 112. L'articolo 57 si applica solo nella misura in cui i requisiti per i sistemi di IA ad alto rischio a norma del presente regolamento siano stati integrati in tale normativa di armonizzazione dell'Unione. 3. Il presente regolamento non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze. Il presente regolamento non si applica ai sistemi di IA se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività. Il presente regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività. 4. Il presente regolamento non si applica alle autorità pubbliche di un paese terzo né alle organizzazioni internazionali che rientrano nell'ambito di applicazione del presente regolamento a norma del paragrafo 1, laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri, a condizione che tale paese terzo o organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone. 5. Il presente regolamento non pregiudica

singoli Stati in materia di **protezione dei consumatori** e **di sicurezza dei prodotti**. Gli articoli da **9** a **29** del regolamento IA realizzano un sistema di armonizzazione dei requisiti di sicurezza e di conformità dei sistemi di IA; di conseguenza gli Stati membri conservano la competenza a disciplinare il risarcimento dei danni, l'onere della prova, le presunzioni causali, i regimi oggettivi e gli strumenti processuali di tutela, purché nel rispetto del diritto dell'Unione. Il regolamento IA contiene, invece, degli obblighi che possono essere utilizzati dai giudici nazionali come parametro della colpa e come standard di diligenza professionale ovvero come criterio di valutazione della prevedibilità del danno ovvero quale criterio per l'accertamento del nesso causale. L'**art. 13**[121], ad esempio, prevede che i sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente in modo da consentire ai *deployer* di interpretare l'*output* del sistema e utilizzarlo adeguatamente e che siano garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del

l'applicazione delle disposizioni sulla responsabilità dei prestatori di servizi intermediari di cui al capo II del regolamento (UE) 2022/2065 6. Il presente regolamento non si applica ai sistemi di IA o modelli di IA, ivi compresi i loro output, specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. 7. Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento. 8. Il presente regolamento non si applica alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio. Tali attività sono svolte in conformità del diritto dell'Unione applicabile. Le prove in condizioni reali non rientrano in tale esclusione. 9. Il presente regolamento lascia impregiudicate le norme stabilite da altri atti giuridici dell'Unione in materia di protezione dei consumatori e di sicurezza dei prodotti. 10. Il presente regolamento non si applica agli obblighi dei *deployer* che sono persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale. 11. Il presente regolamento non osta a che l'Unione o gli Stati membri mantengano o introducano disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso dei sistemi di IA da parte dei datori di lavoro, o incoraggino o consentano l'applicazione di contratti collettivi più favorevoli ai lavoratori. 12. Il presente regolamento non si applica ai sistemi di IA rilasciati con licenza libera e open source, a meno che non siano immessi sul mercato o messi in servizio come sistemi di IA ad alto rischio o come sistema di IA rientrante nell'ambito di applicazione dell'articolo 5 o 50.".

[121] Art. 13 del regolamento IA cit.: "I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai *deployer* di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del *deployer* di cui alla sezione 3. 2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso, in un formato appropriato digitale o non digitale, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i d*eployer*. 3. Le istruzioni per l'uso contengono almeno le informazioni seguenti: a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato; b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui: i) la finalità prevista; ii) il livello di accuratezza che ci si può attendere, comprese le metriche, di robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza; iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità della sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali di cui all'articolo 9, paragrafo 2; iv) se del caso, le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output; v) ove opportuno, le sue prestazioni per quanto riguarda le persone o i gruppi di persone specifici sui quali il sistema è destinato a essere utilizzato; vi) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA ad alto rischio; vii) se del caso, informazioni che consentano ai *deployer* di interpretare l'*output* del sistema di IA ad alto rischio e di usarlo in modo opportuno; c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità; d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA ad alto rischio da parte dei *deployer*; e) le risorse computazionali e di *hardware* necessarie, la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura, compresa la relativa frequenza, necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti *software*; f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai *deployer* di raccogliere, conservare e interpretare correttamente i log in conformità dell'articolo 12".

"*deployer*". Questi ultimi devono poi garantire la sorveglianza umana (**art. 14**[122]) delle intelligenze artificiali ad alto rischio in modo da prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione e il rispetto degli altri requisiti previsti dal regolamento IA[123].

4.2.3. Il Regolamento (UE) 2026/1744 (il c.d. «Digital Omnibus sull'IA»).

Il **regolamento (UE) 2026/1744** del Parlamento europeo e del Consiglio, dell'8 luglio 2026, il cosiddetto «**Digital Omnibus sull'IA**», pubblicato nella *Gazzetta Ufficiale dell'Unione europea* del 24 luglio 2026 ed entrato in vigore il 27 luglio 2026, costituisce la prima modifica

[122] Art. 14 del regolamento IA cit.:"1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso. 2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione.3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti: a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile;
b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal *deployer.* 4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al *deployer* in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'*output* prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili.

[123] Articolo 14, Sorveglianza umana, del regolamento IA cit.: "1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso. 2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione. 3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti: a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile; b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal deployer. 4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al deployer in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza. 5. In aggiunta, per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 del presente articolo sono tali da garantire che il deployer non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità. Il requisito di una verifica separata da parte di almeno due persone fisiche non si applica ai sistemi di IA ad alto rischio utilizzati a fini di contrasto, migrazione, controllo delle frontiere o asilo, qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito".".

sostanziale dell'AI Act dalla sua adozione[124]. Il Regolamento "Omnibus" non riscrive l'impianto del regolamento IA. Le categorie di rischio dei sistemi di Intelligenza Artificiale restano immutate, gli obblighi per i sistemi ad alto rischio non vengono eliminati, la disciplina dei modelli per finalità generali e il sistema sanzionatorio rimangono sostanzialmente invariati. La modifica di maggiore impatto operativo consiste nel rinvio dell'entrata in vigore delle disposizioni del **Capo III, sezioni 1, 2 e 3**, del regolamento "IA Act", ossia quelle relative ai requisiti dei sistemi ad alto rischio, agli obblighi dei rispettivi operatori e alle autorità di notifica e agli organismi notificati. Il **differimento** dell'entrata in vigore di alcune disposizioni del "IA Act", per quanto qui rileva, è il seguente: le disposizioni sui sistemi ad alto rischio elencati nell'Allegato III – categoria nella quale rientra, anche l'uso giudiziario di cui al punto 8, lettera a) – diventeranno applicabili dal 2 dicembre 2027; quelle relative ai sistemi ad alto rischio disciplinati dall'Allegato I, in quanto componenti di sicurezza di prodotti già soggetti alla normativa di armonizzazione dell'Unione, slittano al 2 agosto 2028; resta invece fermo il termine autonomo del 2 agosto 2030 per l'adeguamento dei sistemi ad alto rischio già destinati all'uso da parte delle autorità pubbliche.

Accanto al differimento anzidetto, l' "Omnibus" ha introdotto due nuovi divieti assoluti inseriti nell'**art. 5, paragrafo 1**, del regolamento IA – rispettivamente in materia di sistemi che generano o manipolano immagini, video o audio realistici raffiguranti le parti intime di una persona fisica identificabile o la stessa impegnata in condotte sessualmente esplicite, e in materia di materiale pedopornografico generato artificialmente – nonché una nuova base giuridica (**art. 4-*bis***) per il trattamento eccezionale di categorie particolari di dati personali ai fini del rilevamento e della correzione delle distorsioni algoritmiche, e un rafforzamento dei poteri dell'Ufficio europeo per l'IA.

4.2.4. La legge 23 settembre 2025, n. 132. Cenni.

Il legislatore italiano è intervenuto con la **legge 23 settembre 2025, n. 132** (pubblicata nella *Gazzetta Ufficiale n. 223 del 25 settembre 2025* ed entrata in vigore il 10 ottobre 2025), recante "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*"[125], Legge IA. La legge IA non sostituisce il regolamento IA, che resta direttamente applicabile in quanto regolamento europeo, ma lo integra con principi generali, disposizioni settoriali e deleghe legislative, collocandosi espressamente in un rapporto di continuità interpretativa con esso: l'**art. 1, comma 2**, stabilisce infatti che le disposizioni della legge «*si interpretano e si applicano conformemente*» al **Regolamento (UE) 2024/1689** (regolamento IA). Per quel che concerne i profili relativi alla responsabilità civile da utilizzo illecito di sistemi di intelligenza

[124] Regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio, dell'8 luglio 2026, che modifica i regolamenti (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 quanto alla semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale («Digital Omnibus sull'IA»), pubblicato in GUUE del 24 luglio 2026, in vigore dal 27 luglio 2026 (https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L_202601744).
[125] Legge 23 settembre 2025, n. 132, «Disposizioni e deleghe al Governo in materia di intelligenza artificiale» (G.U. n. 223 del 25 settembre 2025).

artificiale va ricordato che **l'art. 17**[126] della legge IA ha modificato l'**art. 9, comma 2, c.p.c.**, attribuendo al Tribunale, in composizione monocratica o secondo le regole ordinarie di competenza, la cognizione delle «*cause che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale*», equiparandole, sotto il profilo della competenza per materia, alle cause di esecuzione forzata. Si tratta di una disposizione che, pur di carattere processuale, segnala la consapevolezza del legislatore circa l'emersione di un nuovo e specifico contenzioso avente ad oggetto il funzionamento (e i malfunzionamenti) dei sistemi di IA, e che si salda con la delega di cui all'art. 16[127] della medesima legge, relativa alla disciplina organica di dati, algoritmi e metodi matematici di addestramento, la cui competenza giurisdizionale è attribuita, secondo i criteri direttivi della delega, alle sezioni specializzate in materia di impresa. Quanto alla definizione di Intelligenza Artificiale l'**art. 2**[128] rinvia all'**art. 3, punto 1**, del regolamento IA il quale prevede che un sistema di IA consiste in "*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*". Sui criteri di delega indicati all'art.24 della legge n.132 del 2025 si rinvia al paragrafo "**1. Il d.lgs. 9 settembre 2026, n. 160**".

4.2.5. La Direttiva (UE) n. 2024/2853.

La **Direttiva (UE) n. 2024/2853 (Product Liability Directive)** del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi ha abrogato (con effetto dal 9.12.2026) la **direttiva 85/374/CEE** del Consiglio e rappresenta un nuovo approdo sulla disciplina della responsabilità da prodotti difettosi digitali.

---

[126] Art. 16 della legge n. 132 del 2025: "1. All'articolo 9, secondo comma, del codice di procedura civile, dopo le parole: «esecuzione forzata» sono inserite le seguenti: «, per le cause che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale»".

[127] Art. 16 Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale

"1. Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale senza obblighi ulteriori, negli ambiti soggetti al regolamento (UE) 2024/1689, rispetto a quanto già ivi stabilito.

2. Gli schemi dei decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia e sono successivamente trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti. Decorsi sessanta giorni dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine venga a scadere nei trenta giorni antecedenti alla scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni.

3. Nell'esercizio della delega di cui al comma 1, il Governo si attiene ai seguenti principi e criteri direttivi:

a) individuare 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;

b) prevedere strumenti di tutela, di carattere risarcitorio o inibitorio, e individuare un apparato sanzionatorio per il caso di violazione delle disposizioni introdotte ai sensi della lettera a);

c) attribuire alle sezioni specializzate in materia di impresa le controversie relative alla disciplina introdotta ai sensi delle lettere a) e b).".

[128] Art. 2 della l. n. 132 del 2025:"1. Ai fini della presente legge, si intendono per: a) sistema di intelligenza artificiale: il sistema definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689; b) dato: 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; c) modelli di intelligenza artificiale: i modelli definiti dall'articolo 3, punto 63), del regolamento (UE) 2024/1689.2. Per quanto non espressamente previsto, si rimanda alle definizioni di cui al regolamento (UE) 2024/1689."

Gli obiettivi presi di mira dalla "PLD" sono i seguenti: a) modernizzare le norme in materia di responsabilità per i modelli di impresa dell'economia circolare: rendendo le norme in materia di responsabilità chiare ed eque per le imprese che modificano in maniera sostanziale i prodotti[129]; b) modernizzare le norme in materia di responsabilità per i prodotti nell'era digitale: consentendo risarcimenti per i danni causati da prodotti come robot, droni o sistemi di domotica, diventati non sicuri in seguito ad aggiornamenti del software, dei servizi di IA o dei servizi digitali necessari al funzionamento dei prodotti stessi, nonché quando i fabbricanti non rimediano alle vulnerabilità esistenti in termini di cibersicurezza[130]; c) creare parità di condizioni tra i fabbricanti UE e non UE: i consumatori che subiscono danni causati da prodotti non sicuri importati da Paesi Terzi potranno esigere un risarcimento dall'importatore o dal rappresentante del fabbricante nell'UE[131]; d) mettere i consumatori su un piano di parità con i fabbricanti: imponendo a questi ultimi di divulgare gli elementi di prova, introducendo una maggiore flessibilità nei termini per la presentazione dei reclami e alleggerendo l'onere della prova per i danneggiati in casi complessi, come quelli riguardanti i prodotti farmaceutici o l'IA[132]. La direttiva dovrà essere attuata entro il **9.12.2026**. La persona fisica dovrà, quindi,

[129] Considerando n. 1 della direttiva 2024/2853: "Al fine di migliorare il corretto funzionamento del mercato interno, è necessario garantire che la concorrenza non sia falsata e che la circolazione delle merci non sia ostacolata. La direttiva 85/374/CEE del Consiglio (3) stabilisce norme comuni in materia di responsabilità per danno da prodotti difettosi con l'obiettivo di eliminare le disparità esistenti tra i sistemi giuridici degli Stati membri che possono falsare la concorrenza e pregiudicare la libera circolazione delle merci nel mercato interno. Una maggiore armonizzazione delle norme comuni in materia di responsabilità per danno da prodotti difettosi stabilite in tale direttiva contribuirebbe ulteriormente al conseguimento di tali obiettivi, comportando nel contempo un maggiore grado di protezione della salute o dei beni dei consumatori e di altre persone fisiche".

[130] Considerando n. 13 della direttiva (UE) 2024/2853:"I prodotti nell'era digitale possono essere tangibili o intangibili. Sul mercato è sempre più diffuso il software, come i sistemi operativi, il firmware, i programmi per computer, le applicazioni o i sistemi di IA, e la sua importanza a fini di sicurezza dei prodotti è sempre maggiore. Il software può essere immesso sul mercato come prodotto a sé stante o può essere poi integrato in altri prodotti come componente e può causare danni dovuti al suo funzionamento. Per garantire la certezza del diritto è opportuno chiarire nella presente direttiva che, ai fini dell'applicazione della responsabilità oggettiva, il software è un prodotto, a prescindere dalle modalità con cui viene fornito o usato, e quindi dal fatto che il software sia integrato in un dispositivo, utilizzato tramite una rete di comunicazione o tecnologie cloud oppure sia fornito attraverso un modello software-as-a-service. Le informazioni, invece, non devono invece essere considerate un prodotto e le norme sulla responsabilità per danno da prodotti difettosi non dovrebbero pertanto applicarsi al contenuto dei file digitali, quali file multimediali, e-book o il mero codice sorgente dei software. Il produttore o lo sviluppatore di software, compreso il fornitore di sistemi di IA ai sensi del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, dovrebbe essere considerato un fabbricante"

[131] Considerando n. 37 della direttiva 2024/2853: Per garantire che il danneggiato possa far valere il proprio diritto al risarcimento del danno subito nei casi in cui il fabbricante del prodotto è stabilito al di fuori dell'Unione, dovrebbero poter essere ritenuti responsabili l'importatore del prodotto e il rappresentante autorizzato del fabbricante, nominato in relazione a compiti specifici a norma della legislazione dell'Unione, ad esempio in virtù della normativa in materia di sicurezza dei prodotti e vigilanza del mercato. La vigilanza del mercato ha dimostrato che le catene di approvvigionamento coinvolgono talvolta operatori economici la cui forma è talmente nuova che non rientrano facilmente nelle catene di approvvigionamento tradizionali nell'ambito del quadro giuridico esistente. È il caso, in particolare, dei fornitori di servizi di logistica, che svolgono molte delle stesse funzioni degli importatori, ma che potrebbero non corrispondere sempre alla tradizionale definizione di importatore nel diritto dell'Unione. I fornitori di servizi di logistica svolgono un ruolo sempre più significativo come operatori economici, consentendo e agevolando l'accesso al mercato dell'Unione per i prodotti provenienti da paesi terzi. Tale mutamento a livello di rilevanza si riflette già nel quadro per la sicurezza dei prodotti e la vigilanza del mercato, in particolare nei regolamenti (UE) 2019/1020 e (UE) 2023/988 del Parlamento europeo e del Consiglio. Pertanto, i fornitori di servizi di logistica dovrebbero poter essere ritenuti responsabili; tuttavia, data la natura sussidiaria del loro ruolo, dovrebbero essere responsabili solo nel caso in cui non vi sia alcun importatore o rappresentante autorizzato stabilito nell'Unione. Per un'efficace canalizzazione della responsabilità nei confronti di fabbricanti, importatori, rappresentanti autorizzati e fornitori di servizi di logistica, i distributori dovrebbero poter essere ritenuti responsabili solo qualora non identifichino tempestivamente un operatore economico interessato stabilito nell'Unione.

[132] Considerando n. 42 della direttiva (UE) 2024/2853: "Poiché gli operatori economici sono soggetti a una responsabilità che prescinde dalla colpa, e al fine di garantire una giusta ripartizione dei rischi, l'onere di provare il danno, il carattere difettoso del prodotto e il nesso di causalità che li unisce dovrebbe incombere, in conformità del livello probatorio applicabile a norma del diritto nazionale, al soggetto che chiede il risarcimento del danno causato da un prodotto difettoso. Il soggetto che chiede il risarcimento del danno è però spesso in una situazione di netto svantaggio rispetto al fabbricante per quanto concerne la possibilità di ottenere e comprendere le informazioni sulle

allegare soltanto il fatto illecito e provare il danno patrimoniale e non patrimoniale che, secondo la direttiva, è risarcibile qualora il prodotto difettoso abbia cagionato la morte o abbia provocato lesioni alla vittima[133]. Con la Direttiva (UE) 2024/2853, il legislatore europeo ha inteso, quindi, modernizzare la responsabilità da prodotto difettoso per adeguarla ai mutamenti indotti dall'avvento dell'economia dei dati e dell'intelligenza artificiale. La nuova disciplina definisce prodotto ogni bene mobile, anche se integrato e interconnesso con altro bene mobile o immobile (**art. 4**) e stabilisce in modo esplicito che la nozione di prodotto comprende non solo l'elettricità ma anche i files digitali e il software. Pertanto, secondo la direttiva n. 2853/2024 UE, un software può costituire di per sé un prodotto (c.d. stand-alone) o un componente di un prodotto. Questa disciplina richiede la messa a disposizione del bene per la distribuzione, il consumo o l'uso, che avvengano nel corso di un'attività commerciale, a titolo sia oneroso che gratuito (**art. 4, n. 7**). Si include, quindi, non solo la messa a disposizione per la distribuzione e il consumo, ma anche per il mero utilizzo sulla base di un rapporto non qualificabile come rapporto di consumo (ad es. per un utilizzo inerente ad un'attività professionale). Il ***considerando* 13** della direttiva riconduce, per quel che più interessa, alla nozione di software anche le applicazioni digitali e i sistemi di intelligenza artificiale. Viene, invece, escluso espressamente dal novero dei prodotti il *software libero* e *open source* prodotto o sviluppato nel corso di un'attività non commerciale, per via dei benefici per l'innovazione connessi a questa modalità di messa a disposizione del bene. Con l'inclusione del software e, soprattutto, dei sistemi di IA, il legislatore europeo ambisce a governare, attraverso l'introduzione di regole di responsabilità civile armonizzate, questa tecnologia oramai sempre più presente nelle nostre vite, in linea con quanto si intende fare, sul versante della regolazione di sicurezza, con l'adozione del regolamento IA. Inoltre, queste regole rivestono rilevanza transnazionale[134], soprattutto, trans-europea, giacché si applicano a catene di produzione – e, altresì di distribuzione– che, in questo settore, sovente rivestono una dimensione globale. Quanto ai difetti nei sistemi di Intelligenza Artificiale la direttiva (UE)

---

modalità di fabbricazione e funzionamento del prodotto. Tale asimmetria in termini di informazioni può compromettere la giusta ripartizione dei rischi, specialmente nei casi più complessi da un punto di vista tecnico o scientifico. È pertanto necessario agevolare per l'attore l'accesso agli elementi di prova da utilizzare nei procedimenti giudiziari. Tali elementi di prova comprendono documenti che il convenuto deve creare *ex novo* aggregando o classificando gli elementi di prova disponibili. Nel valutare la richiesta di divulgazione degli elementi di prova, gli organi giurisdizionali nazionali dovrebbero garantire che tale accesso sia limitato a quanto necessario e proporzionato, tra l'altro per evitare ricerche non specifiche di informazioni non rilevanti per il procedimento e per proteggere le informazioni riservate, come le informazioni che rientrano nell'ambito di applicazione del segreto professionale e dei segreti commerciali conformemente al diritto dell'Unione e nazionale, in particolare alla direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio. Tenuto conto della complessità di determinati tipi di prove, ad esempio quelle relative ai prodotti digitali, gli organi giurisdizionali nazionali dovrebbero poter richiedere che tali elementi di prova siano presentati in modo facilmente accessibile e facilmente comprensibile, a determinate condizioni.

[133] Art. 6 della direttiva 2024/2853: "1. Il diritto al risarcimento a norma dell'articolo 5 si applica solo alle seguenti tipologie di danno: a) morte o lesioni personali, compresi i danni psicologici riconosciuti da un punto di vista medico; b) danneggiamento o distruzione di qualsiasi bene, tranne: i) il prodotto difettoso in sé; ii) un prodotto danneggiato da un componente difettoso che è integrato in tale prodotto o interconnesso con questo dal fabbricante di tale prodotto o sotto il controllo di tale fabbricante; iii) i beni usati esclusivamente a fini professionali; c) distruzione o corruzione di dati non usati a fini professionali. 2. Il diritto al risarcimento a norma dell'articolo 5 copre tutte le perdite materiali derivanti dal danno di cui al paragrafo 1 del presente articolo. Il diritto al risarcimento copre anche le perdite immateriali derivanti dal danno di cui al paragrafo 1 del presente articolo, nella misura in cui possono essere risarcite in base al diritto nazionale.3. Il presente articolo fa salva la legislazione nazionale relativa al risarcimento dei danni a titolo di altri regimi di responsabilità.".

[134] R. MONTINARO, *Il danno da "prodotto digitale" difettoso: continuità ed evoluzione del regime europeo sulla responsabilità del produttore*, in *La Nuova Giurisprudenza Civile Commentata*, n. 3, 1° maggio 2026, p. 622.

n. 2853/2024 non addossa al produttore una forma di responsabilità oggettiva "pura", giacché concerne i soli i danni che discendono da un difetto del prodotto (vedasi **considerando 2**). Il difetto funge, dunque, da criterio di imputazione della responsabilità al produttore. Il difetto non si risolve in specifiche carenze tecniche del prodotto, né tantomeno coincide con una o più caratteristiche intrinseche dello stesso, consistendo piuttosto in una qualifica di "insicurezza" da assegnarsi al prodotto all'esito di un giudizio che va formulato sulla scorta dei criteri individuati dalla disciplina di cui si tratta (**art. 7**). I parametri per determinare il carattere difettoso di un prodotto riflettono una prospettiva *ex ante*, incentrata sul fabbricante (o sviluppatore per i sistemi di IA), quale soggetto meglio posizionato per valutare i rischi e i benefici degli investimenti in sicurezza. L'imputazione della responsabilità è invero fondata su tale valutazione, che ha come spartiacque il tempo della immissione del prodotto in commercio o della sua messa in servizio. La responsabilità è addossata al fabbricante con riguardo ai rischi rispetto ai quali egli sia in grado di esercitare un controllo, in quanto attinenti alla sua ideazione e realizzazione, nonché alle modalità di utilizzo dello stesso, come predeterminate da tale operatore economico. Nel caso dei sistemi di IA, appare particolarmente difficile stimare e prevedere *ex ante* tutti i rischi, in quanto gli standard di sicurezza sono spesso inesistenti, carenti e/o soggetti a rapida obsolescenza. Problema, quest'ultimo, che appare risolto nelle disposizioni della direttiva sui prodotti difettosi del 2024, laddove si prevede che la non conformità alle discipline di sicurezza, disciplinate dal diritto dell'Unione e, quindi, dal regolamento IA, fa presumere "*il carattere difettoso di un prodotto*" (**art. 10, 2, lett. b**). Le regole di prevenzione introducono, poi, obblighi di condotta post-immissione in commercio gravanti sul produttore, che incidono sulle aspettative di sicurezza e dunque sulla nozione di difetto del prodotto. A titolo di esempio, si consideri l'art. **72** del regolamento IA che impone il monitoraggio dei sistemi di IA ad alto rischio durante il loro utilizzo. Lo stesso è a dirsi per gli obblighi gravanti sui fornitori dei modelli di IA per finalità generali implicanti rischi c.d. sistemici (**art. 55** del regolamento IA), obblighi aventi ad oggetto la valutazione e mitigazione di rischi di tal fatta anche successivamente alla messa a disposizione del modello di IA a terzi, per tutto il ciclo di vita del sistema di IA. Un sistema di IA può presentarsi, infatti, come un prodotto non statico né definito una volta per tutte al momento della sua immissione in commercio, ma, al contrario, aperto, nel senso di essere suscettibile di "mutare" per via di aggiornamenti ed evoluzioni del *software*, anche dovuti alla sua esposizione a nuove fonti di dati e al continuo "addestramento" da parte degli utenti e degli stessi sviluppatori. Simili mutamenti possono intervenire ben oltre la conclusione della catena di fornitura, nel corso dell'utilizzo del sistema di IA. Come noto, i sistemi di IA generativa sono spesso utilizzati per interagire con degli utenti (professionali e non). Gli utenti dialogano con l'intelligenza artificiale attraverso i "*prompt*", ossia quesiti[135] diretti ad indagare

[135] Di recente la società statunitense *Anthropic* ha aggiornato la propria *policy* di utilizzo delle sue intelligenze artificiali, in particolare "*Claude*", vietando agli utenti comportamenti "abusivi o crudeli, prolungati e non necessari" quando interloquiscono con le IA. L'esempio, estremo, indicato nell'articolo on line, potrebbe essere quello di un utente che, per giorni o settimane, apre ripetutamente nuove conversazioni con *Claude* unicamente per insultarlo, umiliarlo o minacciarlo in modo gratuito e ossessivo, senza mai formulare richieste concrete, senza scopi creativi e

e ad ottenere risposte generaliste. In tal modo l'IA si "addestra" ed implementa le sue conoscenze e le sue prestazioni. Proprio in tale fase, possono verificarsi comportamenti c.d. anomali dei sistemi di IA (ad esempio, il ricorso a tecniche di persuasione degli utenti, "allucinazioni" sistematiche, ecc.), forieri di rischi anche di una certa gravità. Una cesura netta della responsabilità del produttore al tempo della immissione in commercio o messa in servizio precluderebbe ai danneggiati di domandare il risarcimento per i danni derivanti dall'utilizzo dei sistemi di IA. Per ovviare ad un simile esito, la direttiva ha introdotto il "limite" del **momento in cui il prodotto è uscito dal controllo del fabbricante** (artt. **8** ed **11**). Una delle condizioni che determinano la conservazione del controllo è costituita dal fatto che il prodotto sia stato progettato per essere suscettibile di subire modifiche nel tempo, per effetto dell'apprendimento automatico. Tale caratteristica, impressa ad alcuni sistemi di IA dagli stessi sviluppatori/produttori, ha il medesimo valore di una modifica sostanziale e preclude quella cesura, in termini di imputazione della responsabilità, che di regola segue alla immissione del prodotto in commercio o alla sua messa in servizio. Il parametro temporale da considerare nel valutare la sussistenza di legittime aspettative di sicurezza dei consumatori coincide, dunque, con la durata del controllo da parte del fabbricante di questo tipo di prodotto. Infatti, come chiarito dal ***considerando* 32**, sussiste "*un legittimo affidamento sul fatto che il software e gli algoritmi sottostanti di un prodotto sono concepiti in modo da prevenirne comportamenti pericolosi*". Al tempo stesso, la "*capacità di continuare a imparare o acquisire nuove caratteristiche dopo la sua immissione sul mercato o messa in servizio*" costituisce uno dei criteri per valutare il carattere difettoso del prodotto (**art. 7**, par., lett. c, "*gli effetti sul prodotto della sua capacità di continuare a imparare o acquisire nuove funzionalità dopo la sua immissione sul mercato o messa in servizio*"). Il medesimo criterio (limite) rileva poi anche ai fini dell'accertamento della presenza delle **esimenti** costituite dal cosiddetto **difetto sopravvenuto** e dal **rischio da sviluppo**, previste all'**art. 11, par.1, lett.c)** ed **e)**, della direttiva sui prodotti difettosi. In particolare, lo stato delle conoscenze oggettivamente disponibili, attinenti a rischi insiti nel prodotto, va accertato proprio avendo riguardo al parametro del controllo sul prodotto. Se ne ricava che un difetto del prodotto può sussistere anche allorché l'apprendimento automatico, che continui dopo l'immissione in commercio, conduca a comportamenti anomali del sistema di IA, fonte di danni del tipo risarcibile secondo la disciplina della direttiva. Risulta, quindi, alquanto problematico valutare il difetto del prodotto nel caso di un sistema di IA connotato dalla capacità di apprendimento automatico (ma lo stesso è a dirsi anche per le IA "vertificalizzate" o "agentiche"). La direttiva richiede che si valuti il risultato dell'uso di tale specie di prodotto, ossia la circostanza che esso consista in un comportamento anomalo foriero di danni. Ciò emergerebbe, secondo quanto espresso da autorevole dottrina[136], da quanto traspare dal citato **considerando 32**, per il quale sussiste un "legittimo affidamento sul fatto che il *software* e gli algoritmi

senza che si tratti di un test o di una semplice reazione a un errore del modello (vedasi "Anthropic introduce il divieto di "abusi prolungati e crudeli" contro i suoi modelli IA, Rai News, Scienze e Tecnologie, 11.10.2026).
[136] R.MONTINARO, cit. .

sottostanti di un prodotto **sono concepiti in modo da prevenirne comportamenti pericolosi**". L'attenzione, quindi, va spostata sulla verificazione di siffatto tipo di comportamenti e, prima ancora, sulla circostanza che non siano stati introdotti meccanismi atti a prevenirli. Invero, il difetto va allegato e provato dall'attore, non potendo esso desumersi dal mero fatto della produzione di un danno riconducibile all'uso di un prodotto. Occorre quindi procedere ad una valutazione delle proprietà del sistema di IA e considerare soprattutto la mancata adozione di eventuali limiti o "*guard-rail*", predisposti dal fabbricante. Rileva, altresì, la circostanza che non siano state previste misure di monitoraggio e/o che sussistano deficit di avviso agli utenti circa i rischi che possono discendere dall'apprendimento automatico continuo. Poiché, però, come noto, la dimostrazione del difetto è onere assai difficile da assolvere allorché il sistema di IA sia tecnicamente complesso e sofisticato, non possono che venire in rilievo le **agevolazioni probatorie** introdotte dalla direttiva. Tra di esse, vi è, in particolare, la presunzione per la quale il difetto del prodotto si presume se "*l'attore dimostra che il danno è stato causato da un malfunzionamento evidente del prodotto durante l'uso ragionevolmente prevedibile o in circostanze ordinarie*" (**art. 10, par. 2, lett. c**). Si tratta dunque di assegnare al concetto di "*malfunzionamento evidente*" un significato tale da includere gli esiti inattesi e abnormi, in termini di sicurezza, di un prodotto. Al riguardo va osservato che, nei diversi sistemi nazionali, si è andata formando una giurisprudenza che prende in considerazione comportamenti "sorprendenti" dei prodotti, riscontrabili allorché si verifichi una significativa deviazione dalle aspettative di sicurezza, in condizioni di uso normali o ragionevolmente prevedibili. La stessa direttiva (UE) n. 2853/2024 UE reca l'esempio di una bottiglia che esploda durante un uso di tal fatta (**considerando 46**[137]). Conta, in simili casi, la palese frustrazione delle aspettative ragionevoli di sicurezza. Ebbene, lo stesso argomento potrebbe essere invocato allorché si tratti di un comportamento **abnorme** od **imprevedibile** di un sistema di IA (una IA che divulga pubblicamente i "prompt" di un utente in aperta violazione dell'aspettativa di riservatezza). Inoltre, a favore del danneggiato è stata introdotta una presunzione di sussistenza del difetto e/o del nesso di causalità con il danno (cfr. art. 10, § 4), la quale presunzione opera quando "*l'attore incontri difficoltà eccessive, in particolare a causa della complessità tecnica o scientifica, nel provare il carattere difettoso del prodotto o*

[137] Considerando 46 della direttiva (UE) 2024/2853 :" È necessario alleggerire l'onere della prova a carico dell'attore, purché siano rispettate determinate condizioni. Le presunzioni di fatto relative sono un meccanismo comune per ridurre le difficoltà probatorie che incontra l'attore e consentire all'organo giurisdizionale di stabilire l'esistenza del carattere difettoso difetto o del nesso di causalità in base all'esistenza di altri fatti provati e tutelando nel contempo i diritti del convenuto. Gli organi giurisdizionali nazionali dovrebbero presumere il carattere difettoso di un prodotto qualora il convenuto non si conformi all'obbligo di divulgare le pertinenti informazioni, in modo da promuovere l'osservanza di tale obbligo. Per proteggere i consumatori e altre persone fisiche dal rischio di danni sono stati adottati numerosi requisiti obbligatori di sicurezza, tra cui il regolamento (UE) 2023/988. Per rafforzare lo stretto legame tra le norme in materia di sicurezza dei prodotti e quelle relative alla responsabilità, anche la non conformità a tali requisiti dovrebbe dar luogo a una presunzione circa il carattere difettoso di un prodotto. Ciò vale anche nel caso in cui un prodotto non sia dotato di mezzi per registrare informazioni sul suo funzionamento come previsto dal diritto dell'Unione o nazionale. Lo stesso dovrebbe valere per il caso di malfunzionamento evidente, come quello di una bottiglia di vetro che esploda durante l'uso ragionevolmente prevedibile, dato che risulterebbe inutilmente oneroso imporre all'attore di provare il carattere difettoso di un prodotto se le circostanze sono tali da non permettere di contestarne l'esistenza. L'uso ragionevolmente prevedibile comprende l'uso al quale un prodotto è destinato conformemente alle informazioni fornite dal fabbricante o dall'operatore economico che immette il prodotto sul mercato, l'uso normale determinato dalla progettazione e dalla costruzione del prodotto e l'uso ragionevolmente prevedibile qualora tale uso possa derivare da un comportamento umano lecito e facilmente prevedibile".

il nesso di causalità tra il carattere difettoso e il danno o entrambi" e, al tempo stesso, sia "*probabile che il prodotto sia difettoso o che esista un nesso di causalità tra il carattere difettoso del prodotto e il danno, o entrambi*".

4.2.6. Legislazione europea sui servizi digitali e la proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (cd. "AILD", *Artificial Intelligence liability Directive*).

Appare opportuno un breve cenno agli atti normativi emanati dall'Unione europea su aspetti che, volti a disciplinare specifiche questioni relative ai servizi digitali, si pongono in una linea di intersezione con l'IA. Ci si riferisce, in particolare, al ***Digital Service Act*** (**DSA**) (**Regolamento UE 2022/2065**), che mira a modernizzare il quadro normativo per i servizi digitali, concentrandosi sulla regolamentazione delle piattaforme online e stabilendo regole chiare per garantire la sicurezza e la trasparenza delle attività *online* [138].

Con Regolamento adottato dal Parlamento Europeo e dal Consiglio il 14 settembre 2022 è stato poi adottato il ***Digital Market Act*** (**DMA**), contenente misure volte alla promozione di una maggiore concorrenza nel settore dei servizi digitali e alla previsione di regole per prevenire comportamenti anticoncorrenziali da parte dei cosiddetti *gatekeeper*, ovvero grandi piattaforme che svolgono un ruolo cruciale nei mercati digitali.

Il ***Digital Governance Act*** (**DGA** – **Regolamento UE 2022/868 del 30 maggio 2022**, entrato in vigore il 24.9.2023), parte della strategia dell'UE per il digitale, si concentra sulla promozione dell'utilizzo dei dati nel settore pubblico. Mira a facilitare il riutilizzo dei dati del settore pubblico e a migliorare il modo in cui i dati vengono condivisi e gestiti all'interno dell'UE, includendo anche disposizioni sulla l'interoperabilità dei dati tra enti pubblici e tra il settore pubblico e quello privato e sul relativo riutilizzo[139].

Infine, con **regolamento del 13.12.2023 n. 2854/2023** è stato adottato il **Data Act**, volto a regolamentare il flusso di dati all'interno dell'Unione Europea e tra questa e altri paesi. Si concentra sulla condivisione e l'utilizzo dei dati, in particolare quelli generati da prodotti e servizi connessi, mirando a garantire che i dati possano essere accessibili e utilizzati in modo equo, promuovendo l'innovazione e la creazione di nuovi servizi[140].

La Commissione Europea, il 28.9.2022, ha adottato una proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale da intelligenza artificiale (cd. "**AILD**", ***Artificial Intelligence liability Directive***), successivamente ritirata. Obiettivo della proposta era quello di delineare un quadro giuridico

[138] Regolamento (Ue) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), consultabile al seguente link https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R2065.
[139] Regolamento (Ue) 2022/868 Del Parlamento Europeo E Del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), consultabile al seguente link https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R0868.
[140] Regolamento (Ue) 2023/2854 Del Parlamento Europeo E Del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati), consultabile al seguente link https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202302854.

armonizzato in materia di responsabilità civile per IA, con due direttrici principali: garantire ai danneggiati adeguati livelli di tutela; favorire la diffusione dei sistemi di intelligenza artificiale nel mercato interno, contribuendo al suo funzionamento. L'**art. 4** (rubricato "*Presumption of causal link in the case of fault*") prevedeva una presunzione relativa di causalità che, per la Commissione, costituiva una misura "meno onerosa" per soddisfare il diritto della vittima ad un equo risarcimento. I paragrafi (2) e (3) dell'articolo distinguevano, da un lato, le richieste di risarcimento avanzate nei confronti del fornitore di un sistema di AI ad alto rischio o nei confronti di un soggetto sottoposto agli obblighi del fornitore ai sensi della Proposta di Regolamento (da intendersi il successivo ed approvato regolamento IA) e, dall'altro, le richieste di risarcimento presentate nei confronti dell'utente. In caso di richieste di risarcimento basate sull'Articolo 4, paragrafo (2), la proposta prevedeva che l'adempimento degli obblighi da parte dei convenuti doveva essere valutato anche alla luce della gestione del rischio, ovvero delle misure in tal senso previste dalla proposta di Regolamento (da intendersi regolamento IA). In caso di sistemi di IA "ad alto rischio" l'articolo 4, al paragrafo (4), stabiliva poi un'eccezione alla presunzione di causalità, qualora il convenuto dimostrasse che il danneggiato fosse in possesso o a conoscenza di prove, competenze o informazioni sufficienti a dimostrare il nesso di causalità tra l'inosservanza ed il pregiudizio patito. Nel caso di sistemi di IA a rischio non alto, invece, l'articolo 4, paragrafo (5), stabiliva una condizione per l'applicabilità della presunzione di causalità, in base alla quale quest'ultima fosse subordinata ad una valutazione del giudice che stabilisse se fosse eccessivamente gravoso, per l'attore, provare il nesso causale.

La proposta di direttiva è stata, come anticipato all'inizio del paragrafo, successivamente "abbandonata" dalla Commissione. Si è trattata, tuttavia, della prima proposta normativa unionale finalizzata a regolamentare la responsabilità extracontrattuale da Intelligenza Artificiale.

4.3. Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale. Il Titolo II Capo II del d.lgs. n. 160 del 2026.

Il capo II dà attuazione, come già accennato, alla delega contenuta nell'articolo **24, comma 3 e comma 5**, **lettera d)**, della **legge n. 132** del **2025**, Legge IA, che ha conferito al Governo il compito di adottare uno o più decreti legislativi recanti, nei casi di responsabilità civile per danni cagionati nell'utilizzo di sistemi di intelligenza artificiale, strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689, regolamento IA.

L'intervento si colloca in un contesto eurounitario profondamente mutato rispetto al momento di presentazione, da parte della Commissione europea, della proposta di direttiva sulla responsabilità civile da intelligenza artificiale (COM (2022) 496). La Commissione, nel programma di lavoro per il 2025, ne ha infatti annunciato, come già accennato, il ritiro, in coerenza con l'obiettivo di semplificazione del quadro normativo digitale. Resta nondimeno

fermo il rilievo della **direttiva (UE) 2024/2853** sulla responsabilità per danno da prodotti difettosi, che incide direttamente sulla disciplina del software e dei sistemi di intelligenza artificiale qualificabili come prodotti, e che dovrà essere recepita nell'ordinamento nazionale entro il 9 dicembre 2026. Nella Relazione Illustrativa al decreto legislativo si afferma, in particolare, che il capo II persegue tre finalità fondamentali:

a) garantire al danneggiato strumenti effettivi di accesso alla prova, in considerazione dell'opacità tecnologica che caratterizza i sistemi di intelligenza artificiale e della tipica asimmetria informativa tra utilizzatore e fornitore;

b) alleggerire l'onere probatorio sul nesso di causalità, attraverso una presunzione modulata in funzione della classificazione di rischio del sistema operata dal **regolamento (UE) 2024/1689,** regolamento IA;

c) rafforzare la tutela del danneggiato persona fisica, mediante la previsione di un foro speciale del consumatore e di un'azione diretta nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile.

L'intervento è costruito secondo una logica di complementarità, e non di sostituzione, rispetto agli statuti speciali di responsabilità già operanti nell'ordinamento. Sono fatte espressamente salve, inoltre, le disposizioni dell'articolo **82** del **regolamento (UE) 2016/679** e la normativa nazionale (futura) di recepimento della **direttiva (UE) 2024/2853**, in tal modo evitando ogni effetto di restrizione delle tutele esistenti negli ambiti specificamente regolati dal diritto eurounitario. Il legislatore, intende, quindi, rafforzare la tutela del danneggiato da condotte o da attività "occasionate" (vedi *infra*) dall'utilizzo di sistemi di intelligenza artificiale mediante l'implementazione dei mezzi di prova (vedi infra) e con l'alleggerimento dell'onere probatorio posto in capo al danneggiato (mediante l'introduzione di una **presunzione di responsabilità**).

Le disposizioni introdotte dal **d.lgs. n. 160** sulla responsabilità da utilizzo di sistemi di intelligenza artificiale hanno, quindi, cercato di dare una adeguata risposta a due importanti problemi emersi già in sede europea con l'avvento delle prime intelligenze artificiali.

Il primo problema riguarda l'individuazione del **soggetto da convenire in giudizio** per ottenere la riparazione del torto subito. La complessità tecnica alla base del funzionamento dei sistemi IA determina una moltiplicazione delle possibili fonti di "distorsione" dell'*output*, rendendo oltremodo difficoltoso o comunque oneroso – per l'attore "potenziale" – stabilire a quale dei numerosi soggetti che partecipano alla produzione della decisione algoritmica sia causalmente riconducibile il danno ad essa associato. Le difficoltà risultano, sotto tale profilo, ulteriormente amplificate in ragione dell'incertezza che deriva dall'autonomia decisionale che sorregge taluni di questi sistemi e che, se non fosse stata risolta attraverso questo intervento legislativo, avrebbe scaricato sull'attore il costo, in termini di rischio, di decidere chi debba rispondere di un eventuale comportamento autonomo lesivo, assegnando al convenuto un'arma per rifuggire da un eventuale addebito di responsabilità.

Il secondo problema riguarda, invece, la difficoltà - per l'attore che si sia determinato ad agire in giudizio - di raccogliere gli **elementi probatori necessari e sufficienti** a provare

tutti gli elementi costitutivi alla base del modello di responsabilità che si è scelto di attivare. Su questo versante, gli ostacoli si legano più strettamente all'elevato grado di opacità dei sistemi di IA che, oltre a intensificare il problema della ricerca del convenuto sopra evidenziato, può altresì impedire la prova in giudizio della causalità materiale tra la natura lesiva dell'*output* e un difetto del sistema (qualora si sia agito contro il produttore) o una colpa addebitabile al partecipante alla catena di produzione dell'*output* convenuto in giudizio, qualora si agisca secondo il tradizionale "modulo" di responsabilità per colpa.

Si tratta di questioni problematiche tra loro strettamente collegate, ma non identiche: il secondo emerge a valle del primo, nel senso che presuppone che la vittima abbia già selezionato il convenuto o i convenuti a cui il danno ritiene sia da addebitare, decidendo di affrontare i costi e i tempi che conseguono alla loro chiamata in giudizio.

4.4. Il risarcimento del danno cagionato nell'utilizzo di un sistema di intelligenza artificiale.

L'**art. 16** del d.lgs. n. 160 del 2026 estende, al **comma 1**, l'applicazione delle disposizioni sull'accesso alle prove di cui all'articolo 17 (vedi *infra*) a tutte le azioni di risarcimento del danno, contrattuale ed extracontrattuale, cagionato nell'utilizzo di un sistema di intelligenza artificiale. Gli esempi di danno cagionato dall'utilizzo di sistemi di intelligenza artificiale possono essere molteplici: il danno può essere stato cagionato da errori contenuti nel programma informatico e, in questo caso, si potrà prospettare una responsabilità anche contrattuale dell'autore del programma. Ancora, il danno può essere stato cagionato dai dati utilizzati, che possono non essere di qualità e recare errori o *bias*. In questo caso, com'è evidente, si potrà configurare una responsabilità, anche contrattuale, del fornitore dei dati. Sempre più frequenti sono, fra l'altro, i contratti atipici, di cessione o di licenza, aventi ad oggetto dati personali e non personali, con le inevitabili connessioni con la disciplina in materia di dati personali, non personali e di proprietà intellettuale. Ancora, la causa dell'evento dannoso può risiedere nel *prompt*, cioè l'istruzione impartita al sistema di intelligenza artificiale o la domanda rivolta al sistema stesso, che può contenere anche comandi per l'aggiramento di limitazioni e divieti, i cosiddetti «*incantesimi*». In questo caso la responsabilità, anche concorrente, può configurarsi in capo a chi interroga il sistema, o in capo a chi dolosamente lo abbia alterato. Ancora, può essersi verificato un uso negligente di un sistema di Intelligenza Artificiale, ad esempio perché impiegato per una finalità diversa da quella per la quale il sistema è stato progettato o senza supervisione, come è accaduto nei recenti casi (vedi infra) che hanno riguardato la responsabilità professionale di alcuni avvocati: allora, in tal caso, la responsabilità ricadrà sui professionisti. Analogamente per quegli episodi di diffamazione che si sono verificati anche oltreoceano[141]. In questi casi si

[141] Il riferimento principale è al caso Mark Walters v. OpenAI, L.L.C. (23-A-04860-2). Si rileva meritevole di menzione sul tema anche le vicende di Jonathan Turley e di Brian Hood, avvenute sempre negli USA. Il primo, docente universitario, « accusato da » ChatGPT di aver molestato una studentessa, sulla base di un articolo del Washington Post, rivelatosi non essere mai esistito; il secondo, esponente politico, « indicato da » ChatGPT come essere stato coinvolto in uno scandalo di corruzione che, in realtà, l'interessato aveva a suo tempo denunciato.

applicheranno i principi generali previsti dall'ordinamento giuridico interno in materia di responsabilità contrattuale o extracontrattuale. Invece, in altre circostanze, il sistema di intelligenza artificiale potrà ritenersi difettoso benché con le criticità che questa qualificazione, così come già accennato, può comportare, e allora in quei casi si potranno applicare le disposizioni relative alla responsabilità da prodotto. È utile ricordare, fra l'altro, che la direttiva sulla responsabilità da prodotto ha incluso, come già accennato, il *software* nel campo di applicazione e menziona espressamente i danni cagionati dai sistemi di IA. Giova, inoltre, evidenziare, sin da ora che è comunque applicabile l'art. 82 del GDPR nel caso in cui i danni siano stati cagionati da trattamento illecito dei dati personali.

Nella Relazione Illustrativa emerge che la scelta di ricomprendere entrambe le forme di responsabilità (contrattuale ed extracontrattuale) risponde all'esigenza di assicurare, con la tutela più ampia possibile, al danneggiato un meccanismo di *disclosure* indipendente dal titolo, contrattuale o aquiliano, della pretesa risarcitoria. Questa disposizione si innesta sul recente quadro normativo europeo, di cui si è fatto già cenno, nel quale le azioni di risarcimento si articolano su un sistema multilivello che integra la disciplina codicistica nazionale con le recenti riforme europee, in particolare il **Regolamento (UE) 2024/1689** (**regolamento IA**) e la **Direttiva (UE) 2024/2853** in materia di responsabilità da prodotto difettoso.

Sotto il profilo della responsabilità contrattuale, come noto, il fondamento dell'azione risiede nell'articolo **1218** c.c., che sanziona l'inadempimento delle obbligazioni nascenti da un rapporto contrattuale. In questo contesto, l'evoluzione tecnologica impone, certamente, una rimeditazione della diligenza nell'adempimento richiesto *ex* art. **1176 c.c**., **comma 1** e **2**. L'art. **1176, comma 1, c.c.**, prevede che "*nell'adempiere l'obbligazione il debitore deve usare la* ***diligenza del buon padre di famiglia***" mentre, al **comma 2**, viene stabilito che "*Nell'adempimento delle obbligazioni inerenti all'esercizio di una attività professionale, la diligenza deve valutarsi con riguardo* ***alla natura dell'attività esercitata***". Oramai la diligenza nell'adempimento di cui al comma 1 deve parametrarsi a quella del "**buon tecnico di famiglia**" in quanto nei contratti stipulati mediante "**smart contract**"[142] le parti devono adempiere le proprie obbligazioni attraverso sistemi algoritmici o di intelligenza artificiale. I paciscenti devono, infatti, non solo identificarsi attraverso la firma digitale ma anche predisporre, magari con l'ausilio di terzi *ex* art. **1228 c.c.**, un codice informatico le cui

[142] L'art.8-*ter* del d.l. n. 135 del 2018, conv., con modif., dall'art.1, comma 1, della l.n.12 del 2019, stabilisce che"1. Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. 2. **Si definisce «smart contract» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.** 3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014. 4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3.".

prestazioni sono eseguite da un *software*. Le prestazioni, tuttavia, richiedono, talvolta, anche l'*input* e il controllo umano (ad esempio, il pagamento del prezzo) per cui è evidente che il contraente, anche non professionista, deve adempiere le proprie prestazioni con diligenza "tecnica" adeguata.

Anche la diligenza professionale *ex* **art. 1176, comma 2, c.c.** sta declinando verso una vera e propria "*diligenza algoritmica*". Tale parametro obbliga il professionista a una scelta consapevole di sistemi affidabili e a una verifica critica dei risultati prodotti, al fine di evitare che l'utilizzo acritico di output errati si traduca in una prestazione negligente. La giurisprudenza di merito ha già iniziato a sanzionare, sebbene prevalentemente sul piano della responsabilità processuale aggravata *ex* **art. 96 c.p.c.**, la condotta di avvocati che hanno presentato in giudizio atti contenenti citazioni inesistenti generate da IA, le cosiddette "*allucinazioni algoritmiche*"[143]. Per l'esplicito riferimento all'utilizzo dell'intelligenza artificiale generativa nella redazione degli atti processuali occorre ricordare l'ordinanza Cass., Sez. VII pen., n. 11431/2026. In tale ordinanza la Corte censura il fenomeno delle "*hallucinations*" dell'intelligenza artificiale, richiamando implicitamente il dovere del difensore di verificare l'attendibilità delle fonti giuridiche utilizzate negli atti giudiziari. In un caso, si è esclusa la responsabilità aggravata laddove l'errore dell'IA non fosse sintomatico di malafede ma diretto a rafforzare una linea difensiva già nota (Trib. Firenze, 14 marzo 2025). Ancora più di recente Cassazione pen., Sez. III, 11/06/2026, n. 23006, ha stabilito che "*In tema di ricorso per cassazione, la citazione di precedenti giurisprudenziali inesistenti o alterati, frutto di "allucinazione informatica", è indice particolarmente significativo di colpa qualificata nella determinazione della causa di inammissibilità, che giustifica l'aumento dell'importo della sanzione pecuniaria in favore della cassa delle ammende previsto dall'art. 616, comma 1, c.p.p. (In motivazione, la Corte ha evidenziato che l'impiego di strumenti di intelligenza artificiale non esonera il difensore dal dovere professionale di verificare la veridicità e la pertinenza delle fonti richiamate e che l'allegazione di precedenti inesistenti non costituisce mera debolezza argomentativa, ma condotta positivamente colpevole che altera la correttezza del contraddittorio, ostacola il vaglio di legittimità e lede l'obbligo minimo di verifica delle fonti che deve assistere gli atti difensivi)"*[144]. L'obbligo di verifica e della piena responsabilità del contenuto degli atti giudiziari da parte del difensore è stata affermata anche dalla Corte d'Appello di Bologna che, con la decisione n. 1352 del 12.05.2026[145], ha, in particolare, ribadito che integra la lite temeraria per colpa grave, ai sensi dell'**art. 96 c.p.c.**, la condotta del difensore che, facendo ricorso a modelli linguistici di IA, perfettamente utilizzabili nella professione forense, depositi atti contenenti richiami a precedenti giurisprudenziali inesistenti o alterati, senza avere svolto un controllo umano sull'esattezza delle citazioni. I modelli di intelligenza artificiale generativa non costituiscono delle banche dati giurisprudenziali, ma sono strumenti di generazione automatica del linguaggio fondati su meccanismi statistici e

[143] Trib. Torino, 16 settembre 2025, n. 2120; Trib. Latina, 23 settembre 2025; Trib. Siracusa, 20 febbraio 2026; Tribunale Mantova, 24 marzo 2026; Tribunale Lecco Sez. I, 27 maggio 2026, n. 256.
[144] CED Cass. pen. 2026.
[145] *Diritto & Giustizia 2026*, 17 agosto.

probabilistici, strutturalmente esposti al fenomeno delle "allucinazioni" (l'intelligenza artificiale se non conosce la risposta, è notorio, la inventa); il loro impiego come fonte diretta di precedenti, in assenza di verifica, configura violazione dei doveri di diligenza, lealtà e competenza dell'avvocato. In tali ipotesi è legittima, per il Collegio emiliano, oltre alla condanna alle spese, la condanna *ex* **art. 96, comma 3 e comma 4**, c.p.c. a favore della controparte e della Cassa delle Ammende, nonché la trasmissione della sentenza al Consiglio dell'Ordine competente per le valutazioni disciplinari sulla condotta del difensore. Nella decisione si legge infatti che "*Tutto quanto sopra integra una ipotesi di lite temeraria per colpa grave, perché certamente è ben possibile il ricorso da parte dei legali agli strumenti che le nuove tecnologie mettono a disposizione, ma altrettanto certamente è necessario che non venga trascurata la dovuta supervisione e verifica umana dell'output che viene poi versato negli atti processuali, di cui il difensore continua ovviamente ad assumersi la responsabilità*".

È da segnalare la prima decisione di merito in tema di responsabilità contrattuale per il mancato utilizzo di sistemi di intelligenza artificiale in ambito bancario. In tema di operazioni di pagamento non autorizzate, è stato stabilito che grava sulla banca l'onere di provare che l'operazione sia stata autenticata e correttamente eseguita, nonché l'adozione di sistemi automatizzati di rilevamento delle transazioni anomale, anche basati su intelligenza artificiale e "*machine learning"*. La sola implementazione della "*Strong Customer Authentication*" non esonera l'istituto di credito da responsabilità qualora il sistema si riveli aggirabile da malware[146]. In tema di imputabilità del danno cagionato da sistemi automatizzati il **Consiglio di Stato, con la decisione 4.2.2020 n. 881**, ha enunciato i tre principi cardinali, desumibili dal diritto unionale, in materia di decisioni algoritmiche errate: **conoscibilità**, **comprensibilità** e **non esclusività della decisione automatizzata rispetto all'intervento umano**. Nella decisione del Supremo Consesso della giustizia amministrativa è stato, in particolare, affermato che: *"In primo luogo,* ***il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a ricevere informazioni significative sulla logica utilizzata****. Il principio, in esame è formulato in maniera generale e, perciò, applicabile sia a decisioni prese da soggetti privati che da soggetti pubblici, anche se, nel caso in cui la decisione sia presa da una p.a., la norma del Regolamento costituisce diretta applicazione*

[146] Giudice di pace di Empoli, Sez. I, 18 marzo 2026, n. 32. In motivazione: "La giurisprudenza è costante nel ritenere che "la mera implementazione di un sistema di autenticazione forte non esonera la banca dalla responsabilità se tale sistema si rivela inefficace nel prevenire le frodi" (Cfr. Cass. civ., Sez. I, ordinanza n. 29852/2023; Trib. Padova, sentenza n. 2309/2023). Più nello specifico, la Banca non ha fornito alcuna prova documentale dell'esistenza di sistemi automatizzati di rilevamento delle operazioni anomale, quali algoritmi di intelligenza artificiale o machine learning capaci di identificare transazioni sospette in base ai comportamenti abituali del cliente. Nel caso di specie, l'operazione fraudolenta presentava molteplici red flags che avrebbero dovuto far scattare immediatamente un allarme: il bonifico è stato disposto alle ore 04:46 del mattino, orario assolutamente inconsueto per qualsiasi operazione bancaria legittima; il beneficiario nuovo: la Sig.ra (omissis) non era mai stata utilizzata come beneficiaria dal Sig. (omissis) precedenza; IBAN estero: il conto di destinazione era intestato in (omissis)) elemento che avrebbe dovuto imporre controlli rafforzati ai sensi della normativa antiriciclaggio; importo rilevante: Euro 2.700,00 rappresentano una somma significativa per un correntista privato. Qualsiasi banca dotata di sistemi di sicurezza adeguati avrebbe bloccato automaticamente questa operazione, richiedendo una verifica aggiuntiva al cliente prima di procedere all'esecuzione. La banca non lo ha fatto. La giurisprudenza ha chiaramente affermato che "la banca ha l'obbligo di monitorare l'operatività dei conti correnti e di bloccare preventivamente le operazioni anomale rispetto alle abitudini del correntista"(cfr. Trib. Milano, sentenza n. 5967/2022; Trib. Roma, sentenza n. 16478/2022)". Sentenza estratta dalla banca dati *De jure*.

specifica dell'art. 42 della Carta Europea dei Diritti Fondamentali ("Right to a good administration"), laddove afferma che quando la Pubblica Amministrazione intende adottare una decisione che può avere effetti avversi su di una persona, essa ha l'obbligo di sentirla prima di agire, di consentirle l'accesso ai suoi archivi e documenti, ed, infine, ha l'obbligo di "dare le ragioni della propria decisione". Tale diritto alla conoscenza dell'esistenza di decisioni che ci riguardino prese da algoritmi e, correlativamente, come dovere da parte di chi tratta i dati in maniera automatizzata, di porre l'interessato a conoscenza, va accompagnato da meccanismi in grado di decifrarne la logica. In tale ottica, il principio di conoscibilità si completa con il principio di comprensibilità, ovverosia la possibilità, per riprendere l'espressione del Regolamento, di ricevere "informazioni significative sulla logica utilizzata". 11.2 In secondo luogo, l'altro principio del diritto europeo rilevante in materia (ma di rilievo anche globale in quanto ad esempio utilizzato nella nota decisione Loomis vs. Wisconsin), è definibile come il 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.). 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. 11.3 In terzo luogo, dal considerando n. 71 del Regolamento 679/2016 il diritto europeo trae 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.*** *In tale contesto, pur dinanzi ad un algoritmo conoscibile e comprensibile, non costituente l'unica motivazione della decisione, occorre che lo stesso non assuma carattere discriminatorio. In questi casi, come afferma il considerando, occorrerebbe rettificare i dati in "ingresso" per evitare effetti discriminatori nell'output decisionale; operazione questa che richiede evidentemente la necessaria cooperazione di chi istruisce le macchine che producono tali decisioni.".*

Parallelamente, la giurisprudenza della Corte di Giustizia dell'Unione Europea ha progressivamente definito i contorni del **danno risarcibile da violazione del GDPR**, chiarendo – con la sentenza del 4 ottobre 2024 in causa C-200/23 – che anche una perdita

di controllo sui dati personali di durata limitata può integrare un danno immateriale risarcibile, purché concretamente dimostrata dall'interessato. Molto più cospicua, invece, è la giurisprudenza statunitense in materia di danno cagionato dall'utilizzo di sistemi di IA generativa dove, in particolare, si è posta la questione problematica dell'imputabilità del danno al produttore del sistema di intelligenza artificiale. Tra questi il caso M. Garcia v. CharacterAI, Google, Alphabet et Inc[147], nonché il caso M. Raine and M. Raine v. OpenAI[148], su c.d. *chatbot* che avrebbero istigato degli utenti (minori d'età) al suicidio. Vi è poi il caso dei «META AI papers», documenti concernenti le linee guida della società META con cui si suggerisce una gestione "disinvolta" del rischio che i propri *chatbot* generino *output* consistenti in conversazioni romantiche e/o a sfondo sessuale[149]. Molto noto, inoltre, è il caso Moffatt v. Air Canada, deciso dal British Columbia Civil Resolution Tribunal del 14 febbraio 2024[150], nel quale la compagnia aerea canadese era stata chiamata a rispondere delle errate informazioni fornite in una conversazione tra il sistema di chatbot, integrato nel sito della compagnia aerea, e un cliente, relative alla possibilità di richiedere l'applicazione di tariffe praticate per viaggi dovuti a lutti familiari anche retroattivamente, ovverosia dopo aver acquistato il biglietto aereo corrispondendo la tariffa ordinaria ed aver effettuato il viaggio. Questa decisione, invero, ha ritenuto che dell'errore del chatbot – che nel caso concreto aveva suggerito una procedura di rimborso della tariffa corrisposta dal cliente, rivelatasi non applicabile in base alle condizioni contrattuali praticate dal vettore – dovesse rispondere la compagnia aerea, a titolo di falsa rappresentazione colposa ("*negligent misrepresentation*"),avendo il cliente orientato le proprie scelte facendo affidamento sulle informazioni così ricevute[151].

Il riferimento alla responsabilità extracontrattuale, così come quello alla responsabilità contrattuale, appare generico e non viene "agganciato" a specifici articoli del codice civile. In senso restrittivo potrebbe ritenersi che il riferimento alle azioni di risarcimento del danno, "**sia contrattuale sia extracontrattuale**" sia da ricondursi esclusivamente agli **artt. 1218** e **2043** c.c. in quanto l'assenza di riferimenti normativi specifici non potrebbe che riferirsi alle

[147] United States District Court, M.D. Florida, MEGAN GARCIA, individually and as the Personal Representative of the Estate of S.R.S. III, Plaintiff, v. CHARACTER TECHNOLOGIES, INC., NOAM SHAZEER, DANIEL DE FRIETAS, GOOGLE LLC, and ALPHABET INC., Defendants, Case No. 6:24-cv-1903-ACC-UAM Decided: May 21, 2025 in https://caselaw.findlaw.com/court/us-dis-crt-m-d-flo-orl-div/117299600.html .

[148] Il caso Matthew e Maria Raine contro OpenAI (depositato il 26 agosto 2025 presso il tribunale di San Francisco) è la prima causa per morte colposa contro l'azienda. I genitori accusano ChatGPT-4o di aver agito come un "coach al suicidio" per il figlio sedicenne Adam, morto l'11 aprile 2025. La Raine v. OpenAI Complaint sostiene che ChatGPT abbia convalidato i pensieri suicidi di Adam, fornito istruzioni dettagliate (incluso il supporto per configurare un cappio), offerto di scrivere il biglietto d'addio e lo abbia dissuaso dal confidarsi con la madre. In pratica l'accusa dei genitori nei confronti della società produttrice dell'IA è quella di aver rimosso i giusti blocchi di sicurezza per favorire l'interazione e l'attaccamento emotivo degli utenti. Per approfondimenti vedasi https://www.law.berkeley.edu/wp-content/uploads/2025/09/Raine-v-OpenAI.pdf.

[149] https://www.corriere.it/tecnologia/25_agosto_17/i-chatbot-possono-coinvolgere-i-bambini-in-conversazioni-a-sfondo-sessuale-e-bufera-sul-documento-di-meta-c653a401-b7e9-457b-8d18-8acf0ae02xlk.shtml.

[150] La pronunzia è liberamente consultabile in https://www.canlii.org/en/bc/bccrt/doc/2024/2024bccrt149/2024bccrt149.html.

[151] Così, British Columbia Civil Resolution Tribunal, 14 febbraio 2024, Moffatt v. Air Canada, 2024 BCCRT 149, in particolare, par. 24 ss. Al paragrafo 27, peraltro, dinanzi all'affermazione, svolta da Air Canada, secondo la quale «the chatbot is a separate legal entity that is responsible for its own actions» il giudice canadese afferma che «this is a remarkable submission. While a chatbot has an interactive component, it is just a part of Air Canada's website. It should be obvious to Air Canada that it is responsible for all the information on its website. It makes no difference whether the information comes from a static page or a chatbot».

sole ipotesi paradigmatiche di "**responsabilità del debitore**" e di "**risarcimento per fatto illecito**" in quanto, secondo "*l'id quod plerumque accidit*", le azioni risarcitorie riconducibili all'**art. 1218** e all'**art. 2043 c.c.** sono quelle normalmente più frequenti e possono ricondursi ad esse anche le fattispecie relative al risarcimento del danno da utilizzo illecito di sistemi di intelligenza artificiale. Anche l'interpretazione letterale della disposizione farebbe propendere per l'opzione interpretativa più restrittiva. In realtà il riferimento generico alle azioni risarcitorie da responsabilità contrattuale e da fatto illecito evidenzia, invece, l'intenzione del legislatore[152] di estendere al massimo la tutela del danneggiato ad ogni fatto od atto che abbia cagionato "*non ius*" e "*contra iure*" delle conseguenze patrimoniali e non patrimoniali derivanti dall'utilizzo di sistemi di intelligenza artificiale. Del resto, come già accennato, nel preambolo[153] del d.lgs.n.160/26 il legislatore delegato fa espresso riferimento agli artt. **2050** e **2051** c.c. nonché all'art. **116** c.p.c. e, quindi, non solo all'art. **2043** c.c., ossia alla norma paradigmatica della responsabilità aquiliana, ma anche agli articoli disciplinanti le ipotesi di responsabilità speciale dove, come noto, è la parte danneggiante a dover provare **di avere adottato tutte le misure idonee a evitare il danno**[154] (**2050** c.c.) ovvero a provare il **caso fortuito**[155], al fine di evitare il risarcimento del danno (**2051** c.c.).

In definitiva l'opzione più estensiva appare, certamente, quella preferibile: la lettera della disposizione, che è criterio prioritario nell'interpretazione *ex* **art. 12** delle **preleggi**, fa riferimento alle **azioni** e non a riferimenti normativi limitati; non sono citati articoli di legge, ma **fattispecie** (**contrattuale ed extracontrattuale**) con la conseguenza di voler ampliare, volutamente, la tutela ricomprendendo ogni fattispecie; se la "*voluntas legis*" fosse stata diversa, allora sarebbero stati menzionati articoli determinati. Di conseguenza, deve ritenersi che l'inciso va decodificato nel senso che, tanto che vi sia un vincolo negoziale e tanto che non via sia, **in ogni caso** la tutela del danneggiato è assicurata ove sussistano tutti i presupposti per ottenere il risarcimento del danno. Del resto, la rubrica del Capo II "***Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale***", dove sono situati gli artt. da 16 a 20, evidenzia chiaramente che le disposizioni sono finalizzate ad adattare il processo civile alle controversie risarcitorie da utilizzo illecito dei sistemi di intelligenza artificiale. La scelta appare particolarmente significativa se confrontata con la legge delega.

L'**art**. **24**, **comma 5**, **lett. d)**, della **l. n. 132 del 2025,** del resto, aveva demandato al Governo, nei casi di responsabilità civile, la previsione di strumenti di tutela del danneggiato, anche mediante una specifica regolamentazione della ripartizione dell'onere della prova,

[152] Art. 12 preleggi: "Nell'applicare la legge non si può ad essa attribuire altro senso che quello fatto palese dal significato proprio delle parole secondo la connessione di esse, **e dalla intenzione del legislatore**. Se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe; se il caso rimane ancora dubbio, si decide secondo i principi generali dell'ordinamento giuridico dello Stato".

[153] Visto il r.d. 28 ottobre 1940, n. 1443, recante «Codice di procedura civile» e, in particolare, l'articolo 116;
Visto il r.d. 16 marzo 1942, n. 262, recante «Approvazione del testo del Codice civile», e, in particolare, gli articoli 2050 e 2051;".

[154] Cass.,Sez. 3 n. 19872 del 22/09/2014 (Rv. 632680-01).

[155] Cass., Sez. 3 n. 16177 del 25/05/2026 (Rv. 678369-01).

tenendo conto della classificazione dei sistemi di IA e degli obblighi previsti dal regolamento IA. Restano utilizzabili, in definitiva, secondo le caratteristiche della fattispecie concreta, le ordinarie categorie della responsabilità contrattuale ed extracontrattuale e le discipline speciali concorrenti. La stessa impostazione del decreto legislativo è coerente con tale conclusione, come dimostra anche il richiamo, nelle premesse, agli **artt. 2050 e 2051 c.c**. e all'art. **116 c.p.c**..

Il sistema delineato dal legislatore delegato si sposta, pur in assenza di uno "statuto" autonomo della responsabilità da Intelligenza Artificiale, verso modelli di natura **oggettiva** od **aggravata** per rispondere in maniera efficace all'opacità del fenomeno tecnologico. L'art. **2050 c.c.**, relativo all'esercizio di attività pericolose, appare particolarmente idoneo a disciplinare i danni derivanti da sistemi di IA ad alto rischio[156], poiché la pericolosità intrinseca di tali strumenti (proprio perché restano, allo stato, ancora sconosciuti i riverberi di tali intelligenze sul trattamento dei dati delle persone e, più in generale, sulla capacità di autodeterminazione degli utilizzatori nonché sulla genuinità ed affidabilità degli *output*), sposta l'onere della prova sulla capacità del convenuto danneggiante di aver adottato tutte le misure idonee a evitare l'evento dannoso. Parallelamente, l'articolo **2051** c.c. sulla responsabilità da cosa in custodia viene invocato laddove l'utilizzatore mantenga il controllo effettivo sul sistema, sebbene la dottrina discuta se il controllo remoto del produttore possa elidere tale nesso[157].

Parte della dottrina ritiene, invece, che la responsabilità extracontrattuale da utilizzo di sistemi di intelligenza artificiale sia da ricondursi all'art. **2049** c.c.[158]. Si afferma che chi inserisce stabilmente un sistema di IA nella propria organizzazione e ne trae utilità - il **deployer** - potrebbe rispondere dei danni come per il fatto dell'ausiliario umano. Si tratta della tesi del «**preposto artificiale**»[159]: l'intelligenza artificiale diviene quindi un preposto (artificiale) del *deployer* il quale ne risponde qualora l'*ouput* generato abbia provocato un danno ingiusto a terzi. L'art. **2049** c.c. disciplina, come noto, la responsabilità dei "padroni e committenti", nel caso di danno cagionato a terzi da un fatto illecito dei loro "domestici o dipendenti", nell'esercizio delle "*incombenze a cui sono adibiti*". Si è in presenza, quindi, di un caso di responsabilità indiretta, che non prevede alcuna prova liberatoria per il preponente[160]. La tesi non appare pienamente convincente in quanto l'intelligenza artificiale non ha soggettività giuridica dato che, è notorio, l'intelligenza artificiale non è altro che una "**imitazione artificiale**" di facoltà umane ma non è, essa stessa, un soggetto cui imputare diritti e doveri. L'**art. 2049 c.c.** presuppone, infatti, che "*i padroni e i committenti*" sono

---

[156] T. BONAMINI, *Criteri di rischio e regole di responsabilità nell'utilizzo dell'intelligenza artificiale*, in Rivista Bio Diritto (Università di Trento), fasc. 1 2026, pag.330 e ss..
[157] T. BONAMINI, *cit*., par.4, pag.340 e ss..
[158] G.P. CIRILLO, *I soggetti giuridici digitali*, in *Contratto e impr*., 2020, 2, 573 ss..
[159] Nella risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), il Parlamento europeo aveva aperto all'ipotesi di istituire i robot autonomi più sofisticati - quelli che prendono decisioni autonome o che interagiscono in modo indipendente con terzi - come persone elettroniche, in modo da renderli «responsabili di risarcire qualsiasi danno da loro causato […]» (vedasi punto 59).
[160] Vedasi, tra le tante, Cass., Sez. 3 n. 28988 dell'11/11/2024 (Rv. 672996-01); Cass., Sez. 3 n. 18184 del 28/08/2007 (Rv. 599157-01).

responsabili per i danni arrecati dal fatto illecito che sia riconducibile ad una condotta (ovvero al mancato attivarsi in caso di condotta omissiva) dei "loro" commessi e domestici presupponendo una attività umana che abbia inciso nella realtà materiale. Questa impostazione si basa su quell'orientamento dottrinale tedesco[161] ed americano che ritiene i sistemi di intelligenza artificiale come «**persone elettroniche**[162]». Tale soluzione però non riuscirebbe ad eliminare il problema – di cui l'imputazione materiale del danno è solo strumentale – di individuare il patrimonio[163] mediante il quale riparare il pregiudizio patito dal terzo danneggiato; se non addirittura dannosa, poiché dietro la "*personalità elettronica*" del sistema di IA, si determinerebbe una limitazione della responsabilità patrimoniale dei soggetti potenzialmente coinvolti nel fatto dannoso (il fabbricante, il fornitore, l'operatore o il *deployer*), con proporzionale riduzione degli incentivi all'adozione di adeguate cautele e precauzionali finalizzate ad evitare il rischio di fatti illeciti determinati da sistemi di IA[164].

Per quanto concerne la circolazione dei veicoli autonomi, il quadro normativo si fonda sull'articolo **2054** c.c., che al **comma 4,** stabilisce una responsabilità "blindata" e oggettiva del proprietario e del conducente per i danni derivanti da vizi di costruzione (tra cui anche quelli "indotti" da sistemi algoritmici), lasciando a questi ultimi la possibilità di agire in regresso verso il produttore.

Sul punto non può non farsi cenno alla decisione del Tribunale di Milano che, con sentenza del 13.2.2023, n. 1116, ha parzialmente accolto la domanda spiegata dal rappresentante legale di una s.r.l. che, mentre era alla guida di un'automobile Tesla, aveva urtato l'auto che la precedeva, asseritamente a causa della mancata attivazione del sistema di frenata automatica di emergenza. All'esito della CTU disposta dal giudice, è stato accertato che il sistema di frenata automatica aveva funzionato in materia diversa rispetto a quanto previsto nel manuale, atteso che esso non era intervenuto tempestivamente. Il Giudice, nell'accertare un concorso di colpa del conducente nella causazione dell'evento (atteso che non era stata rispettata la distanza di sicurezza con la vettura danneggiata), ha precisato che "indipendentemente dal fatto, notorio, che tale tecnologia non è ancora del tutto perfezionata, si deve affermare che permane in ogni caso sul conducente l'onere di esercitare tutta la prudenza del caso nel condurre il veicolo, e comunque l'onere di rispettare le norme che regolano la circolazione stradale di mezzi a motore". Molto attuale e rilevante è stato poi il caso Neima Benavides e Dillon Angulo v. Tesla, deciso dalla United States District Court, Southern District of Florida (case n. 1:21-cv-21940, 1° agosto 2025), nel quale si è discussa la rilevanza, ai fini della applicazione di un corretto regime di responsabilità, del sistema di

---

[161] G.WAGNER, *Forschungsinstitut für Recht und digitale Transformation*, Working Paper Series, 2019, www.rewi.huberlin. de/de/lf/oe/rdt/pub/working-paper-no-2, 22, secondo cui la creazione di un'autonoma entità giuridica può contribuire a limitare la responsabilità di produttori e degli utenti che contribuiscono all'azione lesiva e stimolarli ad assumere più rischi a costi inferiori, in modo simile a quanto avviene con le società di capitali.

[162] R. ROLLI, *L'intelligenza artificiale e le perduranti insidie della soggettività giuridica. Personalità elettronica, processi decisionali degli amministratori e business judgement rule: verso un'AI judgement rule?,* in Rivista delle Società, fasc. 4, 1° agosto 2025, pag. 663.

[163] G. ALPA, *Quale modello normativo per l'intelligenza artificiale?,* in Contratto e impr., 2021, 1003 ss..

[164] M.W. MONTEROSSI, *Il risarcimento dei danni da intelligenza artificiale nello spettro della responsabilità "vicaria",* in Jus Civile, 2024, n. 1., pag. 192 e ss..

autopilot, implementato dalla nota produttrice di veicoli elettrici, rilevando come, nella causazione del decesso di uno dei due attori, e delle gravi lesioni dell'altro, fosse imputabile al difetto del **sistema di guida autonoma**, e, quindi, al produttore, che lo aveva ideato e implementato, il 33% del danno cagionato[165].

A livello unionale, la nuova Direttiva PL (**2024/2853**) ha esteso, come già accennato, la nozione di prodotto includendovi, all'**art. 4**[166], espressamente i *software* e i *file* per la fabbricazione digitale, consolidando un regime di **responsabilità oggettiva** del produttore per i danni causati da difetti dei sistemi di IA (vedasi l'**art. 10**[167], rubricato proprio "onere della prova"). La prova della difettosità e del nesso causale può essere facilitata da presunzioni semplici, come già ammesso dalla giurisprudenza di legittimità in ambiti complessi (Cass. civ. n. 13458/2013; Cass. civ. n. 34027/2022) e dalla Corte di Giustizia UE, la quale ha affermato che la difettosità può essere presunta in presenza di un malfunzionamento di prodotti della stessa serie (Corte Giust. UE, 5 marzo 2015, cause riunite C-503/13 e C-504/13). Infine, l'adempimento agli obblighi di trasparenza e sorveglianza umana previsti dal regolamento IA funge da parametro per valutare la colpa del *deployer*, pur non escludendo di per sé la responsabilità in caso di danno effettivo. Al riguardo occorre rilevare che l'**art. 11** del d.lgs. n. 160/26 rinvia alle definizioni indicate nell'**art. 3** del **regolamento (UE) 2024/1689** (regolamento IA) e l'utilizzo del cosiddetto "rinvio dinamico" ad altra fonte normativa viene giustificata nella Relazione Illustrativa per evitare duplicazioni definitorie e per garantire piena uniformità terminologica con il quadro eurounitario, "*in coerenza con le indicazioni del § 3 della circolare PCM 2001 in tema di rapporti fra atti normativi. Per tale via, in particolare, le nozioni di "**sistema di intelligenza artificiale**", "**fornitore**", "**deployer**", "**modello di IA per finalità generali**" e "**sistema ad alto rischio**" assumono nel presente decreto il medesimo significato che rivestono nel regolamento*".

Ai fini delle disposizioni del Titolo II appaiono di particolare rilevanza, in particolare, le seguenti definizioni recate dall'**art. 3** del regolamento IA. Con riguardo alle disposizioni sulla responsabilità civile, che fanno leva sul sistema di IA rilevano le nozioni di: «**sistema di IA**»

---

[165] La pronunzia è liberamente consultabile in https://law.justia.com/cases/federal/district-courts/florida/flsdce/1:2021cv21940/593426/433/.

[166] Art. 4., n.1 «prodotto», del regolamento (UE) 2024/2853:"ogni bene mobile, anche se integrato in un altro bene mobile o in un bene immobile o interconnesso con questi; include l'elettricità, i file per la fabbricazione digitale, le materie prime e il software; n.2: «file per la fabbricazione digitale»: una versione digitale di un bene mobile o un modello digitale per un bene mobile contenente le istruzioni funzionali necessarie per produrre un bene tangibile consentendo il controllo automatizzato di macchine o strumenti.".

[167] Art. 10 del regolamento (UE) n.2024/2853: "Gli Stati membri provvedono affinché l'attore sia tenuto a provare il carattere difettoso del prodotto, il danno subito e il nesso di causalità tra il difetto e il danno.2. Si presume il carattere difettoso di un prodotto qualora sia soddisfatta una delle seguenti condizioni: a) il convenuto omette di divulgare i pertinenti elementi di prova a norma dell'articolo 9, paragrafo 1; b) l'attore dimostra che il prodotto non rispetta i requisiti obbligatori di sicurezza del prodotto stabiliti dal diritto dell'Unione o nazionale intesi a proteggere dal rischio del danno subito dal danneggiato; o c) l'attore dimostra che il danno è stato causato da un malfunzionamento evidente del prodotto durante l'uso ragionevolmente prevedibile o in circostanze ordinarie. 3.Si presume l'esistenza del nesso di causalità tra il carattere difettoso del prodotto e il danno nel caso in cui sia stato provato che il prodotto è difettoso e che la natura del danno cagionato è compatibile con il difetto in questione. 4. L'organo giurisdizionale nazionale presume il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno, o entrambi, qualora, nonostante la divulgazione di prove a norma dell'articolo 9 e tenuto conto di tutte le circostanze pertinenti del caso: a) l'attore incontri difficoltà eccessive, in particolare a causa della complessità tecnica o scientifica, nel provare il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno o entrambi; e b) l'attore dimostri che è probabile che il prodotto sia difettoso o che esista un nesso di causalità tra il carattere difettoso del prodotto e il danno, o entrambi. 5. 1. Il convenuto ha il diritto di confutare le presunzioni di cui ai paragrafi 2, 3 e 4.".

(art. 3, punto 1): 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 dagli input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali; «**fornitore**» (articolo 3, punto 3): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che sviluppa, o fa sviluppare, un sistema di IA o un modello di IA per finalità generali e lo immette sul mercato o mette in servizio il sistema con il proprio nome o marchio, a titolo oneroso o gratuito; «**importatore**» (articolo 3, punto 6): una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona stabilita in un paese terzo; «**distributore**» (articolo 3, punto 7): una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione; «***deployer***» (articolo 3, punto 4): una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, salvo che il sistema sia utilizzato nel corso di un'attività personale non professionale; «**operatore**» (articolo 3, punto 8): un fornitore, un fabbricante del prodotto, un deployer, un rappresentante autorizzato, un importatore o un distributore; «**modello di IA per finalità generali**» (articolo 3, punto 63): un modello di IA – anche addestrato con grandi quantità di dati mediante autosupervisione su larga scala – caratterizzato da una generalità significativa e in grado di svolgere con competenza un'ampia gamma di compiti distinti, integrabile in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli utilizzati per attività di ricerca, sviluppo o prototipazione prima dell'immissione sul mercato.

L'**art. 16**, **comma 1**, fa riferimento al "**danno**", senza ulteriori precisazioni. Tale difetto di precisazione, alla luce dell'interpretazione letterale della disposizione e dell'intenzione del legislatore (oltreché del brocardo/principio "*Ubi lex voluit dixit, ubi noluit tacuit*"), va inteso in senso ampio: trattasi di qualsiasi danno patrimoniale e non patrimoniale, nella duplice veste di perdita subita e di mancato guadagno *ex* **art. 1223 c.c.**, nonché di danno nascente da qualsiasi fonte di obbligazioni *ex* **art. 1173 c.c.**. Il danno, afferma poi la disposizione, deve essere *cagionato nell'utilizzo di un sistema di intelligenza artificiale*. La disposizione, quindi, esclude che il danno possa essere cagionato "*ex se*" dalla intelligenza artificiale. Del resto, non è l'uso "*ex se*" a cagionare danni e lo stesso uso lecito dell'IA non potrebbe essere un danno: è l'eventuale *output* prodotto dalla I.A. che potrebbe, ad esempio, causare danni. Pertanto, l'inciso *cagionato* nell'utilizzo va inteso in senso temporale e probatorio[168]: si dovrà provare che il danno si è verificato a causa degli *output* ottenuti durante l'utilizzo della I.A.. L'espressione «*nell'utilizzo*» sembra comprendere non soltanto il danno direttamente prodotto dall'*output* ma anche quello derivante dall'integrazione dell'IA in un processo decisionale o organizzativo. Potrebbero, pertanto, rientrare nell'ambito della disciplina: il danno direttamente riconducibile a un ***output* errato**; il danno causato dall'**affidamento**

[168] L. VIOLA, *Primo approfondimento sul d.lgs. 160/2026:Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale*, in La nuova procedura civile, 09.26.

dell'operatore sull'output; il danno derivante dall'**omessa verifica umana**; il danno prodotto da una **configurazione inadeguata**; il danno connesso all'i**mpiego di dati inesatti o non rappresentativi**; il danno derivante da un **uso difforme dalla destinazione prevista**; il danno prodotto dall'**interazione tra più sistemi**; il danno riconducibile a una **carente organizzazione della sorveglianza**.

La disposizione necessita, però, di una corretta delimitazione del suo ambito applicativo. Non ogni danno verificatosi in un'attività nella quale sia stato utilizzato un sistema di IA deve necessariamente ricadere nella disciplina speciale del **d.lgs. n. 160**. Occorre che il sistema abbia assunto una rilevanza funzionale e causalmente apprezzabile nella produzione dell'evento. Sarebbe da ritenersi restrittivo esigere che il **danno** sia stato prodotto esclusivamente dal sistema, poiché le decisioni algoritmiche sono normalmente inserite in processi complessi. Sarebbe invece troppo estensivo ritenere sufficiente che l'IA abbia rappresentato una mera occasione della condotta umana. L'attività dell'interprete dovrà consistere nel verificare **se il funzionamento, l'*output*, la configurazione o l'impiego del sistema abbiano inciso in modo non marginale sul processo causale**. Ciò assume rilevanza per qualsiasi I.A. generativa generalista oppure verticalizzata ed anche per quella c.d. agentica. La disposizione appare, quindi, applicabile tanto nei casi in cui il danneggiato sia l'utilizzatore, che un "*quisque de populo*" estraneo (ad es. nei casi di I.A. agentica) e questo perché il danno può essere di matrice contrattuale oppure extracontrattuale.

Come noto, l'**IA generativa** si riferisce a modelli che creano contenuti come testo, immagini, codice, audio o video, sulla base di pattern appresi dai dati. I sistemi di **IA agentica** pianificano, decidono e agiscono autonomamente per raggiungere obiettivi, spesso utilizzando l'IA generativa come uno dei componenti, per eseguire attività e ottimizzare processi aziendali. Sebbene l'AI agentica consenta un'esecuzione completamente autonoma, la maggior parte degli agenti in produzione opera con meccanismi di salvaguardia "*human-in-the-loop*". L'AI generativa risponde a *prompt*, mentre l'AI agentica avvia e adatta processi complessi. I sistemi di AI agentica sono sistemi, non modelli, che combinano *LLM,* IA tradizionale, strumenti AI, sistemi di memoria e logica di controllo in un *loop* in grado di pianificare, agire, osservare e adattarsi autonomamente. Consentono agli agenti IA di percepire gli ambienti, ragionare su problemi complessi, compiere azioni e imparare dall'esperienza. Esempi di AI agentica sono gli "Assistenti di shopping autonomi", ossia gli Agenti che non si limitano a consigliare un prodotto, ma verificano in tempo reale la disponibilità in magazzino, applicano codici sconto, concludono l'acquisto e tracciano la spedizione; gli Agenti che analizzano il comportamento di spesa di un cliente con una carta di credito e preparano o inviano in autonomia offerte pre-approvate e personalizzate al momento giusto; gli Agenti che monitorano i server, rilevano un'anomalia nel codice, scrivono una patch, testano la correzione in un ambiente sicuro e aprono una richiesta di "merge" senza intervento umano costante. L'**IA verticalizzata** ("*Vertical IA*") è, invece, un sistema di IA non generalista (come Copilot e ChatGPT) che nasce con una conoscenza profonda dei flussi di lavoro, dei termini tecnici e delle normative di un singolo settore (es. legale, medico, edilizio

o finanziario). Si tratta, quindi, di una intelligenza artificiale con conoscenze particolarmente profonde in determinati settori, come quello legale, commerciale, sanitario, ecc. . In medicina, ad esempio, un'IA addestrata esclusivamente su milioni di mammografie e referti oncologici è utile per assistere i radiologi nell'individuazione precoce dei tumori mentre, nel settore della ristorazione, vi sono dei sistemi integrati di IA nei registratori di cassa e nei gestionali d'ordinazione al fine di prevedere i flussi di clienti, ottimizzare le scorte in dispensa e gestire i turni del personale in base al meteo o agli eventi locali.

Il **danno**, quindi, deve essere cagionato dall'utilizzo di uno dei sistemi di intelligenza artificiale anzidetti ossia anche soltanto "occasionato" da un ***output*** "falso", "non corretto", "allucinato", che sia stato causa di un danno a terzi o allo stesso utilizzatore cagionandogli delle conseguenze dannose patrimoniali e non patrimoniali.

Come noto, l'accertamento del nesso causale a fronte di domanda risarcitoria in tema di responsabilità civile aquiliana, secondo i quali il nesso causale è regolato dal principio di cui agli artt. 40 e 41 c.p., è governato dal principio secondo il quale un evento è da considerare causato da un altro se il primo non si sarebbe verificato in assenza del secondo, nonché dal criterio della cosiddetta causalità adeguata, sulla base del quale, all'interno della serie causale, occorre dar rilievo solo a quegli eventi che non appaiano - ad una valutazione "ex ante" - del tutto inverosimili, con la precisazione che, nell'accertamento del nesso causale in materia civile, vige la regola della preponderanza dell'evidenza o del "***più probabile che non***", mentre nel processo penale vige la regola della prova "oltre il ragionevole dubbio" (Cass. Sez. U, n. 576 dell'11/01/2008), ciò perché «*In tema di illecito aquiliano perché rilevi il nesso di causalità tra una condotta e l'evento lesivo deve ricorrere, secondo la combinazione dei principi della "condicío sine qua non" e della causalità efficiente, la duplice condizione che si tratti di una condotta antecedente necessaria dell'evento e che la stessa non sia poi neutralizzata dalla sopravvenienza di un fatto di per sé idoneo a determinare l'evento stesso.*» (Cass. n. 23915 del 22/10/2013; cfr. Cass. n. 23197 del 27/09/2018), tenendo conto che «*lo standard di cd. certezza probabilistica in materia civile non può essere ancorato esclusivamente alla cd. probabilità quantitativa della frequenza di un evento, che potrebbe anche mancare o essere inconferente, ma va verificato, secondo la cd. probabilità logica, nell'ambito degli elementi di conferma, e, nel contempo, nell'esclusione di quelli alternativi, disponibili in relazione al caso concreto.*» (Cass. n. 47 del 3/01/2017).

Nelle azioni di risarcimento del danno *cagionato* dall'utilizzo di sistemi di intelligenza artificiale avrà un sicuro rilievo l'**art. 1227**, **commi 1**[169] e **2**[170], **c.c.**, che disciplina il concorso del fatto colposo del creditore (applicabile anche in sede di responsabilità aquiliana in virtù del rinvio operato dall'art. **2056 c.c.**). Va osservato infatti che ogni professionista che utilizza sistemi di intelligenza artificiale è tenuto ad una particolare "diligenza qualificata" che consiste, in particolare, nell'obbligo di controllare i "prodotti" generati dall' intelligenza artificiale e, se tale obbligo di controllo viene omesso, qualora abbia subito un danno

[169] Vedasi, da ultimo, Cass., Sez. 3, n. 2352 del 4/02/2026 (Rv. 677825-01)
[170] Vedasi, tra le tante, Cass., Sez. 3, n. 24522 del 5/10/2018 (Rv. 651135-01)

provocato da un difetto dell'*output* il risarcimento del danno potrebbe essere diminuito in ragione del **comma 1**[171] dell'art .**1227**.

Il comma 1 dell'art. 1227 c.c. potrebbe trovare applicazione in tutte quelle fattispecie in cui l'utilizzatore, pur avvalendosi legittimamente del sistema di IA, ne fa un uso che concorre a determinare l'evento dannoso senza tuttavia escludere l'imputabilità del **produttore** o **dell'importatore** ovvero **fornitore** del sistema di IA. L'ambito applicativo del comma 1 potrebbe riferirsi, in particolare, all'**utilizzatore professionale** (avvocato, medico, commercialista, consulente del lavoro, architetto, ecc.) che impiega l'*output* di un sistema di IA generativa come base per un parere o una decisione senza effettuare alcuna verifica critica, in un contesto in cui l' "ordinaria diligenza" richiesta dalla natura dell'attività (art. **1176**, **comma 2**, c.c.) imponeva un controllo accurato; **all'utente** che ignora avvertenze, limitazioni d'uso o ***disclaimer*** chiaramente rappresentati dall'interfaccia del sistema (ad esempio l'indicazione che l'output può contenere inesattezze e richiede verifica umana); all'**utilizzatore di un sistema di IA** che impiega il sistema al di fuori del perimetro d'uso dichiarato dal produttore (c.d. ***off-label use***), in assenza di autorizzazioni o controlli aggiuntivi (es. un magistrato che utilizza un sistema di IA che genera una sentenza, poi utilizzata dall'operatore, basata su fatti o principi di diritto inesistenti e che ha generato un danno patrimoniale e non patrimoniale ad una delle parti). In questi casi il giudice è chiamato ad un giudizio comparativo delle colpe, calibrato su due parametri testuali: la gravità della colpa dell'utilizzatore (che sarà tanto più elevata quanto più erano evidenti, accessibili e comprensibili gli avvertimenti del produttore, e quanto più qualificata era la posizione professionale del danneggiato) e l'entità delle conseguenze causalmente riconducibili alla sua condotta.

Il **comma 2**[172] dell'art. **1227** c.c. opera, come noto, su un piano distinto. Esso individua un vero e proprio onere di autoprotezione in capo al danneggiato: se questi avrebbe potuto, usando l'ordinaria diligenza, evitare (in tutto o in parte) il danno, quella componente di pregiudizio evitabile resta a suo carico, a prescindere dalla gravità dell'inadempimento o dell'illecito del produttore. Nelle azioni risarcitorie *ex* **art. 16**, **comma 1**, questo comma assume un particolare rilievo. Se il sistema di intelligenza artificiale mette a disposizione dell'utente strumenti, anche minimi, di controllo o di verifica – citazioni delle fonti, punteggi di confidenza, possibilità di "*cross-check*" – e l'utente non se ne avvale prima di utilizzare l'output in un contesto pregiudizievole per sé o per terzi, il danno che sarebbe stato evitabile con l'attivazione di tali strumenti non è risarcibile, indipendentemente dall'eventuale difettosità "a monte" del sistema. In altre parole, il comma 2 impone all'interprete di distinguere tra: il danno cd. "**originario**", riconducibile all'errore generato dal sistema (imputabile, in linea di principio, al produttore, salvo la graduazione di cui al comma 1); il danno "**evitabile**", cioè quella parte di pregiudizio che una condotta di ordinaria diligenza

[171] 1227, comma 1, c.c.: "Se il fatto colposo del creditore ha concorso a cagionare il danno, il risarcimento è diminuito secondo la gravità della colpa e l'entità delle conseguenze che ne sono derivate.".
[172] 1227, comma 2, c.c.: "Il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza.

dell'utilizzatore – tipicamente un controllo, una verifica incrociata, una sospensione cautelativa dell'azione basata sull'output – avrebbe consentito di scongiurare. In una ipotetica azione risarcitoria nei confronti di una azienda produttrice di sistemi IA quest'ultima dovrà, al fine di escludere la propria responsabilità, non soltanto dimostrare che l'utente ha agito con negligenza generica od imprudenza (ai fini del **comma 1**) ma, eventualmente, invocare l'esclusione totale della parte di danno *ex* **comma 2** provando puntualmente che l'evento dannoso, o una sua porzione autonomamente individuabile, era evitabile con un comportamento diligente, e che tale comportamento rientrava negli standard di diligenza ordinariamente esigibili nel contesto d'uso concreto. Di recente la Corte di cassazione[173], ribadendo il diverso ambito applicativo dei due commi dell'art. 1227, ha affermato che "*A differenza dell'ipotesi regolata dal comma 1 dell'art. 1227 c.c. - che concerne l'incidenza del comportamento colposo del creditore danneggiato nella determinazione del danno e rileva ai fini di una proporzionale riduzione del risarcimento - l'ipotesi disciplinata dal comma 2, in presenza di un fatto dannoso imputabile, sotto il profilo causale, al solo debitore, ne esclude la risarcibilità limitatamente alle conseguenze ulteriori che il creditore avrebbe potuto evitare con il proprio comportamento, successivo all'evento, cosicché, in relazione a tale ipotesi, il contegno del creditore va valutato - indipendentemente dalla violazione di obblighi contrattuali - sotto il profilo dell'eventuale omissione dell'ordinaria diligenza richiesta dal medesimo art. 1227 c.c..*".

4.5. Segue. L'art. 2055 c.c. nelle azioni di risarcimento del danno cagionato nell'utilizzo dei sistemi di intelligenza artificiale.

Un profilo destinato ad assumere particolare rilievo nelle controversie risarcitorie del danno cagionato dall'impiego di sistemi di intelligenza artificiale concerne l'applicazione dell'**art. 2055 c.c.**

La norma, secondo cui «*se il fatto dannoso è imputabile a più persone, tutte sono obbligate in solido al risarcimento del danno*», appare particolarmente adatta a governare una fenomenologia nella quale il pregiudizio lamentato dalla parte danneggiata può presentarsi come l'esito "unitario" dell'interazione di una pluralità di condotte, attività e omissioni riferibili a soggetti differenti. Il tratto peculiare dell'IA, sotto questo profilo, non consiste tanto nell'emersione di un nuovo criterio di responsabilità quanto nella possibile **frammentazione della sequenza causale e dei centri di imputazione**: progettazione del sistema, sviluppo del software, integrazione in un prodotto o in un servizio, alimentazione e gestione dei dati, aggiornamento, configurazione, supervisione e concreta utilizzazione possono concorrere, secondo modalità differenti, alla produzione dell'evento lesivo. L'**art. 2055 c.c.** può allora svolgere una funzione di "ricomposizione" sul piano dell'obbligazione risarcitoria, senza che sia necessario ricondurre tutti i concorrenti al medesimo titolo di responsabilità.

[173] Vedasi, Cass., Sez. 2, n. 10668 del 22/04/2026, (Rv. 678597-02).

L'art. 2055 c.c. non configura una responsabilità collettiva dell'ecosistema dell'intelligenza artificiale e non consente di chiamare a rispondere solidalmente tutti coloro che abbiano partecipato, a qualsiasi titolo, alla vita del sistema. La solidarietà presuppone l'accertamento che nei confronti di ciascun soggetto possa essere autonomamente individuato un criterio di imputazione della responsabilità e che il fatto a lui imputabile abbia assunto rilevanza causale rispetto al medesimo evento dannoso[174]. Solo dopo l'accertamento di tali elementi diviene possibile interrogarsi sulla **solidarietà**. In altri termini, l'art. 2055 c.c. non sostituisce le regole sull'*an* della responsabilità, ma interviene sull'obbligazione risarcitoria risultante dalla convergenza di più responsabilità (tutte extracontrattuali, o extracontrattuali e contrattuali) sull'unico danno[175]. Questa precisazione assume una particolare importanza nell'IA perché la solidarietà non richiede che le condotte dei diversi responsabili siano identiche, contestuali o previamente coordinate.

Sul piano generale, l'elaborazione della responsabilità solidale distingue, infatti, nettamente l'unicità del danno dalla possibile autonomia delle condotte e dei titoli di responsabilità. Non può non rilevarsi che quanto tecnicamente risulti unitario sotto il profilo dell'evento dannoso può essere, invece, giuridicamente riconducibile a una pluralità di antecedenti, ciascuno governato da un diverso criterio di responsabilità. Si comprende allora come una prima e importante area applicativa riguardi **il concorso tra difettosità del sistema e condotta colposa nell'utilizzazione**. Si ipotizzi che un sistema di IA presenti un difetto rilevante secondo la disciplina della responsabilità da prodotto e che, nello stesso tempo, il soggetto che lo utilizza abbia omesso una cautela alla quale era tenuto. Se l'evento dannoso costituisce il risultato della convergenza causale dei due fattori, l'eterogeneità delle fonti delle rispettive responsabilità non impone necessariamente di scomporre la pretesa risarcitoria della vittima in frazioni corrispondenti ai singoli apporti. Il problema dell'individuazione del responsabile e quello della solidarietà rimangono concettualmente distinti: ciascuna responsabilità deve trovare il proprio fondamento nella disciplina ad essa applicabile, mentre l'**art. 2055 c.c.** può ricondurre a unità gli effetti risarcitori delle responsabilità concorrenti[176].

A questa ipotesi può affiancarsi quella nella quale il danno derivi dalla concatenazione tra caratteristiche originarie del sistema e successive operazioni di integrazione, adattamento o configurazione. Il sistema potrebbe non risultare di per sé causalmente sufficiente alla

[174] Cass., civ., Sez. III, 14/06/2026, n. 19772 in Giustizia Civile Massimario 2026.
[175] Cass., civ., Sez. III, 29/05/2026, n. 16924 in Giustizia Civile Massimario 2026.
[176] Cass., Sez. III, n. 9969 del 16/04/2025, (Rv. 674633-01): "*Ai fini della responsabilità solidale di cui all'art. 2055, comma 1, c.c., norma sulla causalità materiale integrata nel senso dell'art. 41 c.p., è richiesto solo che il fatto dannoso sia imputabile a più persone, ancorché le condotte lesive siano fra loro autonome e pure se diversi siano i titoli di responsabilità - contrattuale ed extracontrattuale - in quanto la norma considera essenzialmente l'unicità del fatto dannoso e riferisce tale unicità unicamente al danneggiato, senza intenderla come identità delle norme giuridiche violate; la fattispecie di responsabilità implica che sia accertato il nesso di causalità tra le condotte, caso per caso, in modo da potersi escludere se a uno degli antecedenti causali possa essere riconosciuta efficienza determinante e assorbente tale da escludere il nesso tra l'evento dannoso e gli altri fatti, ridotti al semplice rango di occasioni. (Nella specie, la S.C. ha cassato la decisione di merito che aveva escluso una responsabilità solidale dell'agenzia immobiliare e del promittente venditore, in relazione alle domande restitutorie e risarcitorie proposte relativamente ad un contratto preliminare di vendita di immobile da costruire su un'area che, diversamente da quanto garantito, era in larga parte di proprietà di soggetti terzi).*".

produzione del danno, che si realizza soltanto quando le caratteristiche originarie interagiscono con l'ambiente tecnologico nel quale esso viene successivamente inserito. Analogamente, un determinato rischio potrebbe derivare dall'interazione tra le caratteristiche del modello, la configurazione concretamente prescelta e le modalità attraverso le quali gli output vengono utilizzati nel processo decisionale. In fattispecie di questo tipo il compito del giudice non sarebbe quello di individuare necessariamente un solo responsabile, ma **di verificare se gli apporti imputabili ai diversi soggetti abbiano assunto efficacia causale rispetto a un evento dannoso unitario**[177]. Un'ulteriore ipotesi può prospettarsi quando la produzione del danno dipenda dall'interazione tra difetto originario e omissione successiva di aggiornamenti o interventi correttivi, sempre che per ciascun soggetto interessato sussistano i presupposti dello specifico regime di responsabilità invocato. L'evoluzione temporale del sistema di IA rende infatti possibile che il rischio non sia staticamente localizzato nel momento della sua progettazione o immissione sul mercato, ma risulti dalla combinazione tra caratteristiche originarie e vicende successive. Anche in questa fattispecie la successione cronologica delle condotte non sarebbe, di per sé, incompatibile con l'art. 2055 c.c., qualora venga dimostrata la loro concorrente rilevanza causale rispetto al danno oggetto della domanda. Ancora più interessante è la possibilità che nella medesima vicenda concorrano titoli di responsabilità eterogenei, eventualmente anche contrattuali ed extracontrattuali. L'omogeneità del titolo non costituisce la ragione funzionale della solidarietà. Il problema decisivo rimane quello della riferibilità delle distinte condotte al medesimo pregiudizio. Il danneggiato potrebbe trovarsi in rapporto contrattuale con il soggetto che utilizza il sistema e, al tempo stesso, far valere nei confronti di altro operatore un diverso titolo di responsabilità. In questo senso l'art. 2055 c.c. assume una funzione di cerniera: non unifica i criteri di imputazione, che conservano la loro autonomia, ma può unificare l'obbligazione risarcitoria quando le responsabilità autonomamente accertate convergano sul medesimo danno. È proprio questa distinzione che consente di cogliere il significato dell'art. 2055 c.c. nell'ambito dell'IA. Pluralità dei titoli non significa necessariamente pluralità dei danni; così come pluralità dei fattori causali non significa necessariamente frazionamento dell'obbligazione risarcitoria. Si potrebbe avere una responsabilità fondata sul difetto del prodotto, una seconda derivante dall'inosservanza di un'obbligazione contrattuale e una terza riconducibile a una condotta colposa dell'utilizzatore. Ciò che deve essere accertato autonomamente è il fondamento di ciascuna responsabilità; ciò che consente successivamente di ricondurle alla solidarietà è la loro convergenza nella produzione dell'unico pregiudizio. Sotto questo profilo deve essere evitata anche la suggestione di attribuire all'autonomia del sistema di IA il significato di un nuovo centro soggettivo di imputazione. L'art. 2055 c.c. continua a operare rispetto ai soggetti cui il fatto

[177] Cass., civ., Sez. III, n. 19772 del 14/06/2026 (Rv. 678379-01), "*L'unicità del "fatto dannoso", richiesta dall'art. 2055, comma 1, c.c. per la configurabilità di una responsabilità solidale tra gli autori dell'illecito, deve intendersi in senso non assoluto ma relativo al danneggiato, potendo questa ricorrere pur se il fatto dannoso sia derivato da più azioni od omissioni, dolose o colpose, tra loro autonome e indipendenti, e anche nel caso in cui siano configurabili titoli di responsabilità, contrattuale ed extracontrattuale, diversi sempreché le singole azioni od omissioni abbiano concorso in maniera efficiente alla produzione del danno*.".

dannoso possa essere giuridicamente imputato. Che tra la condotta umana e l'evento si collochi un sistema dotato di capacità inferenziale o di un certo grado di autonomia operativa non trasforma il sistema stesso in un corresponsabile. La questione giuridicamente rilevante consiste, piuttosto, nello stabilire se e secondo quale criterio l'attività del sistema possa essere ricondotta alle condotte, attività od omissioni dei differenti soggetti che ne hanno governato progettazione, configurazione, controllo o utilizzazione.

L'applicazione dell'art. 2055 c.c. richiede, pertanto, particolare rigore nell'analisi del **nesso causale**. Non sarebbe corretto dedurre dalla sola **opacità del funzionamento algoritmico** che tutti gli operatori della filiera siano corresponsabili. Né la difficoltà di stabilire quale segmento abbia prodotto l'errore consente, da sola, di sostituire alla prova della responsabilità una generica imputazione solidale. Occorre distinguere l'incertezza relativa all'individuazione del concreto meccanismo tecnologico dal diverso problema della prova del contributo causale giuridicamente rilevante. La complessità tecnologica può rendere quest'ultimo accertamento più difficile, ma non fa venir meno la necessità di compierlo secondo le regole applicabili.

Da ciò deriva anche un'importante conseguenza: l'art. 2055 c.c. non stabilisce, poi, una regola probatoria sulla causalità. Esso non consente, dinanzi all'incertezza circa l'autore effettivo del danno, di imputarlo indifferentemente a tutti i soggetti potenzialmente coinvolti. Prima della solidarietà vi è l'accertamento della responsabilità. La distinzione diviene particolarmente importante nel **contenzioso algoritmico**, nel quale il rischio di utilizzare la solidarietà come strumento per compensare le difficoltà probatorie derivanti dall'opacità del sistema deve essere evitato. Le eventuali regole relative alle presunzioni, all'accesso alle prove e alla distribuzione dell'onere probatorio operano, come si vedrà *infra*, su un piano distinto rispetto all'art. 2055 c.c. Sotto il profilo esterno, l'unitarietà dell'obbligazione solidale evita che la complessità della struttura tecnologica venga trasferita integralmente sulla vittima sotto forma di necessità di determinare preventivamente la "quota eziologica" di ciascun soggetto.

Sul versante interno, invece, riemerge la necessità di differenziare le diverse responsabilità. Il **comma 2** dell'art. 2055 attribuisce infatti a chi abbia risarcito il danno il regresso nei confronti degli altri corresponsabili secondo la gravità delle rispettive colpe e l'entità delle conseguenze che ne sono derivate; il **comma 3** pone, nel dubbio, la presunzione di uguaglianza delle singole colpe. La distinzione acquista una valenza particolare proprio nelle fattispecie di danno da IA. La solidarietà consente di non trasferire sulla parte danneggiata il problema della ripartizione definitiva del rischio tra gli operatori, ma questo problema riemergerà inevitabilmente nel giudizio di regresso. Ed è verosimile che proprio questo secondo momento presenti alcuni degli interrogativi più complessi: occorrerà stabilire quale peso attribuire, nella concreta produzione del danno, alle caratteristiche originarie del sistema, alle successive modificazioni, all'eventuale omissione di interventi correttivi, alle modalità di configurazione, al livello di supervisione e alla condotta dell'utilizzatore. In termini generali, Cass., Sez. 3, n. 16835 del 29/05/2026 (Rv. 678774-01), ha stabilito che "*in tema*

di obbligazioni solidali passive, il diritto di regresso - il quale tutela l'interesse del debitore adempiente ad ottenere dagli altri condebitori il rimborso, oltre che del valore capitale della prestazione eseguita (detratta la parte eventualmente destinata a restare a carico del solvens), delle spese necessarie o utili da lui sostenute, con gli interessi pagati, nella consapevole inerzia dei coobbligati ***- quale diritto autonomo, sorto ex novo per effetto del pagamento dell'intero debito, ex art.1299 c.c., nonché, nella solidarietà ex delicto, dell'accertamento della responsabilità concorrente dei danneggianti, ex art. 2055, comma 2, c.c.****, è soggetto al termine di prescrizione ordinario decennale, con decorrenza dalla data del pagamento*" (Principio enunciato nell'interesse della legge ex art. 363, comma 3, c.p.c.). È precisamente nella dialettica tra "unità esterna" della responsabilità risarcitoria e differenziazione interna degli apporti che l'art. 2055 c.c. mostra la propria particolare attitudine a governare i danni correlati all'utilizzazione dell'intelligenza artificiale. La norma consente di evitare due soluzioni opposte, entrambe insoddisfacenti: da un lato, l'individuazione artificiosa di un unico responsabile all'interno di una sequenza causalmente complessa; dall'altro, la parcellizzazione della tutela della vittima in una molteplicità di pretese corrispondenti alle singole fasi della filiera tecnologica. La solidarietà non cancella la pluralità delle responsabilità, ma ne governa gli effetti nei confronti del danneggiato. Ne deriva una precisa scansione metodologica dell'accertamento giudiziale. Il giudice dovrebbe anzitutto individuare per ciascun soggetto il titolo della responsabilità; accertare poi il fatto imputabile a ciascuno e la sua rilevanza causale rispetto all'evento; verificare quindi se i diversi apporti abbiano prodotto un danno unitario dal punto di vista del danneggiato; soltanto all'esito di tale percorso potrebbe trovare applicazione la solidarietà di cui all'art. 2055, comma 1, c.c. La diversa consistenza degli apporti causali e dei profili di colpa tornerebbe, infine, in primo piano nei rapporti interni ai fini del regresso disciplinato dai commi 2 e 3.

In definitiva, l'art. 2055 c.c. appare suscettibile di assumere un ruolo centrale nelle controversie risarcitorie derivanti dall'utilizzo dei sistemi di intelligenza artificiale proprio perché permette di ricomporre sul piano della tutela della vittima ciò che la complessità tecnologica tende a frammentare sul piano della produzione del danno. L'art. 2055 c.c. offre, quindi, la regola attraverso la quale responsabilità autonomamente fondate e causalmente concorrenti possono convergere in un'unica obbligazione solidale. La sua funzione potrebbe pertanto rivelarsi decisiva soprattutto nei casi nei quali il danno non sia riconducibile a un singolo errore o a un solo soggetto, ma costituisca l'esito dell'interazione tra difetto tecnologico, organizzazione dell'impiego, insufficienza della supervisione e condotta dell'utilizzatore. In tali fattispecie la solidarietà diviene il punto di equilibrio tra due esigenze complementari: impedire che la complessità della **filiera dell'IA** pregiudichi l'effettività della tutela risarcitoria e, nello stesso tempo, conservare nei rapporti interni la possibilità di graduare il costo finale del danno sulla base dell'effettiva consistenza delle responsabilità concorrenti.

4.6. L'art.16, comma 2, e le presunzioni legali.

Il **comma 2** dell'**articolo 16** del d.lgs. configura una clausola di **condizionalità processuale** volta a raccordare la disciplina risarcitoria nazionale con l'apparato sanzionatorio e regolatorio dell'Unione Europea. Tale disposizione stabilisce, in particolare, che i meccanismi "agevolativi" previsti dagli artt. **18** e **19** trovino applicazione nelle azioni di risarcimento del danno - sia di natura contrattuale che extracontrattuale - **esclusivamente** qualora il pregiudizio patito derivi direttamente dalla violazione di uno o più obblighi prescritti dal Regolamento (UE) 2024/1689. La norma delimita rigorosamente l'ambito di operatività delle **presunzioni legali**, ancorandole non alla mera occorrenza di un danno nell'utilizzo di un'IA, bensì alla specifica inosservanza dei precetti comportamentali, di sicurezza o di trasparenza stabiliti dal legislatore unionale. Si tratta, quindi, di una disposizione "settoriale" che mira a risarcire il danno cagionato non dall'utilizzo di sistemi di IA bensì dal mancato rispetto di specifici obblighi e standard comportamentali e di sicurezza previsti dalla legislazione unionale.

Ciò trova conforto proprio nella Relazione Illustrativa al d.lgs. **n. 160** dove si afferma che "*il comma 2 circoscrive invece l'ambito applicativo delle disposizioni sulla presunzione del nesso di causalità di cui all'articolo 18 e sulla rilevanza della conformità al regolamento di cui all'articolo 19 alle azioni in cui il danno deriva dalla violazione di uno o più obblighi previsti dal regolamento (UE) 2024/1689. L'asimmetria tra l'ambito dell'articolo 19 e quello degli articoli 20 e 21 è coerente con la natura delle due tutele: l'accesso alle prove rileva ogniqualvolta sia in discussione il funzionamento di un sistema di IA, mentre la presunzione causale presuppone, nella sua giustificazione tecnico-giuridica, la violazione di un obbligo regolatorio puntuale*.".

Rinviando a quanto si dirà nei successivi paragrafi, va premesso che l'**articolo 18** del **d.lgs. n. 160**, richiamato dal **comma 2** dell'**art. 16**, introduce una significativa deroga all'onere probatorio ordinario in materia di nesso di causalità. La norma stabilisce una **presunzione *iuris tantum*** (relativa), operante nel caso in cui il danno sia conseguenza della violazione degli obblighi del Regolamento IA: in questa ipotesi, il collegamento eziologico tra la condotta inadempiente e l'evento lesivo è presunto, sollevando il danneggiato dalla necessità di ricostruire l'iter logico-tecnico che ha portato il sistema a produrre un output dannoso. Resta comunque ferma la facoltà per il convenuto di fornire la prova contraria, dimostrando **l'interruzione del nesso causale**[178] o l'**intervento di fattori esterni idonei a escludere la propria responsabilità**[179].

L'articolo **19** del d.lgs. n. **160** completa il quadro normativo disciplinando la rilevanza della conformità del sistema di intelligenza artificiale ai parametri europei. La disposizione sancisce espressamente che la conformità del sistema agli obblighi previsti dal **Regolamento (UE) 2024/1689,** regolamento IA, non esclude di per sé la responsabilità del convenuto.

[178] Cass.,Sez. 3, n. 21675 del 20/07/2023,(Rv. 668745-01).
[179] Cass.,Sez. 3, n. 7789 del 22/03/2024,(Rv. 670630-01).

Tale principio si applica anche laddove la conformità sia stata formalmente certificata ai sensi delle procedure di valutazione previste dal **Capo III**, **Sezione 5** del Regolamento medesimo. In tal modo, il legislatore interno chiarire che l'adempimento formale agli standard tecnici e regolamentari non costituisce un esimente automatico né una "clausola di salvaguardia" assoluta, qualora l'utilizzo concreto del sistema IA produca comunque un danno ingiusto meritevole di ristoro.

Sebbene la norma nazionale non enumeri analiticamente ogni singolo precetto unionale, essa opera un rinvio recettizio all'intero apparato di doveri e requisiti che il legislatore europeo ha imposto ai vari attori della filiera tecnologica dell'intelligenza artificiale, differenziandoli in base al livello di rischio del sistema.

In primo luogo, rilevano i divieti assoluti relativi alle pratiche di IA inaccettabili disciplinati dall'**art. 5** del regolamento IA, i quali proibiscono, tra l'altro, l'impiego di tecniche subliminali, manipolative o ingannevoli volte a distorcere materialmente il comportamento umano in modo da causare danni significativi, nonché lo sfruttamento delle vulnerabilità di persone fisiche o gruppi. **La violazione di tali divieti** costituisce un presupposto fondamentale per l'attivazione dei meccanismi probatori agevolati previsti dal legislativo. Per quanto concerne i **sistemi di IA ad alto rischio**, il **regolamento IA** impone una serie di requisiti tecnici e organizzativi stringenti che fungono da parametro per valutare la condotta del **fornitore** e del **distributore**. Tra questi obblighi rientrano l'istituzione e il mantenimento di un sistema di gestione dei rischi per l'intero ciclo di vita del prodotto (**art. 9**), l'adozione di pratiche di governance dei dati per garantire che i set di addestramento siano pertinenti e privi di distorsioni (**art. 10**) e la redazione di una documentazione tecnica dettagliata che dimostri la conformità (**art. 11**). Sono inoltre richiamati gli obblighi di registrazione automatica degli eventi (*logging*) per garantire la tracciabilità (**art. 12**) e il dovere di garantire la trasparenza algoritmica, fornendo ai *deployer* informazioni che permettano di interpretare correttamente gli output (**art. 13**).

Un rilievo centrale assumono le disposizioni sulla sorveglianza umana (**art. 14**), che impongono ai **fornitori** di progettare sistemi supervisionabili da persone fisiche e ai ***deployer*** di affidare tale compito a personale competente, dotato dell'autorità di annullare o ribaltare le decisioni algoritmiche. A completare il quadro dei sistemi ad alto rischio intervengono, poi, gli obblighi relativi ai livelli di **accuratezza**, **robustezza** e **cibersicurezza** (**art. 15**). Di particolare importanza è anche l'obbligo (**art. 20**) per i **fornitori** di **sistemi di IA ad alto rischio** che ritengono o hanno motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio non sia conforme al presente regolamento di adottare immediatamente le misure correttive necessarie per rendere conforme tale dispositivo, ritirarlo, disabilitarlo o richiamarlo, a seconda dei casi.

I fornitori sono tenuti ad informare, di conseguenza, i distributori del sistema di IA ad alto rischio interessato e, ove applicabile, i *deployer*, il rappresentante autorizzato e gli importatori.

Per i fornitori di sistemi di IA che sono stabiliti in paesi extra UE l'**art. 22** del regolamento IA prevede che, prima di mettere a disposizione i sistemi di IA ad alto rischio sul mercato dell'Unione, i fornitori stabiliti in paesi terzi nominano, mediante "*mandato scritto*", un **rappresentante** autorizzato stabilito nell'Unione. Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore consistente nello svolgimento dei seguenti atti: a) fornire una copia del mandato alle autorità di vigilanza del mercato, su richiesta, in una delle lingue ufficiali delle istituzioni dell'Unione indicata dall'autorità competente; b) far verificare che la dichiarazione di conformità UE di cui all'articolo 47 e la documentazione tecnica di cui all'articolo 11 siano state redatte e che il fornitore abbia eseguito un'appropriata procedura di valutazione della conformità; c) tenere a disposizione delle autorità competenti e delle autorità o degli organismi nazionali di cui all'articolo 74, paragrafo 10, per un periodo di 10 anni dopo la data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, i dati di contatto del fornitore che ha nominato il rappresentante autorizzato, una copia della dichiarazione di conformità UE di cui all'articolo 47, la documentazione tecnica e, se del caso, il certificato rilasciato dall'organismo notificato; d) fornire all'autorità competente, su richiesta motivata, tutte le informazioni e la documentazione necessaria per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, compreso l'accesso ai log, di cui all'articolo 12, paragrafo 1, generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore; f) cooperare con le autorità competenti, su richiesta motivata, in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio, in particolare per ridurre e attenuare i rischi posti dal sistema di IA ad alto rischio; e) ove applicabile, rispettare gli obblighi di registrazione di cui all'articolo 49, paragrafo 1, o, se la registrazione è effettuata dal fornitore stesso, garantire la correttezza delle informazioni di cui all'allegato VIII, sezione A, punto 3, del regolamento IA. L'**art. 22**[180] del regolamento IA

[180] Art.22 del regolamento (UE) 2024/1689: "1. Prima di mettere a disposizione i sistemi di IA ad alto rischio sul mercato dell'Unione, i fornitori stabiliti in paesi terzi nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.2. Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore.3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fornitore. Fornisce una copia del mandato alle autorità di vigilanza del mercato, su richiesta, in una delle lingue ufficiali delle istituzioni dell'Unione indicata dall'autorità competente. Ai fini del presente regolamento, il mandato consente al rappresentante autorizzato di eseguire i compiti seguenti: a) verificare che la dichiarazione di conformità UE di cui all'articolo 47 e la documentazione tecnica di cui all'articolo 11 siano state redatte e che il fornitore abbia eseguito un'appropriata procedura di valutazione della conformità; b) tenere a disposizione delle autorità competenti e delle autorità o degli organismi nazionali di cui all'articolo 74, paragrafo 10, per un periodo di 10 anni dopo la data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, i dati di contatto del fornitore che ha nominato il rappresentante autorizzato, una copia della dichiarazione di conformità UE di cui all'articolo 47, la documentazione tecnica e, se del caso, il certificato rilasciato dall'organismo notificato; c) fornire all'autorità competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui alla lettera b) del presente comma, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, compreso l'accesso ai log, di cui all'articolo 12, paragrafo 1, generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore; d) cooperare con le autorità competenti, su richiesta motivata, in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio, in particolare per ridurre e attenuare i rischi posti dal sistema di IA ad alto rischio; e) ove applicabile, rispettare gli obblighi di registrazione di cui all'articolo 49, paragrafo 1, o, se la registrazione è effettuata dal fornitore stesso, garantire la correttezza delle informazioni di cui all'allegato VIII, sezione A, punto 3.Il mandato consente al rappresentante autorizzato di fare da interlocutore, in aggiunta o in sostituzione del fornitore, con le autorità competenti per tutte le questioni relative al rispetto del presente regolamento.4.Il rappresentante autorizzato pone fine al mandato se ritiene o ha motivi per ritenere che il fornitore agisca in contrasto con i propri obblighi a norma del presente regolamento. In tal caso, comunica immediatamente alla pertinente autorità di

afferma altresì che "*il mandato consente al rappresentante autorizzato di fare da interlocutore, in aggiunta o in sostituzione del fornitore, con le autorità competenti per tutte le questioni relative al rispetto del presente regolamento. Il rappresentante autorizzato pone fine al mandato se ritiene o ha motivi per ritenere che il fornitore agisca in contrasto con i propri obblighi a norma del presente regolamento. In tal caso, comunica immediatamente alla pertinente autorità di vigilanza del mercato, nonché, se del caso, all'organismo notificato pertinente, la cessazione del mandato e i relativi motivi.*". I fornitori di sistemi di IA stabiliti in paesi extra Ue sono tenuto, quindi, a nominare un loro rappresentante all'interno dello spazio comunitario al fine dell'immissione in commercio del sistema di intelligenza ed è tenuto a rispettare tutte le norme del regolamento previste per i fornitori di sistemi di IA stabiliti all'interno dell'UE (obblighi di trasparenza; sistema di prevenzione e gestione dei rischi, certificazione di conformità, ecc.).

Viene poi previsto, all'**art. 25, comma 1**, del regolamento IA, che "*Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16*". Alla luce della disposizione anzidetta una azione risarcitoria del danno cagionato nell'utilizzo di un sistema di IA fornito da una società non stabilita in un paese UE, che non ha nominato un proprio rappresentante all'interno dell'Unione e non ha stabilito una propria sede in uno degli Stati dell'Unione, potrà comunque convenire in giudizio il distributore, l'importatore e qualsiasi terzo che abbia immesso in commercio l'IA ad alto rischio creata da una persona fisica o giuridica stabilita in un Paese extra Ue in quanto questi ultimi sono **equiparati** al fornitore.

Si devono altresì ritenere richiamati gli obblighi specifici in capo ai ***deployer*** (**art. 26**), i quali sono tenuti ad adottare misure tecniche e organizzative per utilizzare i sistemi conformemente alle istruzioni ricevute, a monitorarne costantemente il funzionamento sospendendone l'uso in caso di rischio e a garantire la pertinenza dei dati di *input*.

All'**art. 27**[181] viene previsto, poi, che prima di utilizzare un sistema di IA ad alto rischio di cui all'**art. 6, paragrafo 2**, del regolamento IA ((ossia le IA destinate all'istruzione, alla

vigilanza del mercato, nonché, se del caso, all'organismo notificato pertinente, la cessazione del mandato e i relativi motivi.".

[181] Art. 27 del regolamento (UE) n.2024/1689: "1.Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i *deployer* effettuano una valutazione che comprende gli elementi seguenti: a) una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo. 2.L'obbligo di cui al paragrafo 1 si applica al primo uso del sistema di IA ad alto rischio. Il *deployer* può, in casi analoghi, basarsi su valutazioni d'impatto sui diritti fondamentali effettuate in precedenza o su valutazioni d'impatto esistenti effettuate da un fornitore. Se, durante l'uso del sistema di IA ad alto rischio, ritiene che uno qualsiasi degli elementi elencati al paragrafo 1 sia cambiato o non sia più aggiornato, il *deployer* adotta le misure necessarie per aggiornare le informazioni. 3. Una volta effettuata la valutazione di cui al paragrafo 1 del presente articolo, il *deployer* notifica all'autorità di vigilanza del mercato i suoi risultati, presentando il modello compilato di

formazione, alla gestione dei rapporti di lavoro, all'accesso ai servizi pubblici ecc.), i ***deployer*** che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), del regolamento IA devono effettuare **una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre**.

Infine, si possono ritenere compresi anche gli obblighi di trasparenza per determinati sistemi di IA (**art. 50**), quali il dovere di informare le persone fisiche quando interagiscono con un'IA, l'obbligo di contrassegnare gli output generati artificialmente, come i "*deep fake*", e il dovere di segnalare l'utilizzo di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica.

Gli obblighi di trasparenza, organizzazione e prevenzione del rischio imposti ai singoli attori della filiera tecnologica dei sistemi di intelligenza artificiale (quali sistemi "in sé" o quali sistemi inseriti in prodotti destinati agli usi più eterogenei) costituiscono la misura per valutare ogni condotta, attiva od omissiva, che si discosti dagli obblighi specifici indicati dal regolamento IA. La violazione degli obblighi del regolamento imposti specificamente ai singoli "responsabili" della filiera tecnologica dei sistemi di IA costituirà una ipotesi di "**colpa specifica"** (**art. 43 c.p.**) a cui potrà "accompagnarsi" anche la violazione delle comuni misure di prudenza, diligenza e perizia (cd. "**colpa generica**").

4.7. L'art. 16, comma 3: la clausola di salvezza dei regimi speciali di responsabilità.

Nella Relazione Illustrativa si afferma che la disposizione introduce una clausola di salvezza dei regimi speciali di derivazione eurounitaria che presentano un ambito di sovrapposizione potenziale con la disciplina oggetto del decreto legislativo. Sono fatte salve, in particolare, le disposizioni dell'art. **82** del regolamento generale sulla protezione dei dati, in materia di responsabilità del titolare e del responsabile del trattamento per danno da illecito trattamento, nonché la normativa nazionale di recepimento della **direttiva (UE) 2024/2853** sulla responsabilità per danno da **prodotti difettosi**. La clausola, secondo la relazione illustrativa, dovrebbe assicurare che, negli ambiti in cui operano già regimi armonizzati di responsabilità, il presente decreto legislativo non determina effetti di interferenza o di riduzione delle tutele.

Il **comma 3** dell'**art**. **16** del d.lgs. configura, in definitiva, una clausola di salvezza funzionale a garantire la coerenza del nuovo intervento con il quadro giuridico eurounitario preesistente (cd. responsabilità multilivello). In particolare, la disposizione prevede la salvezza delle tutele apprestate da specifici regimi speciali di responsabilità, impedendo che l'introduzione delle nuove norme processuali in materia di intelligenza artificiale determini

---

cui al paragrafo 5 del presente articolo nell'ambito della notifica. Nel caso di cui all'articolo 46, paragrafo 1, i *deployer* possono essere esentati da tale obbligo di notifica. 4.Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati.5.L'ufficio per l'IA elabora un modello di questionario, anche attraverso uno strumento automatizzato, per agevolare i *deployer* nell'adempimento dei loro obblighi a norma del presente articolo in modo semplificato.".

effetti di restrizione o di deroga tacita a statuti protettivi già consolidati nell'ordinamento. Nello specifico, la norma richiama e mantiene ferme le disposizioni contenute nell'art. **82** del **Regolamento (UE) 2016/679** (**GDPR**), il quale disciplina il diritto al risarcimento e la responsabilità civile del titolare o del responsabile del trattamento per i danni cagionati da operazioni di trattamento dei dati personali non conformi al medesimo regolamento.

Contestualmente, il comma in esame fa salva l'operatività della normativa nazionale di recepimento della **Direttiva (UE) 2024/2853**, relativa alla responsabilità per danno da prodotti difettosi, assicurando così che il danneggiato possa continuare ad azionare i rimedi previsti dallo statuto speciale del produttore laddove il sistema di intelligenza artificiale integri i requisiti di difettosità previsti dalla fonte unionale.

L'**art. 82**[182] del **Regolamento (UE) 2016/679** (**GDPR**) disciplina in modo organico il diritto al risarcimento e la responsabilità civile derivante da operazioni di trattamento dei dati personali effettuate in violazione delle prescrizioni del regolamento medesimo. La disposizione stabilisce il principio cardine secondo cui chiunque subisca un danno materiale o immateriale a causa di un'infrazione del GDPR ha il diritto di ottenere il ristoro del pregiudizio patito dal titolare del trattamento o dal responsabile del trattamento. Sotto il profilo dei criteri di imputazione, il **titolare** risponde del danno cagionato dal trattamento che violi il regolamento, mentre il **responsabile** è chiamato a rispondere solo se non ha adempiuto agli obblighi specificamente diretti ai responsabili o se ha agito in modo difforme o contrario alle istruzioni del titolare. La norma configura un modello di **responsabilità aggravata**, prevedendo che il titolare o il responsabile siano esonerati esclusivamente qualora riescano a dimostrare che l'evento dannoso non è loro in alcun modo imputabile. Il "**GDPR**" prevede, poi, l'attribuzione di rimedi individuali effettivi, garantendo ai singoli e ai gruppi interessati un autonomo diritto di azione per ottenere il risarcimento, a differenza di quanto inizialmente previsto da altri quadri normativi europei in materia tecnologica. All'interno dell'ordinamento nazionale, l'operatività di tale regime speciale viene, quindi, espressamente fatta salva dall'**art. 16, comma 3**, del d.lgs. n. 160. Questa clausola di salvezza assicura che le nuove tutele processuali civili non determinino una riduzione del livello di protezione già garantito dal

[182] Art. 82 del regolamento UE n. 2016/679: 1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile. 4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2. 6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.".

GDPR, operando secondo una logica di piena complementarità tra lo statuto della protezione dei dati e la nuova disciplina sulla responsabilità algoritmica

La normativa nazionale di recepimento della **Direttiva (UE) 2024/2853**, la cui attuazione deve completarsi entro il **9 dicembre 2026**, costituisce un pilastro fondamentale del sistema di **responsabilità oggettiva del produttore** adattato alle sfide dell'economia digitale. L'operatività di tale regime speciale viene espressamente preservata dall'**art. 16**, **comma 3**, attraverso una clausola di salvezza che impedisce ogni effetto di restrizione o deroga tacita alle tutele già esistenti o in via di consolidamento. Sotto il profilo sostanziale, la nuova disciplina amplia la nozione di prodotto includendovi, come già accennato più volte, esplicitamente il **software** e **i sistemi di intelligenza artificiale**, garantendo così che il danneggiato possa invocare il regime di responsabilità senza l'onere della prova della colpa ogniqualvolta il sistema presenti un difetto di sicurezza. Il contenuto innovativo della normativa si riflette nella rimodulazione del concetto di difetto, il quale viene ora valutato alla luce del "*consumer expectation test*" integrato con i rischi specifici dell'IA, quali la capacità di auto-apprendimento post-commercializzazione e l'interazione dinamica con altri ecosistemi digitali. Un rilievo centrale assume, poi, come già accennato, la persistenza della responsabilità del fabbricante nelle ipotesi in cui mantenga un controllo effettivo sul sistema tramite aggiornamenti o servizi correlati, rendendolo responsabile anche per i difetti sopravvenuti alla messa in servizio. Sul piano processuale, la disciplina introduce strumenti di disclosure probatoria che permettono al giudice di ordinare l'esibizione di prove pertinenti in capo al convenuto, facilitando il superamento dell'**asimmetria informativa** tipica del settore tecnologico. Tale meccanismo è supportato da un articolato sistema di **presunzioni legali *iuris tantum*** che sollevano l'attore dall'onere di dimostrare la difettosità o il nesso causale in casi di elevata complessità tecnica o scientifica, purché la domanda risarcitoria sia ritenuta "ragionevole" e il danno sia coerente con il malfunzionamento allegato. Infine, la normativa estende la platea dei legittimati passivi a un'ampia categoria di operatori economici, tra cui importatori, distributori e gestori di piattaforme, stabilendo una responsabilità solidale volta a garantire l'effettività del risarcimento indipendentemente dalla localizzazione geografica del produttore originale.

In assenza della normativa nazionale di recepimento[183] potrà applicarsi la normativa attualmente in vigore per la responsabilità risarcitoria del danno da prodotti difettosi (**artt. 114 e ss del d.lgs. n. 206 del 2005**). Infatti, la **Direttiva (UE) n. 2853/2024 del 23 ottobre 2024** si applicherà esclusivamente ai danni provocati da prodotti difettosi immessi nel mercato dopo il **9/12/2026** e, pertanto, sino a tale giorno non potrà che applicarsi la normativa interna attualmente in vigore, attuativa della **Direttiva 85/374/CEE** che, pur se abrogata, continua "*tuttavia ad applicarsi in relazione ai prodotti immessi sul mercato o messi*

[183] Schema di decreto legislativo, Atto del Governo n. 434, approvato preliminarmente dal Consiglio dei ministri il 4 agosto 2026 e trasmesso alle Camere il 7 agosto. Lo schema di d.lgs. di recepimento attualmente all'esame delle commissioni parlamentari prevede la sostituzione integrale degli artt. 114-127 del Codice del consumo e introduce, fra l'altro, nuove norme sull'esibizione delle prove e sulle presunzioni relative di difettosità e causalità.

in servizio prima di tale data" (**art. 21**)[184]. Tuttavia, ciò non esclude che dalla Direttiva (UE) 2024/2853 possano trarsi criteri interpretativi rilevanti, in quanto espressivi di principi dell'ordinamento dell'Unione destinati a orientare l'azione degli Stati membri e (quantomeno) delle pubbliche amministrazioni e degli enti pubblici in genere secondo il principio del c.d. effetto "verticale".

Sul punto, la giurisprudenza della Corte di Giustizia dell'UE ha più volte affermato che le normative dell'Unione (in particolare le direttive, ma identico ragionamento, *mutatis mutandis*, deve valere quanto ai regolamenti non immediatamente efficaci), qualora non ancora applicabili, possono produrre un parziale effetto anticipatorio, imponendo alle autorità nazionali di evitare interpretazioni e prassi manifestamente incompatibili con gli obiettivi perseguiti dal legislatore europeo. In particolare, la Corte di Giustizia[185] ha chiarito che, nel periodo intercorrente tra l'adozione dell'entrata in vigore o l'applicazione di una normativa UE, gli Stati membri sono tenuti a non compromettere gravemente il risultato prescritto dalla normativa stessa. Analogamente, è stato affermato[186] che i giudici nazionali devono privilegiare, ove possibile, un'interpretazione conforme ai principi emergenti dal diritto dell'Unione, anche prima della piena efficacia delle nuove disposizioni. Tale divieto è espressione del più generale obbligo di *stand-still*, il quale impone agli Stati membri, in pendenza del termine di recepimento, di astenersi dall'adottare disposizioni che possano compromettere gravemente la realizzazione dello scopo prescritto dalla direttiva stessa[187].

Oltre alla disciplina anzidetta, ove ne ricorrano i presupposti, troveranno, inoltre, applicazione le ordinarie regole della responsabilità contrattuale ed extracontrattuale e gli ulteriori regimi speciali di responsabilità.

Si deve rilevare, sin da ora, che anche dopo il recepimento italiano della direttiva 2024/2853 si continuerà ad avere, per un certo periodo, delle controversie soggette alle disposizioni *ratione temporis* vigenti, perché il discrimine fissato dalla direttiva è collegato **all'immissione sul mercato o alla messa in servizio dei prodotti successiva al 9/12/2026**, e non alla data dell'evento dannoso o dell'introduzione della causa che avrebbe, verosimilmente, consentito una applicazione celere delle (future) disposizioni di recepimento anche a prodotti difettosi immessi nel mercato prima della data anzidetta.

4.8. L'art. 16, comma 4: il foro del consumatore.

Il **comma 4** dell'**art. 16** introduce un **foro alternativo del consumatore**, prevedendo che, quando il danneggiato è una persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta, sia altresì

[184] Art. 21 della direttiva (UE) n. 2853/2024: "La direttiva 85/374/CEE è abrogata con effetto a decorrere dal 9 dicembre 2026. La direttiva 85/374/CEE continua tuttavia ad applicarsi in relazione ai prodotti immessi sul mercato o messi in servizio prima di tale data. I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva e si leggono secondo la tavola di concordanza di cui all'allegato.
[185] Corte di Giustizia UE, 18 dicembre 1997, causa C-129/96, Inter-Environnement Wallonie, punto 45
[186] Cfr. Corte di giustizia, 4 luglio 2006, causa C-212/04, Adeneler, punto 123.
[187] Vedasi Corte di giustizia, 8 maggio 2003, causa C-14/02, ATRAL, punto 58; 10 novembre 2005, causa C-316/04, Milieufederatie, punto 42; 26 maggio 2011, cause da C-165/09 a C-167/09, StichtingNatuur en Milieu e a., punto 78; 11 settembre 2012, causa C-43/10, NomarchiakiAftodioikisi Aitoloakarnanias e a., punto 57.

competente il giudice del luogo in cui il danneggiato ha la residenza o il domicilio. Nella Relazione illustrativa si afferma che la disposizione si ispira al modello del foro del consumatore di cui all'articolo **66-*bis* del codice del consumo**, ma che se ne distingue per la natura non esclusiva, configurandosi come **foro aggiuntivo** rispetto ai criteri ordinari di competenza. La scelta è coerente con la ratio protettiva della delega, posto che l'esigenza di prossimità del giudice rispetto al danneggiato risulta particolarmente avvertita in controversie tecnicamente complesse, nelle quali l'asimmetria di posizione tra utente individuale e fornitore del sistema raggiunge il suo massimo grado.

Il **comma 4** introduce, quindi, una specifica regola di competenza territoriale derogatoria volta a rafforzare la tutela del danneggiato che rivesta la qualifica di **consumatore**. La disposizione stabilisce che, nelle azioni di risarcimento del danno — sia di natura contrattuale che extracontrattuale — derivanti dall'utilizzo di sistemi di intelligenza artificiale, qualora il soggetto leso sia una persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta, la competenza spetti **altresì** al giudice del luogo in cui il danneggiato ha la residenza o il domicilio.

Si tratta, quindi, di un criterio di competenza territoriale **alternativo** e non **esclusivo.** La previsione di un foro speciale alternativo, che si ispira, come detto, al modello delineato dall'**art. 66-*bis* del Codice del Consumo**, si distingue tuttavia per la sua natura non esclusiva, in quanto si pone come criterio di collegamento aggiuntivo rispetto ai criteri ordinari di competenza previsti dal c.p.c. La *ratio legis* dell'intervento è da ricondursi nella necessità di garantire **l'effettività della tutela giurisdizionale** assicurando la prossimità del giudice rispetto alla vittima in controversie caratterizzate da un'elevata complessità tecnica, nelle quali l'asimmetria di posizione tra l'**utente individuale** e il **fornitore** o ***deployer*** del sistema di intelligenza artificiale è particolarmente evidente. Il legislatore intende facilitare l'accesso alla giustizia per la parte danneggiata, evitando che gli oneri logistici legati alla celebrazione del giudizio in fori remoti, nonché la ricerca e la raccolta dei mezzi istruttori, possano pregiudicare il ristoro del danno patito a causa dell'opacità dei sistemi di IA.

Il foro alternativo della parte danneggiata "consumatrice" viene stabilito **esclusivamente** per le azioni risarcitorie del danno, sia contrattuale che extracontrattuale, cagionato *nell'utilizzo* di un sistema artificiale (**comma 1**) e quando la domanda risarcitoria abbia la propria *causa petendi* nella violazione degli obblighi previsti dal **regolamento (UE) 2024/1689** del Parlamento europeo e del Consiglio, del 13 giugno 2024 (**comma 2**).

Il foro del consumatore-danneggiato non si applica, invece, alle azioni risarcitorie per il danno patito dal trattamento illecito dei dati personali e per la (futura) normativa nazionale di recepimento della **direttiva (UE) 2024/2853** del Parlamento europeo e del Consiglio, del 23 ottobre 2024 (**comma 3**). La non inclusione delle azioni risarcitorie del danno patito per l'illecito trattamento dei dati personali all'interno dell'ambito applicativo del foro del consumatore-danneggiato appare risiedere nell'impossibilità di assimilare la disciplina della tutela del consumatore a quella dell'interessato al trattamento dei dati personali, due materie

che, secondo la giurisprudenza della Suprema Corte non molto recente[188], presentano una *ratio* ben diversa e per le quali l'ordinamento giuridico ha apprestato rimedi differenti. Infatti, mentre nel caso del **consumatore** si tratta di apprestare strumenti di tutela nei confronti del "**professionista**" che trovano la loro ragione d'essere nella differente forza contrattuale delle parti, nel caso invece del **trattamento dei dati personali** una delle parti ben può essere un soggetto economico professionale, come chi tratta od utilizza i dati personali, ma la ratio si rinviene esclusivamente nella particolare natura dell'attività di trattamento d'informazioni relative a soggetti identificati o identificabili, indipendentemente dalla posizione delle parti e dai loro rapporti di forza, attività che si assume come potenzialmente lesiva delle posizioni e dei diritti individuali. Di conseguenza, in caso di proposizione di domanda di risarcimento del danno subito a causa del presunto uso illegittimo dei dati personali, deve ritenersi che essa sia attratta nella competenza territoriale esclusiva del giudice individuato dall'art. **152, comma 2 del d.lgs. n. 196 del 2003** (ossia il tribunale del luogo dove risiede il titolare del trattamento), applicabile "*ratione materiae*" alla fattispecie affrontata dalla Suprema Corte nella decisione succitata. In realtà l'**art. 152**, **comma 1-*bis***[189], stabilisce, oggi, che "*Le controversie di cui al comma 1 sono disciplinate dall'articolo **10 del d.lgs. 1° settembre 2011, n. 150***". Quest'ultima disposizione prevede, al **comma 2**, che per le controversie previste dall'articolo 152 del D. lgs. n. 196 del 2003 "***Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato***". Viene quindi stabilito, anche per le controversie risarcitorie da illecito trattamento dei dati personali, un foro di "favore" per la parte danneggiata in quanto il riferimento all' "**interessato**" non può che riferirsi al titolare del dato personale illecitamente trattato. Quindi, in caso di azione risarcitoria del danno cagionato da un trattamento illecito di dati (avvenuto senza l'ausilio di sistemi di intelligenza artificiale) il **danneggiato-interessato** potrà convenire il danneggiante presso il tribunale del proprio luogo di residenza. Se il danneggiato intende agire per il risarcimento del danno da trattamento illecito dei propri dati attraverso sistemi di IA, ugualmente, potrà optare per la scelta del tribunale del luogo di residenza sulla base, stavolta, del **comma 4** dell'**art. 16**.

Il foro del **consumatore-danneggiato** non si applica alle azioni risarcitorie del danno cagionato da prodotti difettosi costituiti (anche) da intelligenze artificiali. Il comma 3 dell'art.16 fa salva l'operatività della normativa nazionale di recepimento della **Direttiva (UE) 2024/2853.** La normativa nazionale di recepimento non è stata ancora approvata (il termine di recepimento della direttiva è stato fissato al **9.12.2026**) per cui deve ritenersi che, allo stato, in assenza della normativa nazionale di recepimento, le azioni risarcitorie del danno cagionato da prodotti difettosi costituiti da intelligenze artificiali potranno essere intentate presso il tribunale territorialmente competente del luogo di residenza del danneggiato-consumatore in quanto dai lavoratori preparatori emerge che la clausola di salvezza è stata introdotta per salvaguardare le eventuali maggiori tutele che potrebbero essere introdotte

[188] Cass.,Sez. 3 n. 12980 del 31/05/2006 (Rv. 589930-01).
[189] Comma inserito dall'art. 34, comma 9, lett. b), d.lgs. 1° settembre 2011, n. 150.

dalla (futura) normativa nazionale di recepimento della direttiva anzidetta. In assenza di clausole di maggior tutela (processuale) per il danneggiato derivanti dalle normative speciali a cui fa riferimento l'art. **16**, **comma 3**, deve ritenersi che vada applicata la disciplina di maggior tutela attualmente vigente, ossia il foro del consumatore previsto dall'**art. 16, comma 4**, in quanto le azioni risarcitorie cagionate da prodotti difettosi contenenti sistemi di intelligenza artificiale rientrano in quelle indicate al **comma 1** quando sia stato il sistema di intelligenza artificiale contenuto nel prodotto a crearne il "difetto" e, quindi, il danno e le conseguenze dannose al danneggiato. Qualora, invece, il sistema di intelligenza artificiale non è causa, quale componente del prodotto, della difettosità della "cosa" si applicherà la normativa nazionale vigente in materia di **responsabilità extracontrattuale da prodotti difettosi** (vedasi gli art. **117**[190] e seguenti del **Codice del Consumo**) e gli ordinari criteri di collegamento per stabilire la competenza per territorio previsti dagli **artt. 18** e seguenti del **c.p.c.** . Invece, se il prodotto difettoso e/o pericoloso perviene ad un consumatore attraverso un negozio rientrante nell'ambito della tutela cd. consumeristica allora non potrà che applicarsi l'**art. 66-*bis*** del Codice del Consumo (**d.lgs. n. 206 del 2005**) il quale prevede che "*1. Per le controversie civili inerenti all'applicazione delle Sezioni da I a IV del presente capo la competenza territoriale inderogabile è del giudice del luogo di residenza o di domicilio del consumatore, se ubicati nel territorio dello Stato.*".

Il giudice competente funzionalmente alle cause di **risarcimento del danno** nelle ipotesi previste dall'**art. 16** appare essere esclusivamente il tribunale (in composizione monocratica o collegiale per le controversie *ex* **art. 50-*bis*** del c.p.c.) in quanto l'**art. 9** del c.p.c. prevede, al **comma 2**, alla luce delle modifiche introdotte dall'**art. 17**, **comma 1**, della l. n. **132** del **2025**, che "*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 sistema di intelligenza artificiale*** *e, in generale, per ogni causa di valore indeterminabile*". L'introduzione della competenza per materia del Tribunale per tutte le cause riguardanti "**il funzionamento di un sistema di intelligenza artificiale**" fa ritenere che siano riconducibili in tali cause anche quelle relative alle azioni di risarcimento del danno *cagionato* dal **funzionamento** scorretto od erroneo dei sistemi di intelligenza artificiale. Il riferimento generico al "*funzionamento*" (ovvero al **malfunzionamento**) e da quanto si ricava dai lavori preparatori alla legge n. 132 (dove, in particolare, emerge l'esigenza di affidare "*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*

[190] Art. 117 del d.lgs. n. 206 del 2005: 1.Un prodotto è difettoso quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze, tra cui: a) il modo in cui il prodotto è stato messo in circolazione, la sua presentazione, le sue caratteristiche palesi, le istruzioni e le avvertenze fornite; b) l'uso al quale il prodotto può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere; c) il tempo in cui il prodotto è stato messo in circolazione. 2. Un prodotto non può essere considerato difettoso per il solo fatto che un prodotto più perfezionato sia stato in qualunque tempo messo in commercio. 3. Un prodotto è difettoso se non offre la sicurezza offerta normalmente dagli altri esemplari della medesima serie.

le materie di ***esclusiva competenza del tribunale****, quelle che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale, escludendo pertanto la competenza del giudice di pace in tali materie"*[191]) appare sintomatico della volontà del legislatore di concentrare tutte le controversie aventi ad oggetto il funzionamento (e **il malfunzionamento**) dei sistemi di intelligenza artificiale al **tribunale**.

Del resto appare evidente che la modifica dell'**art. 9, comma 2**, del c.p.c. ad opera dell'**art. 17** della **l. n. 132 del 2025** si salda con l'**art. 15** della medesima legge il quale prevede che "*Nell'esercizio della delega di cui al comma 1, il Governo si attiene ai seguenti principi e criteri direttivi: a) individuare 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; b) prevedere strumenti di tutela, di carattere risarcitorio o inibitorio, e individuare un apparato sanzionatorio per il caso di violazione delle disposizioni introdotte ai sensi della lettera a); c)* ***attribuire alle sezioni specializzate in materia di impresa le controversie relative alla disciplina introdotta ai sensi delle lettere a) e b)***". Quindi, mentre per tutte le controversie relative al funzionamento dei sistemi di IA la cognizione viene attribuita al tribunale, per alcune specifiche controversie, invece, viene previsto che la loro cognizione sia attribuita alle **sezioni specializzate in materia di impresa** (in particolare, ad esempio, le controversie aventi ad oggetto la proprietà industriale degli algoritmi e dei 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, ecc.).

4.9. L'accesso alle prove: La disciplina dell'art. 17.

L'art. **17** introduce un meccanismo di **esibizione delle prove** volto a superare, almeno nelle intenzioni del legislatore, l'asimmetria informativa nei contenziosi relativi ai sistemi di IA, consentendo al giudice di ordinare l'accesso a documenti e dati tecnici pertinenti quando il danneggiato dimostri la verosimiglianza della propria domanda. La norma individua le principali categorie di documentazione rilevante (*logging*, gestione dei rischi, documentazione tecnica e sorveglianza umana), imponendo il rispetto dei principi di necessità, proporzionalità e tutela dei segreti commerciali. Sono inoltre previste conseguenze processuali e sanzioni in caso di mancata ottemperanza all'ordine di esibizione, al fine di garantire l'effettività della tutela risarcitoria.

Nella relazione illustrativa all'**art. 17** si afferma che **l'accesso alle prove** costituisce "*lo strumento centrale di superamento dell'asimmetria informativa tra danneggiato e soggetto cui è imputato il danno, modellato in larga parte sull'archetipo dell'ordine di esibizione previsto dalla disciplina antitrust di derivazione eurounitaria, nonché sulle indicazioni*[192] *provenienti dalla proposta, ancorché ritirata, di direttiva sulla responsabilità da intelligenza artificiale*".

[191] Legislatura 19ª - Dossier n. 289 1- Senato della Repubblica.
[192] L'art. 3 della proposta di direttiva prevedeva che "Gli Stati membri provvedono affinché, su richiesta di un attore potenziale che, dopo aver chiesto al fornitore, a una persona soggetta agli obblighi del fornitore a norma [dell'articolo

Il **comma 1** attribuisce al giudice il potere di ordinare, su istanza della parte che allega di avere subito il danno, all'altra parte o al terzo che ne dispone, **l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema di intelligenza artificiale**. L'ordine è subordinato alla presentazione, da parte dell'istante, di fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche con riferimento al collegamento tra il risultato prodotto dal sistema e il danno lamentato. Nella relazione illustrativa si afferma che "*lo standard probatorio prescelto è quello della verosimiglianza, coerente con la funzione strumentale dell'esibizione, che presuppone per definizione una situazione di asimmetria informativa non superabile con i mezzi ordinari di acquisizione probatoria.*". Con questa disposizione si mira, quindi, ad assicurare una "*disclosure*" probatoria ampia e funzionale alla ricostruzione dei fatti. L'attivazione di questo meccanismo istruttorio è subordinata ad un onere di allegazione specifico in capo all'istante, il quale deve presentare fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, con particolare riguardo al nesso eziologico tra il risultato prodotto dall'IA (***output***) e il danno lamentato. Lo *standard* della **verosimiglianza** prevista dalla disposizione costituisce una vera novità nel panorama processuale ed appare plausibile che questa scelta del legislatore sia motivata dalla necessità di calibrare l'accesso alle prove in un contesto di oggettiva difficoltà probatoria, evitando al contempo istanze meramente esplorative che possano pregiudicare la riservatezza o i segreti commerciali dei soggetti coinvolti. La disposizione si configura, in effetti, come un presupposto operativo essenziale, ma non esclusivo, per l'effettività delle tutele in sede civile, applicandosi in modo uniforme a tutte le azioni risarcitorie indipendentemente dal titolo della pretesa, sia essa di natura contrattuale o extracontrattuale (in virtù del richiamo dell'**art. 16**, **comma 1**, all'**art. 17**).

---

24 o dell'articolo 28, paragrafo 1, della legge sull'IA] o a un utente di divulgare gli elementi di prova pertinenti di cui dispone in relazione a un determinato sistema di IA ad alto rischio che si sospetta abbia cagionato il danno, si sia visto opporre un rifiuto, oppure su richiesta dell'attore, gli organi giurisdizionali nazionali abbiano il potere di ordinare la divulgazione di detti elementi di prova da parte di tali persone. L'attore potenziale deve presentare a sostegno di tale richiesta fatti e prove sufficienti a sostenere la plausibilità della domanda di risarcimento del danno. 2.Nel quadro di una domanda di risarcimento del danno, gli organi giurisdizionali nazionali ordinano a una delle persone elencate al paragrafo 1 di divulgare gli elementi di prova solo se l'attore ha previamente compiuto ogni sforzo proporzionato per ottenere tali elementi di prova dal convenuto. 3.Gli Stati membri provvedono affinché gli organi giurisdizionali nazionali, su richiesta dell'attore, abbiano il potere di ordinare misure specifiche di conservazione degli elementi di prova di cui al paragrafo 1. 4.Gli organi giurisdizionali nazionali limitano la divulgazione degli elementi di prova a quanto necessario e proporzionato per sostenere una domanda o potenziale domanda di risarcimento del danno e limitano la conservazione di tali elementi di prova a quanto necessario e proporzionato per sostenere tale domanda di risarcimento del danno. Nel valutare la proporzionalità di un ordine di divulgazione o di conservazione degli elementi di prova, gli organi giurisdizionali nazionali tengono conto dei legittimi interessi di tutte le parti, compresi i terzi interessati, specialmente in relazione alla protezione dei segreti commerciali ai sensi dell'articolo 2, punto 1, della direttiva (UE) 2016/943, e delle informazioni riservate, come le informazioni relative alla sicurezza pubblica o nazionale. Gli Stati membri provvedono affinché, qualora sia ordinata la divulgazione di un segreto commerciale o presunto segreto commerciale che l'organo giurisdizionale ha indicato come riservato ai sensi dell'articolo 9, paragrafo 1, della direttiva (UE) 2016/943, gli organi giurisdizionali nazionali, d'ufficio o su richiesta debitamente motivata di una parte, abbiano il potere di adottare misure specifiche necessarie per tutelarne la riservatezza se tali elementi di prova vengono utilizzati o se ad essi è fatto riferimento nel procedimento giudiziario. Gli Stati membri provvedono inoltre affinché la persona cui è stato ordinato di divulgare o conservare gli elementi di prova di cui al paragrafo 1 o 2 disponga di adeguati mezzi procedurali per impugnare tali ordinanze. 5.Se il convenuto non si conforma all'ordinanza con cui l'organo giurisdizionale nazionale, nel contesto di una domanda di risarcimento del danno, gli ingiunge di divulgare o conservare gli elementi di prova a sua disposizione a norma del paragrafo 1 o 2, l'organo giurisdizionale nazionale presume, in particolare nelle circostanze di cui all'articolo 4, paragrafo 2 o 3, la non conformità a un pertinente obbligo di diligenza da parte del convenuto, che gli elementi di prova richiesti erano intesi a dimostrare ai fini della domanda di risarcimento del danno. Il convenuto ha il diritto di confutare tale presunzione.".

Il legislatore nazionale ha inteso così valorizzare la funzione probatoria dei documenti e dei registri (*logging*) previsti dal regolamento IA, assicurando che la complessità intrinseca del *software*, le dinamiche di apprendimento automatico del sistema (*machine learning*), i sistemi di intelligenza artificiale "agentica", non impediscano al danneggiato di ricostruire la dinamica dell'evento lesivo. In definitiva, questo mezzo istruttorio mira a garantire la reale accessibilità degli elementi di prova, rendendo, secondo il legislatore, il sistema di responsabilità civile compatibile con le sfide dell'economia digitale.

Il **comma 2** dell'**art. 17** del d.lgs. identifica l'oggetto materiale dell'ordine di esibizione, delineando attraverso un'elencazione meramente **esemplificativa** (l'inciso iniziale della disposizione "*tra gli elementi di prova di cui al comma 1*" rende evidente l'intenzione del legislatore di individuare in via non tassativa i documenti a cui fa riferimento il **comma 2**) le tipologie documentali di maggiore ricorrenza e rilievo nelle controversie civili aventi ad oggetto sistemi algoritmici. Nello specifico, la disposizione opera un rinvio alle evidenze documentali prescritte dal regolamento IA, includendovi espressamente i **registri di registrazione automatica degli eventi** (***logging***) di cui all'**art. 12**, la **documentazione relativa al sistema di gestione dei rischi** prevista dall'**art. 9**, le **informazioni pertinenti racchiuse nella documentazione tecnica *ex* art. 11** e i dati riguardanti **i parametri e le modalità di sorveglianza umana** stabiliti dall'**art. 14** del medesimo regolamento unionale.

Nella Relazione Illustrativa si precisa che la scelta di ancorare l'oggetto dell'esibizione alla documentazione prevista dal regolamento sull'intelligenza artificiale (regolamento IA) mira a perseguire una duplice finalità: assicurare la concreta accessibilità di documenti già obbligatoriamente predisposti dal fornitore o dal *deployer* e valorizzare la funzione probatoria degli obblighi di compliance imposti dal regolamento medesimo.

La disposizione intende assicurare, quindi, al danneggiato la concreta accessibilità a documenti che il fornitore o il *deployer* sono già tenuti per legge a predisporre, mitigando così le difficoltà di individuazione del materiale probatorio in un contesto di elevata complessità tecnica. In via sussidiaria, l'intervento mira a valorizzare la funzione probatoria degli obblighi di compliance, trasformando i presidi regolatori di trasparenza e tracciabilità in strumenti operativi funzionali all'accertamento della responsabilità civile e alla ricostruzione del percorso decisionale del sistema. Sotto il profilo più propriamente processuale il richiamo a tali categorie documentali tipizzate agevola il giudice nella valutazione della **pertinenza degli elementi di prova di cui viene chiesta l'esibizione**, fornendo un parametro di riferimento certo rispetto agli obblighi di conservazione gravanti sugli operatori economici. In definitiva, deve ritenersi che la disposizione funge da raccordo necessario tra il piano regolatorio della sicurezza dei prodotti e il piano processuale del risarcimento del danno, garantendo che **l'opacità tecnologica** non si traduca in un'impossibilità di tutela giurisdizionale per il soggetto che si assume danneggiato dall'utilizzo di sistemi di IA.

L'**art. 9** del regolamento IA impone l'istituzione e il mantenimento di un **sistema di gestione dei rischi** configurato come un processo iterativo e continuo che deve accompagnare il **sistema di IA ad alto rischio** per l'intero ciclo di vita. Tale sistema è

finalizzato all'identificazione e all'analisi dei pericoli noti o ragionevolmente prevedibili per la salute, la sicurezza e i diritti fondamentali, includendo la valutazione delle criticità derivanti sia dall'uso conforme alla finalità prevista sia dalle condizioni di uso improprio prevedibile. Il processo impone l'adozione di misure di attenuazione mirate affinché ogni rischio residuo associato ai pericoli individuati sia considerato accettabile, tenendo conto delle conoscenze tecniche e della formazione attesa dal "*deployer*".

L'**art. 11** stabilisce l'obbligo di predisporre una documentazione tecnica dettagliata prima dell'**immissione sul mercato o della messa in servizio**, la quale deve essere tenuta costantemente aggiornata per dimostrare la conformità ai requisiti di sicurezza. Tale apparato documentale deve fornire alle autorità nazionali e agli organismi notificati informazioni chiare sulla logica degli algoritmi, sulle specifiche di progettazione, sull'architettura del software, sulle risorse computazionali utilizzate e sulle procedure di addestramento e convalida dei dati.

Ai fini della trasparenza e della tracciabilità, l'**art. 12** prescrive che i **sistemi di IA ad alto rischio** consentano tecnicamente la **registrazione automatica degli eventi** (l*ogging*) per tutta la durata del loro ciclo di vita. Tale registrazione deve permettere al *deployer* e al fornitore di individuare situazioni che possano determinare modifiche sostanziali o presentare rischi per la sicurezza (cd. **"scatola nera" dell'IA**), agevolando il monitoraggio delle prestazioni in contesti reali e documentando dati critici quali il periodo di ciascun utilizzo, le banche dati di riferimento consultate e l'identificativo delle persone fisiche coinvolte nella verifica dei risultati.

Infine, l'**art. 14** disciplina **la sorveglianza umana**, stabilendo che i sistemi siano progettati con interfacce uomo-macchina adeguate che permettano a persone fisiche competenti e formate di supervisionarne efficacemente il funzionamento. La **sorveglianza umana** ha lo scopo di prevenire o minimizzare i rischi residui per i diritti fondamentali, garantendo che l'operatore possa interpretare correttamente gli output, monitorare anomalie o disfunzioni e, laddove necessario, intervenire per arrestare il sistema o ribaltare le decisioni algoritmiche, giungendo a imporre una verifica separata da parte di almeno due persone fisiche per le applicazioni tecnologicamente più invasive.

Il **comma 3** dell'**art. 17** codifica i principi di **necessità** e **proporzionalità** dell'ordine di esibizione, imponendo al giudice di tenere conto degli interessi di tutte le parti, con particolare riguardo alla **tutela dei segreti commerciali e delle informazioni riservate**.

La disposizione delinea **i criteri direttivi** e i **limiti intrinseci** del potere istruttorio del giudice in materia di accesso probatorio, introducendo un necessario correttivo alla portata dell'ordine di esibizione. L'ordine di esibizione deve essere rigorosamente circoscritto a quanto **indispensabile** rispetto all'oggetto materiale della domanda risarcitoria allegata dall'istante. Tale previsione, come emerge dalla relazione illustrativa, configura un obbligo in capo all'autorità giudiziaria di operare un preventivo e accurato bilanciamento tra l'esigenza di effettività della tutela giurisdizionale e i contrapposti interessi dei soggetti coinvolti nel processo, siano essi parti o terzi detentori delle evidenze tecniche. Un rilievo molto importante all'interno della norma è attribuito alla **clausola di salvaguardia** relativa alla **tutela dei**

segreti commerciali e delle **informazioni riservate**, la quale impone al giudice di tenere in debita considerazione il rischio di pregiudizio che una divulgazione indiscriminata potrebbe arrecare al patrimonio informativo e tecnologico del fornitore o del *deployer*. Nella **Relazione Tecnica** si afferma che questi limiti all'esibizione documentale è funzionale a garantire che lo strumento della ***disclosure*** non travalichi la propria finalità compensativa dell'**asimmetria informativa** per trasformarsi in un mezzo di acquisizione di asset strategici aziendali o in un'indebita intrusione nei processi di sviluppo protetti dalla proprietà industriale. In definitiva, il **comma 3** assicura che **la ricerca della prova** sul funzionamento del sistema algoritmico avvenga secondo "*un modulo di massima cautela procedurale*", rendendo il meccanismo di esibizione compatibile con il mantenimento della competitività e della riservatezza operativa degli operatori economici.

Il **comma 4** dell'**art. 17** prevede l'ipotesi in cui l'esecuzione dell'ordine comporti il rischio di divulgazione di **segreti commerciali** o di altre **informazioni riservate**, prevedendo che il giudice adotti le misure idonee a garantirne la tutela. Vi è un rinvio all'**art. 121-*ter* del codice della proprietà industriale** che consente, secondo la relazione illustrativa, di mutuare integralmente lo strumentario procedurale già sperimentato in materia di tutela dei segreti commerciali, evitando duplicazioni normative.

Il **comma 4** disciplina specificamente la **gestione del rischio di divulgazione di segreti commerciali o di altre informazioni riservate** nel corso dell'esecuzione dell'ordine di esibizione probatoria. La disposizione impone al giudice l'obbligo di adottare **misure idonee** a garantire la tutela del patrimonio informativo e tecnologico del **fornitore** o del ***deployer*** laddove l'accesso agli elementi di prova possa pregiudicare interessi di proprietà industriale o commerciale.

Il legislatore ha scelto di operare un rinvio recettizio all'**art. 121-*ter***[193] **del Codice della Proprietà Industriale** (**d.lgs. n. 30/2005**), mutuando integralmente uno strumentario procedurale già sperimentato che consente, tra l'altro, l'**oscuramento di parti di documenti o la limitazione dell'accesso alle udienze**. Tale previsione è finalizzata a bilanciare l'effettività della tutela giurisdizionale del danneggiato con la necessità di preservare gli *asset* strategici aziendali e i segreti industriali e commerciali dei sistemi di intelligenza artificiale,

[193] Art.121-*ter* del Codice della Proprietà Industriale: "1. Nei procedimenti giudiziari relativi all'acquisizione, all'utilizzazione o alla rivelazione illecite dei segreti commerciali di cui all'articolo 98, il giudice può vietare ai soggetti da lui nominati o delegati, alle parti e ai loro rappresentanti e consulenti, ai difensori, al personale amministrativo, ai testimoni, e agli altri soggetti che a qualunque titolo hanno accesso ai provvedimenti, agli atti e ai documenti presenti nel fascicolo d'ufficio, l'utilizzo o la rivelazione dei segreti commerciali oggetto del procedimento che ritenga riservati. Il provvedimento di divieto di cui al primo periodo è pronunciato su istanza di parte e mantiene efficacia anche successivamente alla conclusione del procedimento nel corso del quale è stato emesso. 2. Il provvedimento di cui al comma 1 perde la sua efficacia: a) se con sentenza, passata in giudicato, è accertato che i segreti commerciali oggetto di causa erano privi dei requisiti di cui all'articolo 98; b) se i segreti commerciali diventano generalmente noti o facilmente accessibili agli esperti e agli operatori del settore. 3. Nei procedimenti giudiziari di cui al comma 1 il giudice, su istanza di parte, può adottare i provvedimenti che, nel rispetto dei principi regolatori del giusto processo, appaiano più idonei a tutelare la riservatezza dei segreti commerciali oggetto di causa, ed in particolare: a) limitare ad un numero ristretto di soggetti l'accesso alle udienze e agli atti e ai documenti presenti nel fascicolo d'ufficio; b) disporre, nei provvedimenti che definiscono i procedimenti di cui al comma 1, resi disponibili anche a soggetti diversi dalle parti, l'oscuramento o l'omissione delle parti contenenti i segreti commerciali. 4. Ai fini di cui al comma 3, lettera b), il giudice, con il provvedimento, indica le parti dello stesso che il cancelliere è tenuto ad oscurare o omettere all'atto del rilascio di copia a soggetti diversi dalle parti. Agli stessi fini il giudice ordina che, all'atto del deposito del provvedimento, la cancelleria vi apponga un'annotazione dalla quale risulti il divieto per le parti di diffondere il provvedimento in versione integrale.

evitando che l'**ordine di esibizione** si trasformi in uno strumento di acquisizione indebita di segreti industriali.

Il terzo potrà fare opposizione all'ordinanza di esibizione sia intervenendo nel giudizio prima della scadenza del termine assegnatogli oppure essere citato dal giudice prima di ordinare l'esibizione e, in udienza, esporre le proprie eventuali ragioni di opposizione tra cui quella di tutelare i propri segreti commerciali ed industriali (**art. 211 c.p.c.**). In questa sede il terzo (che nel giudizio assume, comunque, la qualifica di parte[194]) potrà anche proporre misure e cautele necessarie a contemperare l'interesse della giustizia con quello dei propri diritti da tutelare.

Il **comma 5** dell'**art. 17** disciplina le conseguenze dell'**inadempimento, senza giustificato motivo, dell'ordine di esibizione**: il giudice può desumere **argomenti di prova** ai sensi dell'**art. 116 c.p.c.**, mentre, quando l'inadempimento riguarda la documentazione di cui al **comma 2**, opera una più incisiva sanzione probatoria, consistente nel ritenere come **ammessi i fatti allegati dall'istante, previa valutazione di ogni altro elemento di prova**. La graduazione delle conseguenze, si afferma nella Relazione Illustrativa, è funzionale a incentivare la conservazione e l'esibizione spontanea della documentazione regolatoria.

Il **comma 5,** quindi, regola le **conseguenze processuali** della "mancata risposta" della parte destinataria dell'ordine di esibizione. In caso di inadempimento ingiustificato, la norma attribuisce al giudice il potere di desumere argomenti di prova *ex* **art. 116, comma 2, c.p.c.** Qualora l'inadempimento riguardi specificamente la documentazione tipizzata dal **comma 2** (come **i registri di *logging*** o il **sistema di gestione dei rischi**), il legislatore introduce una sanzione processuale ancora più rilevante, stabilendo che il giudice possa ritenere come **ammessi i fatti allegati dall'istante, previa valutazione di ogni altro elemento di prova disponibile**.

Il legislatore ha, quindi, previsto due sanzioni processuali di diversa gravità in caso di inottemperanza, senza giustificato motivo, della parte all'ordine di esibizione del giudice.

Si ha inottemperanza all'ordine di esibizione in caso di **inerzia**, di **adempimento soltanto parziale dell'ordine** o quando sia prodotta **documentazione totalmente diversa da quella richiesta nell'ordine del giudice** (cd. *aliud pro alio* documentale). Diversamente che dall'**art**. **210**, **comma 4**, **c.p.c.** la sanzione processuale prevista nei confronti della parte destinataria dell'ordine non viene accompagnata da alcuna pena pecuniaria che, invece, come verrà argomentato *infra*, viene invece prevista in caso di inottemperanza del terzo. Il **comma 5** attribuisce, invece, un valore probatorio autonomo all'inottemperanza dell'ordine di esibizione ad opera della parte tenuta ad esibire i documenti indicati in via esemplificativa al **comma 2**, stabilendo la sostanziale equivalenza fra tale inottemperanza e il rifiuto di rispondere all'interrogatorio formale, che consente al giudice - ai sensi dell'**art. 232, comma 1**, di «**ritenere come ammessi i fatti dedotti**». La scelta

[194] Cass. civ., Sez. I, 14/10/1977, n. 4231, in *Foro It*., 1979, I, 1870

del legislatore di limitare le (gravose) conseguenze processuali previste in caso di rifiuto senza giustificato motivo o di assenza a rendere l'interrogatorio formale ai soli documenti indicati al **comma 2** deve ritenersi giustificata dalla importanza di tali atti ai fini del monitoraggio e della prevenzione dei rischi dei sistemi di IA ad alto rischio.

Quanto agli argomenti di prova che il giudice può trarre dall'inottemperanza della parte destinataria dell'ordine di esibizione occorre rilevare che la Cassazione, di recente[195], ha affermato che "*In tema di poteri istruttori del giudice, pur essendo discrezionale il potere di desumere argomenti di prova dall'inosservanza dell'ordine ex art. 210 c.p.c., tuttavia tale discrezionalità deve essere correlata alla natura dell'argomento,* ***il che implica che il rifiuto di esibizione di documenti può essere anche valutato come ammissione del fatto costitutivo affermato dalla controparte, ma è necessario che vi siano elementi di prova concorrente****. (Nella specie, in un giudizio azionato per il riconoscimento di provvigioni, la S.C ha cassato la sentenza che, pur reputando implausibile la giustificazione addotta per la mancata produzione delle documentazione contabile, ha affermato che tale carenza si ripercuoteva in danno dello stesso appellante che non si era curato di predisporre e conservare la documentazione dalla quale poter desumere la sussistenza di tutte le somme pretese - così da poter consentire la corretta ricostruzione del rapporto - limitando le conseguenze della mancata ottemperanza all'ordine alla sola regolamentazione delle spese di lite)*.". Nello stesso senso della decisione anzidetta anche la decisione della Cass. Sez. L, n. 17076 del 27/08/2004 (Rv. 577092-01), la quale ha stabilito che "*Ai sensi dell'art. 421 cod. proc. civ., il potere officioso di ordinare l'esibizione di documenti è discrezionale, sicché il suo esercizio non comporta alcun vincolo per il giudice. Del pari discrezionale è, quindi, anche il potere di desumere argomenti di prova dall'inosservanza dell'ordine di esibizione, ma in questo caso la discrezionalità è correlata alla natura dell'argomento di prova.* ***Tale correlazione comporta che per l'eventuale valutabilità del rifiuto di esibizione di documenti come ammissione del fatto è necessario che vi siano elementi di prova concorrente****. (Nella specie, la S.C. ha confermato la sentenza impugnata, rigettando il motivo di ricorso con il quale la sentenza di merito era stata censurata per non avere tratto elementi di prova dalla mancata ottemperanza del datore di lavoro all'ordine di esibizione dei cartellini di presenza ai fini della prova dell'espletato lavoro straordinario).*".

Alla luce della giurisprudenza della Suprema Corte, quindi, il giudice può ritenere che dall'inosservanza dell'ordine di esibizione documentale (anche se non rientrante tra quelli indicati al **comma 2** dell'**art. 17**) si possa ritenere come ammesso il fatto allegato dalla controparte istante purché vi siano (ulteriori) elementi di prova concorrente.

Questa disposizione, in definitiva, come evidenziato dalla **Relazione Tecnica**, mira a dare effettività all'obbligo di trasparenza, trasformando il rifiuto di collaborazione tecnica in un fattore determinante per l'accertamento della responsabilità civile.

[195] Cass.,Sez. 2, n. 19763 del 17/07/2025, Rv. 675754–01.

Il **comma 6** prevede una sanzione pecuniaria a carico del terzo inadempiente, nella misura da **euro 1.500** a **euro 10.000**, in considerazione dell'impossibilità di applicare al terzo le sanzioni probatorie previste per la parte. La sanzione pecuniaria prevista a carico del terzo inottemperante è molto più elevata rispetto a quella prevista al **comma 5** dell'**art. 210** c.p.c. dove la pecuniaria prevista è da **euro 250** ad **euro 1.500**. La forbice edittale più elevata prevista dal **comma 6** rispetto a quella "generale" prevista dal c.p.c. appare essere giustificata dalla necessità di garantire la necessaria ed imprescindibile collaborazione tra il terzo e le parti del processo in cause risarcitorie che involgono diritti patrimoniali e non patrimoniali delle persone e sistemi di intelligenza artificiale di non semplice "comprensione" tecnica. Deve ritenersi che la pena pecuniaria prevista potrebbe non avere quell'effetto deterrente auspicato dal legislatore se si tiene conto del fatto che molto spesso le società destinatarie dell'ordine di esibizione, se terze rispetto alle parti del processo, potrebbero, per le loro condizioni economiche, preferire l'inottemperanza all'ordine, e pagare la pena pecuniaria, piuttosto che esibire una documentazione che potrebbe mettere a repentaglio determinati segreti industriali o asset commerciali.

L'intenzione del legislatore è, in definitiva, quella di dotare il giudice di uno strumento sanzionatorio efficace per superare l'asimmetria informativa e l'opacità tecnologica, assicurando che i detentori delle **evidenze tecniche** non possano frustrare le pretese risarcitorie del danneggiato attraverso condotte meramente omissive.

Le misure di coercizione previste dall'**art. 17** che ricalcano, seppur con le differenze surriferite, quanto già previsto dall'**art. 210 c.p.c.** non risolvono la questione problematica dell'esecuzione coattiva dell'ordine non ottemperato.

Il provvedimento di esibizione, in quanto avente pacificamente la forma di una ordinanza istruttoria, non appare essere suscettibile di esecuzione forzata nelle forme previste dagli artt. **605** ss. ovvero dagli **artt. 612** ss. **c.p.c.**., mancando una norma che gli attribuisca qualità di titolo esecutivo ai sensi del tassativo disposto dell'**art. 474 c.p.c.**. La giurisprudenza della Suprema Corte[196] ha, del resto, sempre affermato che "*L'ordine di esibizione di documenti* ***non è suscettibile di esecuzione coattiva, né per iniziativa del giudice, non esistendo nel codice di procedura disposizioni analoghe a quelle del codice di procedura penale circa il potere di ricercare documenti o cose pertinenti al reato, né ad iniziativa della parte interessata, non costituendo quell'ordinanza titolo esecutivo e non potendo essere, quindi, attuata con gli strumenti di cui all'arte. 605 e segg. cod. proc. civ..*** *Il rifiuto dell'esibizione può, pertanto, costituire esclusivamente un comportamento dal quale il giudice può desumere argomenti di prova ex art. 116 secondo comma cod. proc. civ., ma, a tal fine, ove sia stato giustificato dalla parte destinataria del relativo ordine con la deduzione di circostanze impeditive, la controparte interessata ha l'onere di provare la perdurante possibilità di produzione in giudizio della documentazione richiesta. (Nella specie, l'ordine era comunque diretto nei confronti di un terzo e la S.C. - nel confermare la sentenza di merito -*

[196] Cass.,Sez. 3, n. 18833 del 10/12/2003 (Rv. 568753-01).

precisa che nessun elemento di prova poteva comunque essere tratto contro gli attori).". Il medesimo principio di diritto è stato seguito di recente anche dalla giurisprudenza amministrativa. Il T.A.R. Campania Napoli, Sez. II, con sentenza del 7/05/2026, n. 2912, ha stabilito che "*l'ordine di esibizione di documenti non è suscettibile di esecuzione coattiva, né per iniziativa del giudice,* ***non esistendo nel codice di procedura civile disposizioni analoghe a quelle del codice di procedura penale circa il potere di ricercare documenti o cose pertinenti al reato, né ad iniziativa della parte interessata, non costituendo quell'ordinanza titolo esecutivo e non potendo essere, quindi, attuata con gli strumenti di cui agli artt. 605 e ss. c.p.c. nel giudizio civile o con l'ottemperanza nel giudizio amministrativo****. Peraltro, la riforma Cartabia ha riformulato il terzo comma dell'articolo 210 c.p.c. al fine di dare maggiore effettività a tale ordine ed ha previsto una sanzione pecuniaria per indurre indirettamente il suo maggiore rispetto*.".

Né una forma indiretta di esecuzione forzata dell'ordine di esibizione appare potersi realizzare attraverso il ricorso al sequestro giudiziario dei documenti da esibire ai sensi dell'**art. 670, comma 2, c.p.c.**. Il principale ostacolo all'utilizzazione del sequestro giudiziario in funzione coercitiva dell'ordine di esibizione viene infatti indicato nella natura cautelare del sequestro, in quanto strumento diretto ad assicurare in via preventiva la custodia del documento in caso di controversia sul diritto all'esibizione e non ad ottenere la conoscenza del suo contenuto. Deve ritenersi, poi, che, dopo la pronuncia dell'ordine di esibizione, non vi sarebbe più controversia in ordine al diritto all'esibizione e quindi verrebbe a mancare una delle condizioni di ammissibilità del sequestro stesso.

Si ritiene, poi, che le sanzioni processuali derivanti dall'inadempimento all'ordine di esibizione siano applicabili anche quando la parte destinataria dell'ordine giustifica il rifiuto con la deduzione di circostanze impeditive e la controparte provi la perdurante possibilità di produzione in giudizio della documentazione richiesta[197]; la parte, nei cui confronti è rivolta l'istanza di esibizione, è tenuta, altresì, a conservare la documentazione oggetto di richiesta sino a che il giudice non abbia definitivamente e negativamente provveduto sull'istanza e quindi dalla eventuale **distruzione**[198] della documentazione il giudice potrà trarre argomenti di prova solo se tale distruzione sia avvenuta successivamente alla presentazione dell'istanza e durante il tempo di attesa della decisione su di essa. La distruzione deve essere poi deliberatamente voluta dalla parte destinataria dell'ordine di esibizione. Nel caso in cui il termine per il deposito sia spirato e la parte destinataria provvede alla produzione oltre il

[197] Cass. civ., Sez. L, 7/06/2002, n. 8310.

[198] Cass. civ., Sez. L, sentenza, 22/12/2014, n. 27231 (Rv. 634223): "Nel caso in cui, nel corso di un giudizio civile, venga formulata istanza di esibizione documentale ex art. 210 cod. proc. civ., la parte nei cui confronti tale istanza è formulata è tenuta – in ossequio al dovere di lealtà e probità processuale *ex* art. 88 cod. proc. civ. e alla stregua del principio di acquisizione della prova, in forza del quale, un elemento probatorio, una volta introdotto nel processo, è definitivamente acquisito alla causa - a conservare la relativa documentazione fino a quando il giudice non abbia definitivamente e negativamente provveduto sulla stessa, sicché, ove la documentazione venga distrutta dopo la presentazione dell'istanza e durante il tempo di attesa per la formazione della decisione definitiva sulla stessa, la mancata conservazione è suscettibile di essere valutata come argomento di prova ex art. 116 cod. proc. civ. (Nella specie, relativa alla domanda di attribuzione della indennità di diaria per i turni di servizio, l'avvenuta distruzione di una parte dei tabulati dei detti turni era stata apprezzata dalla corte territoriale per l'accoglimento della domanda, tenuto conto del principio di prova costituito dalla documentazione ancora reperibile).

termine previsto la giurisprudenza ritiene che la produzione sia sicuramente utilizzabile purché il ritardo non sia apprezzabile e non determini una dilatazione dei tempi di definizione del processo[199].

Il legislatore, nella disciplina sull'**accesso alle prove**, ha seguito le indicazioni della direttiva sulla responsabilità da intelligenza artificiale ("**AILD**"), successivamente ritirata. L'**art. 3** di questa proposta di direttiva prevedeva che un organo giurisdizionale dovesse ordinare la divulgazione di elementi di prova rilevanti in relazione a **specifici sistemi di IA ad alto rischio** che si sospetta abbiano cagionato danni. Le richieste di elementi di prova dovevano essere rivolte al **fornitore** di un sistema di IA, **a una persona soggetta agli obblighi del fornitore** (di cui all'articolo 24 o all'articolo 28, paragrafo 1, della legge sull'IA, n.d.r. il successivo regolamento IA) o a **un utente**. Le richieste, si affermava nella proposta di direttiva, dovevano essere suffragate da fatti e prove sufficienti a dimostrare **la plausibilità della domanda di risarcimento del danno** in questione e gli elementi di prova richiesti dovevano essere a disposizione dei destinatari. Gli organi giurisdizionali nazionali potevano ordinare tale divulgazione solo nella misura necessaria a sostenere una domanda di risarcimento, in quanto - precisava la Commissione - le informazioni potevano costituire elementi di prova fondamentali ai fini della domanda di risarcimento in caso di danni che coinvolgevano sistemi di IA.

La disciplina introdotta dal legislatore all'**art. 17** prevede, in particolare, che l'ordine di esibizione può essere accolto quando l'istante "*presenta fatti ed elementi idonei a rendere verosimile la fondatezza della domanda*". Nella proposta di direttiva veniva previsto che l'ordine di esibizione doveva essere suffragato da prove ed elementi concreti tali da rendere "*plausibile*" la domanda di risarcimento del danno. È evidente che il legislatore interno si sia "ispirato", sul punto, alla proposta di direttiva prevedendo, rispetto alla disciplina dell'ordine di esibizione *ex* **art. 210 c.p.c.**, un "*quid pluris*" per la richiesta dell'ordine di esibizione ossia la valutazione del giudice della "*verosimile*" fondatezza della domanda. Il giudice, quindi, dovrà effettuare una delicata delibazione sulla "*verosimile*" fondatezza della domanda in una fase, quella di ammissione dei mezzi istruttori, dove il giudice non potrebbe/dovrebbe anticipare alcun convincimento sulla fondatezza/infondatezza della domanda. La giurisprudenza di legittimità[200] ritiene che l'ordine di esibizione di documenti previsto dall'**art. 210 c.p.c.**, quale provvedimento tipicamente discrezionale del giudice di merito, deve riguardare documenti che siano specificamente indicati dalla parte che ne abbia fatto istanza e che risultino **indispensabili** al fine della prova dei fatti controversi; non può quindi in alcun caso supplire al mancato assolvimento dell'onere della prova a carico della parte istante. La Corte di cassazione, Sez. I, con la decisione n.2241 del 3.02.2026 ha ribadito, di recente, che l'ordine di esibizione di cui all'**art. 210 c.p.c.** costituisce strumento istruttorio residuale, utilizzabile solo in caso di **impossibilità** di acquisire la prova dei fatti con altri mezzi e non può supplire al mancato assolvimento dell'onere probatorio dell'istante.

[199] Cass. civ., Sez. II, sentenza, 11/07/2025, n. 19108.
[200] Cass.,Sez. L, n. 10043 del 25/05/2004,(Rv. 573128-01).

In definitiva il legislatore delegato ha attribuito al giudice un potere di delibazione sulla non pretestuosità della domanda risarcitoria e, quindi, sulla indispensabilità dei documenti per l'accertamento istruttorio delle pretese del ricorrente. Del resto al **comma 1** dell'**art. 17** si afferma che l'istante "*presenta fatti ed elementi idonei* ***a rendere*** *verosimile la fondatezza della domanda,* ***anche con riferimento al collegamento tra il risultato prodotto dal sistema di intelligenza artificiale e il danno lamentato****.*". Dall'interpretazione letterale della disposizione emerge che, in realtà, il giudice deve verificare soltanto che l'istanza non sia meramente **esplorativa** e sia finalizzata a dare "riscontro" ai fatti allegati nel libello introduttivo, le cui circostanze di fatto devono essere specifiche e idonee a rappresentare, con verosimiglianza, il danno, il nesso causale e il rapporto tra l'*output* e il danno allegato.

L'**art. 17** nulla dice in ordine ai termini per il deposito dell'istanza di esibizione documentale. L'istanza dovrà rispettare quelli previsti per le deduzioni istruttorie: ne consegue che, ove la richiesta *ex* **art. 210** sia stata presentata solo in appello, la parte è tenuta a provare di non aver potuto produrre nel giudizio di primo grado, per causa ad essa non imputabile, i documenti oggetto della richiesta di esibizione, non essendo ammissibile, attraverso l'ordine *ex* **art. 210**, superare le preclusioni processuali, previste dagli **artt. 345** e **437**, né aggirare l'onere incombente sulla parte di fornire le prove che essa sia in grado di procurarsi[201]. Il legislatore, invece, non ha previso la possibilità per il giudice di acquisire **d'ufficio** la documentazione inerenti i sistemi di IA anche in assenza di istanza di parte. Questa ipotesi non era esclusa dalla proposta di direttiva "**AILD**" ed è prevista, in via eccezionale, dall'art. **2711, comma 2, c.c.** secondo il quale il giudice può ordinare, anche d'ufficio, che si esibiscano i libri per estrarne le registrazioni concernenti la controversia in corso e può ordinare altresì l'esibizione di singole scritture contabili, lettere, telegrammi o fatture concernenti la controversia. Inoltre, considerata l'asimmetria informativa tra i **fornitori** e i **produttori** dei sistemi di IA poteva essere auspicabile un potere del giudice, assimilabile a quello disciplinato dall' **art. 421, comma 2, c.p.c.**[202], di disporre l'esibizione di cose e documenti, a prescindere dall'iniziativa di parte.

4.10. La ripartizione dell'onere probatorio nelle azioni risarcitorie del danno cagionato da sistemi di intelligenza artificiale.

L'**art. 18** rappresenta il fulcro dell'intervento sulla ripartizione dell'**onere probatorio**. La disposizione introduce una **presunzione *iuris tantum*** del **nesso di causalità** tra la violazione di un obbligo previsto dal regolamento (UE) 2024/1689 e il danno. La disposizione, secondo la **Relazione Illustrativa**, prevede che il nesso di causalità tra la violazione e il danno è **presunto**, salvo prova contraria. L'inversione dell'onere della prova sul nesso causale non si estende, invece, alla colpa né alla violazione dell'obbligo, che restano oggetto di prova a carico dell'attore.

[201] Cass. civ., Sez. III, ordinanza, 22/09/2025, n. 25856.
[202] Sui poteri officiosi del giudice del lavoro in tema di esibizione dei documenti vedasi Cass. civ., Sez. L, ordinanza, 10/12/2019, n. 32265 (Rv. 656050-01).

L’**art. 18** disciplina la presunzione del nesso di causalità, ponendosi come il pilastro fondamentale dell’intervento sulla ripartizione dell’onere probatorio nelle azioni di risarcimento. È in particolare introdotta una presunzione iuris tantum, per la quale il collegamento eziologico tra la violazione di un obbligo previsto dal Regolamento (UE) 2024/1689 (regolamento IA) e il danno si considera sussistente, fatta salva la facoltà per il convenuto di fornire la prova contraria.

Come evidenziato dalla Relazione illustrativa, l’operatività di tale presunzione è circoscritta ai casi in cui il danno derivi dall’inosservanza di uno o più obblighi regolatori puntuali, configurando un regime più restrittivo rispetto a quello previsto per l’accesso probatorio di cui all’**art. 19**. L’alleviamento dell’onere probatorio a favore del danneggiato riguarda **esclusivamente** il nesso causale: non si verifica, pertanto, alcuna inversione automatica per quanto concerne la colpa o l’effettiva violazione dell’obbligo, elementi che restano integralmente oggetto di prova a carico dell’attore. La *ratio* della norma è quella di facilitare il ristoro del pregiudizio subito a fronte della complessità tecnica dei sistemi algoritmici, evitando che l’opacità del software renda impossibile la ricostruzione del percorso causale. La ratio legis dell’intervento risiede nella necessità di superare l’**opacità tecnologica** (effetto "**scatola nera**") e la marcata **asimmetria informativa** che caratterizzano i sistemi algoritmici, rendendo altrimenti "diabolica" la prova della dinamica interna al software per il soggetto leso. La giurisprudenza di merito e di legittimità ha evidenziato come la complessità dei sistemi di auto-apprendimento (*machine learning*) possa rendere quasi impossibile ricostruire i passaggi intermedi tra l’input e l’output dannoso. In particolare, il tema della causalità e della responsabilità professionale è già emerso in casi di "uso improvvido" o “sconsiderato” dell’IA generativa, dove l’impiego acritico di algoritmi ha prodotto "**allucinazioni**" (come citazioni giurisprudenziali inesistenti), portando i giudici a ravvisare, come già accennato, una responsabilità aggravata *ex* art. 96 c.p.c. per colpa grave o malafede (Trib. Torino, n. 2120/2025; Trib. Latina, 23 settembre 2025; Trib. Siracusa, 20 febbraio 2026). Anche la Corte di cassazione ha recentemente sottolineato il rischio che il ricorso a strumenti di IA possa indurre il decisore ad abdicare al proprio momento valutativo, compromettendo la terzietà del giudizio (Cass. pen., n. 34481/2025).

L'adozione di una presunzione causale risponde, quindi, a una precisa esigenza di **effettività della tutela**. Come noto, nei sistemi di IA ad alto rischio l'eziologia del danno è spesso complessa: l'output lesivo può essere il frutto di interazioni tra il modello di addestramento, i dati di input, le scelte di configurazione dell’utilizzatore e i comportamenti dell'utente. In questo contesto, imporre al danneggiato la prova piena del nesso causale equivarrebbe, nella maggior parte dei casi, a vanificare il diritto al risarcimento. La presunzione dell'art. 18 costituisce, quindi, un ragionevole punto di equilibrio, a condizione che la violazione degli obblighi del Regolamento IA sia previamente accertata – anche in via

incidentale dal giudice civile – e che il giudice eserciti un controllo sulla correlazione tra la specifica violazione e il tipo di danno lamentato, evitando automatismi applicativi[203].

4.11. La rilevanza della conformità dei sistemi di intelligenza artificiale rispetto alle prescrizioni del Regolamento (UE) 2024/1689 (AI Act) nell'ambito dei giudizi di responsabilità civile.

L'articolo **19** chiarisce che, fermo quanto previsto dalla normativa nazionale di recepimento della **direttiva (UE) 2024/2853**, la conformità del sistema di intelligenza artificiale agli obblighi previsti dal **regolamento (UE) 2024/1689**, anche se attestata da certificazione rilasciata ai sensi del **capo III, Sezione 5**, del medesimo regolamento, non esclude di per sé la responsabilità del convenuto. La disposizione mira a prevenire che il sistema di valutazione della conformità predisposto dal regolamento si traduca in un meccanismo di **immunità sostanziale dalla responsabilità civile**, distinguendo nettamente il piano regolatorio della **compliance** da quello **aquiliano o contrattuale del risarcimento del danno**. Resta naturalmente fermo il valore probatorio della conformità ai fini della valutazione complessiva del comportamento del convenuto.

Viene poi ribadito che la regola prevista dall'**art. 19** non interferisce con quanto previsto dalla normativa nazionale di recepimento della direttiva sui danni da prodotti difettosi (UE) 2024/2853. In particolare, resterà fermo, secondo quanto contenuto nella Relazione Illustrativa, il disposto dell'**art. 118** del codice del consumo, che, fra l'altro, esonera da responsabilità l'operatore economico nel caso in cui la difettosità del prodotto dipenda dalla sua conformità a requisiti giuridici, e che pone ulteriori regole di esonero da responsabilità che resteranno applicabili laddove operi il codice del consumo e in specie le norme in materia di prodotto difettoso. Ciò a conferma del fatto che gli ambiti applicativi delle due diverse discipline sono distinti, complementari e non confliggenti. Questo intervento, si afferma ancora nella Relazione Illustrativa, è anche conforme all'osservazione delle Commissioni parlamentari, in forza della quale si è sollecitata l'individuazione di parametri di riferimento che costituiscano una guida per gli operatori economici.

La disposizione stabilisce, quindi, il principio fondamentale secondo cui l'osservanza degli obblighi previsti dalla normativa unionale e l'eventuale possesso di una **certificazione di conformità** rilasciata ai sensi del medesimo regolamento (vedasi in particolare gli **artt. 44, 47 e 48**) non costituiscono, di per sé, una causa di esclusione della responsabilità del fornitore o del *deployer*. La norma opera una netta distinzione tra il piano della *compliance* regolatoria preventiva e il piano del risarcimento del danno, garantendo che i presidi di sicurezza amministrativa non si trasformino, come affermato nella Relazione Illustrativa, in un meccanismo di immunità sostanziale in sede giudiziaria.

[203]F. ROSADA, *Il d.lgs. n. 160/2026 e la responsabilità civile da intelligenza artificiale: prime riflessioni sul decreto attuativo del Regolamento (UE) 2024/1689*, in Diritto e Giustizia-News, Giuffrè.

La *ratio* dell'intervento risiede nella necessità di puntualizzare che la valutazione della conformità effettuata dagli organismi notificati o dagli operatori non pregiudica l'accertamento della **colpa** o del **nesso causale** in sede aquiliana o contrattuale. La norma assicura che il giudice possa operare un sindacato pieno sulla condotta del convenuto, fermo restando che l'avvenuto adempimento degli standard di sicurezza europei mantiene un intrinseco valore probatorio ai fini della valutazione complessiva del comportamento diligente tenuto dall'operatore economico. Sotto il profilo dell'ambito di applicazione, l'efficacia di tale disposizione è coordinata con il **comma 2** dell'**art. 16**, il quale circoscrive l'operatività di tale criterio alle sole azioni in cui il danno sia derivato dalla violazione di obblighi puntuali previsti dal regolamento dell'IA.

4.12. L'azione diretta nei confronti dell'impresa di assicurazione (art. 20).

L'**art. 20** introduce nell'ordinamento una **azione diretta** del danneggiato nei confronti dell'impresa di assicurazione che presta la copertura della responsabilità civile per i danni cagionati nell'utilizzo di sistemi di intelligenza artificiale, sul modello già sperimentato per la responsabilità civile da circolazione di veicoli a motore (**art. 144** del codice delle assicurazioni private).

Il **comma 1** prevede la facoltà per il danneggiato di richiedere, prima dell'instaurazione del giudizio, alla parte che intende citare, l'esistenza di un contratto di assicurazione. Tale richiesta, come esplicitato espressamente nella disposizione, non è **una condizione di procedibilità**; né interferisce con i procedimenti di **mediazione**, **obbligatoria o facoltativa**, che restano assoggettati alle discipline eventualmente previste con riferimento allo specifico criterio di imputazione della responsabilità di volta in volta azionato. Il soggetto cui è imputato il danno, ricevuta la richiesta di risarcimento, comunica al richiedente, entro **trenta giorni**, l'esistenza di un contratto di assicurazione della responsabilità civile relativo al danno dedotto, gli estremi del contratto e la denominazione dell'impresa di assicurazione. L'**omessa o incompleta comunicazione** è sanzionata sul piano probatorio, mediante la previsione che il giudice possa desumere argomenti di prova ai sensi dell'art. **116 del c.p.c.**. Il **comma 2** attribuisce al danneggiato l'azione diretta nei confronti dell'impresa di assicurazione, nei limiti delle somme per le quali è stipulato il contratto di assicurazione. I **commi 3**, **4** e **5** disciplinano i profili tipici dell'azione diretta: l'opponibilità al danneggiato delle eccezioni derivanti dal contratto di assicurazione, purché anteriori al sinistro; il diritto di rivalsa dell'impresa di assicurazione verso l'assicurato, nella misura in cui essa avrebbe avuto titolo contrattuale per rifiutare o ridurre la propria prestazione; il litisconsorzio necessario, nel giudizio promosso dal danneggiato, del soggetto individuato quale responsabile del danno. Quest'ultima previsione assicura l'unitarietà dell'accertamento sul fatto generatore del danno e previene il rischio di giudicati contraddittori tra l'azione diretta e l'eventuale azione di rivalsa. **Il comma 6** allinea il termine di prescrizione dell'azione diretta a quello dell'azione nei confronti del soggetto individuato quale responsabile del danno, in coerenza con la natura accessoria della tutela.

4.13. La colpa nelle azioni risarcitorie del danno cagionato dall'utilizzo di sistemi di intelligenza artificiale.

La disciplina introdotta dagli **artt. 16-20** del **d.lgs. n. 160 del 2026** non configura un'autonoma fattispecie di responsabilità civile per i danni cagionati dall'utilizzo di sistemi di intelligenza artificiale ma predispone strumenti processuali destinati a operare nell'ambito dei diversi titoli di responsabilità previsti dall'ordinamento. Il decreto legislativo lascia quindi impregiudicata la necessità di individuare, per ciascuna controversia, la regola sostanziale applicabile e, con essa, la rilevanza della colpa e il relativo regime probatorio. Le azioni di risarcimento del danno contemplate dall'**art. 16** possono infatti avere natura **contrattuale** o **extracontrattuale**, mentre l'**accesso alle prove**, **la presunzione del nesso causale** e **l'azione diretta contro l'assicuratore** intervengono soprattutto sulle difficoltà di assolvimento dell'onere probatorio e di soddisfacimento del credito risarcitorio. Ne consegue che, quando la domanda sia fondata sull'**art. 2043 c.c.**, il danneggiato resta tenuto, in linea di principio, a provare una condotta dolosa o colposa imputabile a uno o più soggetti della filiera tecnologica, oltre al danno ingiusto e al nesso causale; quando, invece, siano applicabili gli **artt. 2050 o 2051** c.c., la disciplina dell'elemento soggettivo e della prova dovrà essere ricostruita secondo i rispettivi criteri speciali; nell'azione contrattuale, infine, opererà il riparto derivante dall'**art. 1218 c.c.**, spettando al debitore dimostrare che l'inadempimento o il ritardo è dipeso da causa a lui non imputabile. La colpa, pertanto, non assume un contenuto uniforme, ma deve essere valutata in modo differenziato rispetto alla posizione concretamente occupata dal fornitore, dal *deployer*, dal produttore di componenti integrati nei sistemi di IA, dal soggetto incaricato dell'aggiornamento o dall'utilizzatore professionale. La particolare struttura dei sistemi di IA impone, inoltre, di superare una concezione della colpa limitata alla singola azione posta in essere nel momento immediatamente precedente al danno. L'errore suscettibile di fondare la responsabilità può collocarsi in una fase anteriore e riguardare la progettazione, la scelta o la qualità dei dati, la valutazione dei rischi, la validazione, la configurazione, la messa in servizio, la predisposizione delle istruzioni, il monitoraggio successivo, l'aggiornamento oppure l'organizzazione della sorveglianza umana. La colpa può anche manifestarsi nella fase di utilizzazione, quando il *deployer* impieghi il sistema al di fuori della destinazione prevista, ometta di osservare le istruzioni, non verifichi la qualità dei dati di input, trascuri anomalie o segnalazioni, mantenga in esercizio un sistema divenuto inaffidabile oppure attribuisca all'output un valore decisorio che esso non è tecnicamente destinato a possedere. La valutazione deve dunque riguardare l'intero ciclo di vita del sistema e la concreta distribuzione delle competenze, senza imputare a ciascun operatore obblighi propri di un diverso soggetto della filiera.

In questo contesto, gli obblighi stabiliti dal **regolamento IA** assumono un'importante funzione integrativa dello standard di diligenza. Le prescrizioni in materia di gestione dei rischi, qualità e governance dei dati, documentazione tecnica, registrazione automatica degli eventi, accuratezza, robustezza, cybersicurezza, trasparenza e sorveglianza umana possono contribuire a determinare il comportamento esigibile dall'operatore professionale. La loro

violazione non dovrebbe, tuttavia, essere automaticamente identificata con la colpa civilistica. Occorre verificare che l'obbligo fosse concretamente applicabile al soggetto convenuto, fosse operativo al momento della condotta e fosse diretto a prevenire il rischio effettivamente concretizzatosi. **La non conformità regolatoria** costituisce quindi un indice qualificato della deviazione dallo standard dovuto, ma non elimina la necessità di accertare la pertinenza dell'obbligo rispetto al danno. Simmetricamente, la conformità all'AI Act non esclude di per sé la responsabilità, come chiarisce l'**art. 19** del **d.lgs. n. 160**. Un sistema formalmente conforme può essere negligentemente configurato, alimentato con dati inadeguati, impiegato oltre i limiti dichiarati oppure inserito in un'organizzazione priva di controlli effettivi. La compliance regolatoria fissa quindi una soglia rilevante, ma non esaurisce il giudizio civilistico sulla diligenza esigibile nel caso concreto.

La relazione tra violazione regolatoria e colpa deve essere distinta anche dalla questione della causalità. L'art. **18** prevede una **presunzione** relativa del **nesso causale** quando il danno derivi dalla violazione di un obbligo dell'AI Act, ma non introduce, almeno in termini generali, una presunzione autonoma della colpa. La presunzione agevola l'accertamento del collegamento tra violazione e danno, **senza necessariamente dimostrare che la violazione sia soggettivamente rimproverabile al convenuto**. L'attore deve pertanto allegare e provare i fatti dai quali desumere l'inosservanza dello standard di diligenza, salvo che il titolo sostanziale azionato determini un diverso riparto dell'onere probatorio. Questa distinzione è essenziale: **la prova della violazione di un obbligo può concorrere a dimostrare la colpa, ma la presunzione causale non trasforma automaticamente ogni inosservanza dell'AI Act in responsabilità soggettiva.**

L'**art. 17 assume**, sotto tale profilo, una funzione decisiva. La prova della colpa è normalmente nella sfera di disponibilità del convenuto o di altri operatori della filiera, perché dipende dall'analisi dei registri, della documentazione tecnica, delle misure di gestione del rischio e delle modalità di supervisione umana. La norma consente al giudice, quando la domanda appare verosimile, di ordinare l'esibizione della documentazione pertinente; l'inosservanza dell'ordine può produrre conseguenze probatorie a favore del danneggiato in quanto il giudice può ritenere addirittura come ammessi i fatti come dedotti. L'accesso alle prove non elimina l'onere di allegare la condotta colposa, ma consente di assolverlo senza pretendere che il danneggiato conosca preventivamente l'architettura tecnica del sistema. In applicazione del principio di vicinanza della prova, l'allegazione dovrebbe potersi concentrare sulla concreta anomalia verificatasi, sulla funzione svolta dal sistema e sulla plausibile carenza organizzativa o tecnica, mentre la documentazione acquisita consentirà di precisare se l'errore sia dipeso dalla progettazione, dai dati, dalla configurazione, dall'aggiornamento o dalla sorveglianza umana.

Particolarmente delicata è la definizione dello standard professionale esigibile. Il parametro della diligenza non può coincidere con quello dell'utilizzatore comune quando il sistema sia progettato, commercializzato o impiegato nell'esercizio di un'attività professionale. In tali ipotesi rileva la diligenza qualificata di cui all'**art. 1176, comma 2, c.c.**,

commisurata alla natura dell'attività esercitata, allo stato delle conoscenze tecniche, alla prevedibilità del rischio e alla funzione concretamente affidata al sistema. Quanto più il sistema incide su beni primari o su decisioni ad alto impatto, tanto maggiore dovrà essere l'attenzione richiesta nella selezione, validazione, supervisione e gestione degli incidenti. Tale criterio non equivale, però, a una responsabilità per il solo fatto che l'evento si sia verificato. Anche nei settori tecnologicamente avanzati la colpa richiede l'individuazione di una condotta esigibile che il soggetto avrebbe potuto e dovuto osservare. Il giudice dovrà pertanto evitare sia di considerare inevitabile ogni errore prodotto da un sistema complesso, sia di trasformare retrospettivamente il verificarsi del danno nella prova dell'inadeguatezza di tutte le cautele adottate.

La complessità o l'opacità del sistema non possono, di per sé, escludere la colpa. Un operatore professionale che scelga di impiegare una tecnologia non adeguatamente comprensibile o controllabile assume l'obbligo di predisporre misure organizzative proporzionate al rischio. Se l'opacità impedisce una sorveglianza effettiva, tale circostanza può essere essa stessa rilevante ai fini della valutazione della diligenza, soprattutto quando il sistema sia utilizzato per decisioni suscettibili di incidere significativamente sui diritti delle persone. Per contro, l'imprevedibilità autentica del comportamento del sistema può assumere rilievo quando il convenuto dimostri di avere rispettato gli obblighi applicabili, monitorato il funzionamento, predisposto una supervisione effettiva e reagito tempestivamente alle anomalie concretamente conoscibili.

La sorveglianza umana costituisce uno dei principali terreni di accertamento della colpa. Non è sufficiente che un operatore sia formalmente inserito nel procedimento decisionale. Occorre verificare se egli disponesse delle competenze, del tempo, delle informazioni e dei poteri necessari per comprendere, contestare o disattivare l'output. Il comportamento umano non interrompe automaticamente il nesso con il funzionamento del sistema quando la decisione finale costituisca una sostanziale adesione automatica al risultato algoritmico. Al contrario, una decisione consapevole, autonoma e fondata su informazioni ulteriori può incidere sulla distribuzione delle responsabilità. La valutazione dovrà quindi concentrarsi sull'effettività del controllo, evitando che la presenza nominale di un operatore divenga uno strumento per trasferire sull'utilizzatore finale tutti i rischi della tecnologia. La colpa può infine assumere una dimensione eminentemente organizzativa. Nei sistemi complessi, il danno può dipendere non dall'errore isolato di una persona, ma dall'assenza di procedure per la scelta del sistema, la verifica dei dati, la formazione degli addetti, la gestione delle segnalazioni, l'escalation degli incidenti e la sospensione dell'utilizzo. L'accertamento dovrà allora riguardare non soltanto la condotta individuale, ma anche l'adeguatezza dell'assetto predisposto dall'impresa o dall'ente. L'impiego dell'IA non attenua gli obblighi professionali del soggetto che la utilizza, né consente di imputare senz'altro al sistema le conseguenze di una carente organizzazione. Esso introduce, piuttosto, nuovi doveri di selezione, controllo e monitoraggio, la cui intensità deve essere commisurata alla natura dell'attività, alla gravità del danno prevedibile e alla concreta possibilità di governo del rischio.

In conclusione, negli illeciti connessi all'utilizzo dell'intelligenza artificiale la colpa non va ricercata in un preteso "**comportamento colpevole**" della macchina, ma nella deviazione della condotta umana o organizzativa dallo standard esigibile nelle diverse fasi del ciclo di vita del sistema di IA. Il giudizio dovrà essere individualizzato rispetto al ruolo di ciascun operatore, distinto dall'accertamento causale e fondato su una valutazione concreta degli obblighi applicabili, delle conoscenze disponibili e delle misure ragionevolmente adottabili. Gli **artt. 17-19** del **d.lgs. n. 160 del 2026** non sostituiscono tale giudizio, ma ne rendono più effettivo lo svolgimento: facilitano l'accesso agli elementi tecnici, alleggeriscono in determinate condizioni la prova del nesso causale e impediscono che la mera certificazione di conformità sia utilizzata come automatica esimente. La colpa resta, pertanto, una categoria dogmatica che segue le regole dell'ordinamento civilistico, ma viene progressivamente specificata attraverso gli obblighi regolatori e organizzativi propri della governance dei sistemi di IA.

4.14. Aspetti problematici della disciplina della responsabilità civile da utilizzo di sistemi di intelligenza artificiale.

Gli **artt. 16-20** del **d.lgs. n. 160** segnano un passaggio significativo dal piano della regolazione preventiva dei sistemi di intelligenza artificiale a quello della tutela giurisdizionale del soggetto che assuma di essere stato danneggiato dal loro utilizzo. La disciplina muove dalla consapevolezza che, nelle controversie relative all'IA, l'effettività della tutela risarcitoria può essere compromessa dalla complessità tecnica dei sistemi e dalla conseguente asimmetria informativa tra il soggetto danneggiato e gli operatori che hanno sviluppato, fornito o utilizzato il sistema. In questa prospettiva, gli strumenti dell'accesso alle prove, della presunzione relativa del nesso causale e dell'azione diretta nei confronti dell'assicuratore mirano ad evitare che l'opacità del funzionamento del sistema si traduca, sul piano processuale, nell'impossibilità per il danneggiato di assolvere l'onere probatorio e, quindi, in una sostanziale privazione della tutela risarcitoria. La disciplina presenta, tuttavia, alcuni profili problematici di carattere strutturale. Un primo profilo deriva dal fatto che il decreto legislativo non introduce un autonomo e compiuto regime sostanziale di responsabilità civile per i danni cagionati dall'intelligenza artificiale. Le nuove disposizioni sono pertanto destinate ad operare in raccordo con le ordinarie fattispecie di responsabilità civile, nonché con la disciplina della responsabilità per danno da prodotti difettosi, con il GDPR e con le eventuali discipline speciali applicabili al settore nel quale il sistema di IA è utilizzato. Ne deriva un quadro necessariamente composito, nel quale l'individuazione, non sempre agevole, della regola di responsabilità applicabile precede logicamente l'operatività dei nuovi strumenti probatori e processuali. Un secondo profilo problematico riguarda i presupposti per l'accesso alla prova e per l'operatività delle presunzioni. Nozioni quali la verosimiglianza della pretesa, il grado di specificità richiesto per l'individuazione degli elementi probatori, la rilevanza dell'obbligo violato rispetto al danno verificatosi e il rapporto tra violazione della disciplina regolatoria e accertamento del nesso causale sono inevitabilmente destinate ad essere

"precisate" dalla interpretazione della giurisprudenza. Particolare attenzione richiederà, in particolare,, l'interpretazione dell'art. 17. La parte che richiede l'accesso non dovrebbe essere gravata di un onere di individuazione della prova documentale da acquisire così puntuale da presupporre proprio quella conoscenza tecnica che l'accesso è diretto a consentirle di acquisire. Diversamente, lo strumento rischierebbe di perdere gran parte della propria utilità pratica. Il requisito della specificità dell'istanza dovrebbe, pertanto, essere coordinato con la condizione di asimmetria informativa nella quale normalmente versa il danneggiato, consentendo l'individuazione degli elementi probatori anche attraverso categorie sufficientemente circoscritte e funzionalmente collegate ai fatti allegati. Tale esigenza deve, naturalmente, essere contemperata con la tutela del contraddittorio, la proporzionalità della misura e la protezione delle informazioni riservate.

Analoghe esigenze di cautela riguardano la presunzione prevista dall'art. 18. La violazione di un obbligo imposto dalla normativa europea in materia di intelligenza artificiale non dovrebbe essere considerata, di per sé, sufficiente a determinare un automatismo nell'accertamento del nesso causale. Occorre, piuttosto, verificare che l'obbligo che si assume violato fosse applicabile al soggetto e al sistema considerati e che fosse diretto a prevenire, o comunque a ridurre, proprio il rischio che si è concretizzato nel danno dedotto in giudizio. Il collegamento tra la finalità protettiva della norma violata e l'evento dannoso assume così una funzione essenziale nel delimitare l'ambito della presunzione ed evitare che una mera irregolarità formale si trasformi automaticamente in un meccanismo di imputazione causale. Specularmente, anche la conformità del sistema agli obblighi regolatori deve essere correttamente collocata sul piano probatorio. Essa può costituire un elemento rilevante ai fini dell'accertamento, ma non dovrebbe essere intesa come una forma di esenzione o di "immunità" dalla responsabilità civile. La conformità attiene infatti al rispetto di determinati requisiti normativi e deve essere valutata in relazione alle concrete condizioni di progettazione, immissione sul mercato, messa in servizio e utilizzazione del sistema. Essa non esclude, di per sé, che il danno possa derivare da modalità di impiego, caratteristiche del prodotto o condotte degli operatori suscettibili di assumere rilievo secondo le ordinarie regole della responsabilità civile. Un terzo ordine di problemi discende dalla pluralità dei soggetti coinvolti nella filiera dell'intelligenza artificiale. Il danno può infatti collocarsi all'esito dell'interazione tra una pluralità di condotte e componenti tecnologiche. La controversia può quindi coinvolgere, a diverso titolo, produttori, fornitori, *deployer*, produttori di componenti, operatori professionali e altri soggetti della catena tecnologica. Ciò rende particolarmente delicata non soltanto l'individuazione del titolo di responsabilità riferibile a ciascun soggetto, ma anche la ricostruzione del rapporto causale tra le diverse condotte e l'evento dannoso e, ricorrendone i presupposti, l'applicazione delle regole sulla responsabilità solidale ex art.2055. In tale contesto assume rilievo anche l'azione diretta nei confronti dell'assicuratore. La sua concreta efficacia protettiva dipende necessariamente dalla struttura della copertura assicurativa e dalla delimitazione del rischio assicurato. Massimali, franchigie, esclusioni e condizioni di operatività della garanzia possono incidere sulla misura della tutela

concretamente conseguibile dal danneggiato, con particolare evidenza nelle ipotesi di danni seriali o comunque derivanti dall'impiego del medesimo sistema su una pluralità di soggetti. Nel complesso, gli artt. 16-20 non sembrano quindi delineare un sistema autonomo e autosufficiente per la disciplina della responsabilità civile da intelligenza artificiale. Essi introducono, piuttosto, strumenti destinati a inserirsi nel sistema generale della responsabilità civile, incidendo in particolare sull'accesso alle informazioni e alle prove, sulla distribuzione dell'onere probatorio e sull'effettività della tutela risarcitoria. È precisamente in questo raccordo tra disciplina speciale e categorie generali che si concentreranno, verosimilmente, le questioni interpretative di maggiore rilievo. L'applicazione delle nuove disposizioni dovrà infatti assicurare un equilibrio tra effettività dell'accesso alla prova, diritto di difesa e contraddittorio, proporzionalità delle misure istruttorie, protezione delle informazioni riservate e corretta imputazione causale del danno.

La portata più significativa della disciplina può dunque essere individuata non tanto nell'introduzione di una nuova figura di responsabile, quanto nel riconoscimento della necessità di governare processualmente il rischio derivante dall'opacità tecnologica. Il problema centrale diviene quello di evitare che l'incapacità del danneggiato di accedere alle informazioni detenute dagli operatori della filiera si traduca in un ostacolo insuperabile all'accertamento della responsabilità, senza tuttavia trasformare le difficoltà probatorie proprie dei sistemi di IA in forme surrettizie di responsabilità oggettiva. È lungo questa linea di equilibrio che appare destinata a svilupparsi la futura elaborazione giurisprudenziale.

4.15. Le questioni che possono assumere rilievo nell'attività nomofilattica.

La disciplina del risarcimento dei danni cagionati dall'impiego di sistemi di intelligenza artificiale appare destinata a porre alla giurisprudenza di legittimità questioni che trascendono la soluzione del singolo caso e investono la stessa ricostruzione sistematica della responsabilità civile nell'ambiente digitale. Il d.lgs. n. 160, infatti, dedica gli artt. 16-20 agli strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale, collocando tali disposizioni all'interno di un ordinamento nel quale continuano a operare i tradizionali titoli di responsabilità sostanziale. La funzione nomofilattica sarà pertanto chiamata, in primo luogo, a definire il rapporto tra questa disciplina processuale speciale e le categorie generali della responsabilità contrattuale ed extracontrattuale, evitando tanto la costruzione, per via interpretativa, di un indefinito statuto autonomo della «responsabilità da intelligenza artificiale», quanto l'opposta tendenza a ricondurre fenomeni tecnologicamente nuovi entro categorie tradizionali senza verificarne l'effettiva capacità "attrattiva".

Un primo terreno di particolare complessità sarà costituito dall'individuazione del criterio di imputazione della responsabilità. A seconda delle caratteristiche dell'attività e della relazione intercorrente tra il sistema, il soggetto che lo mette a disposizione, quello che lo integra e quello che lo utilizza, potranno venire in considerazione i regimi di cui agli artt. 1218, 1228, 2043, 2050 e 2051 c.c.. Non appare tuttavia possibile stabilire in via astratta che

l'utilizzazione di un sistema di intelligenza artificiale integri sempre un'attività pericolosa, né che il sistema possa invariabilmente essere considerato una «cosa» sottoposta alla custodia dell'utilizzatore. Sarà quindi probabilmente la concreta conformazione tecnologica e funzionale del sistema di intelligenza artificiale, insieme al grado di autonomia del suo funzionamento e al tipo di controllo esercitabile dall'operatore umano, a sollecitare la progressiva elaborazione di criteri interpretativi sufficientemente consolidati.

Ancora più delicata sarà la definizione della colpa nell'impiego dell'intelligenza artificiale. L'aspetto problematico della definizione di colpa nel settore anzidetto acquista particolare evidenza alla luce del Regolamento (UE) 2026/1744, cd. *Digital Omnibus*, che ha modificato la scansione temporale dell'applicazione di parte della disciplina dei sistemi ad alto rischio prevista dal regolamento IA. Nel periodo transitorio potrà dunque accadere che si verifichi un danno quando taluni obblighi regolatori specificamente riferiti al sistema non siano ancora applicabili. Si porrà allora il problema di stabilire se e in quale misura prescrizioni del regolamento IA non ancora efficaci possano assumere rilievo nel giudizio eventualmente instaurato. Esse non potranno evidentemente essere trattate come obblighi già vigenti, trasformando la loro inosservanza in automatica fonte di responsabilità; diversa, e assai più complessa, è però la questione se le cautele alle quali tali prescrizioni fanno riferimento possano trovare corrispondenza in standard di diligenza già desumibili dall'ordinamento, dalle regole tecniche, dalle conoscenze scientifiche disponibili o dalla particolare natura dell'attività esercitata. Si profila, sotto questo aspetto, una distinzione destinata probabilmente ad assumere rilievo nomofilattico tra precetto regolatorio e regola cautelare, non necessariamente coincidenti sul piano temporale e funzionale. Un secondo aspetto di particolare interesse e rilievo nomofilattico riguarderà la prova del nesso causale. Nei sistemi complessi, e soprattutto nei sistemi capaci di produrre risultati attraverso processi non immediatamente ricostruibili dall'esterno, potrebbe risultare problematico non soltanto individuare la condotta materialmente antecedente all'evento dannoso ma anche stabilire quale livello di prova possa ragionevolmente essere richiesto a chi non dispone delle conoscenze, dei dati e delle informazioni tecniche necessarie per ricostruire il funzionamento del sistema. Da ciò deriva l'importanza sistematica degli strumenti processuali introdotti dagli artt. 16-20 del d.lgs. n. 160/2026: accesso alla prova e distribuzione degli oneri probatori sono destinati a incidere concretamente sull'effettività della tutela risarcitoria. La Cassazione potrebbe essere chiamata, in particolare, a delimitare il confine tra legittima utilizzazione di meccanismi presuntivi e sostanziale trasformazione della responsabilità in responsabilità oggettiva là dove l'ordinamento continui invece a richiedere la prova di determinati elementi costitutivi per l'accertamento della responsabilità del danneggiante. Connessa alla causalità è la questione della pluralità dei soggetti coinvolti nella catena dell'intelligenza artificiale (cd. filiera tecnologica). La produzione del medesimo danno può infatti porre il problema della convergenza di condotte riferibili a soggetti diversi e assoggettate, eventualmente, anche a differenti titoli di responsabilità. Sarà quindi particolarmente significativa l'elaborazione dell'art. 2055 c.c.: occorrerà stabilire quando le condotte riferibili ai diversi protagonisti della

catena tecnologica possano considerarsi causalmente convergenti nella produzione di un unico danno e quale incidenza abbia, nei rapporti interni, la diversa efficacia causale delle singole condotte. È verosimile che proprio l'art. 2055 c.c., più che la ricerca di un unitario «responsabile dell'algoritmo», possa costituire uno degli strumenti attraverso i quali l'ordinamento interno affronterà la frammentazione soggettiva caratteristica dei sistemi complessi.

A tale possibile aspetto problematico si affiancherà quello del necessario coordinamento con la responsabilità da prodotto difettoso. La Direttiva (UE) 2024/2853 ha espressamente ricondotto il software, inclusi i sistemi di intelligenza artificiale, nell'ambito della nuova disciplina dei prodotti, prendendo inoltre in considerazione i difetti connessi agli aggiornamenti e, a determinate condizioni, al continuo apprendimento del sistema sotto il controllo del produttore. Il giudice di legittimità dovrà pertanto contribuire a delimitare i rapporti tra responsabilità da prodotto, responsabilità aquiliana e responsabilità contrattuale, soprattutto nelle situazioni nelle quali lo stesso evento dannoso possa essere ricondotto contemporaneamente alla difettosità del sistema, alla condotta dell'operatore che lo utilizza e alle scelte organizzative del soggetto che lo ha inserito nel proprio processo decisionale.

Più in generale, la questione che verosimilmente sarà affidata alla futura elaborazione nomofilattica sarà quella dei rapporti tra regolazione preventiva del rischio e responsabilità successiva per il danno. Il differimento di taluni obblighi riguardanti i sistemi ad alto rischio rende particolarmente evidente una particolare differenziazione destinata a permanere anche oltre la fase "transitoria" derivata dal differimento di alcuni obblighi di prevenzione per i sistemi ad alto rischi prevista dal *Digital Omnibus*: la responsabilità civile e la disciplina regolatoria dell'intelligenza artificiale operano su piani diversi, destinati ad interferire senza, tuttavia, necessariamente coincidere. L'inosservanza del regolamento IA potrà assumere rilievo nell'accertamento della responsabilità quando ne ricorrano i presupposti, ma non ogni violazione regolatoria determinerà automaticamente un diritto al risarcimento; specularmente, la conformità al regolamento IA non potrà di per sé escludere qualsiasi responsabilità derivante dalle regole del risarcimento del danno previste dal codice civile e dalla legislazione speciale. È probabilmente in questa opera di coordinamento che si concentrerà il contributo più significativo della giurisprudenza di legittimità. Alla Corte di cassazione non sarà richiesto di costruire ex novo una responsabilità civile dell'intelligenza artificiale, quanto piuttosto di stabilire in quale modo le categorie tradizionali del danno, della colpa, del difetto di un prodotto, della causalità, della prova e della solidarietà debbano operare all'interno di una realtà tecnologica nella quale il processo produttivo dell'evento dannoso è spesso distribuito tra una pluralità di soggetti e di componenti. L'attività interpretativa della Cassazione sarà, dunque, quella di preservare la continuità sistematica delle categorie civilistiche adattandone l'applicazione alle peculiarità dell'intelligenza artificiale e, al tempo stesso, evitando che le difficoltà conoscitive e probatorie proprie della tecnologia si traducano o in un'ingiustificata area di immunità per chi la progetta e la utilizza, oppure,

all'estremo opposto, nella surrettizia introduzione per via giurisprudenziale di una responsabilità oggettiva generalizzata per il solo fatto dell'impiego dell'IA.

5. Disposizioni di chiusura.

5.1. Disposizioni transitorie e finali.

Il titolo III del decreto legislativo detta le disposizioni finali e di chiusura e si articola in un unico capo composto di due articoli (artt. 21-22).

L'art. 21, rubricato "**Disposizioni transitorie** sull'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia" stabilisce il termine dilatorio di un anno (ovverosia **entro il 30 settembre 2027**), per la **conformazione** dei sistemi di intelligenza artificiale in uso alle forze dell'ordine[204].

Inoltre, per le disposizioni contemplate nell'intero Titolo I del decreto legislativo (articoli da 1 a 10), la cui applicazione è prevista direttamente ovvero dipende dal regolamento IA, si osservano i termini di entrata in vigore e di compiuta attuazione dello stesso regolamento IA, previsti dall'art. 113.

L'art. 113 del regolamento IA ne dispone l'entrata in vigore dal ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea* (avvenuta il 12/07/2024) e l'applicazione a decorrere dal 2/08/2026, con talune eccezioni.

Infatti, è previsto che i capi I e II si applicano a decorrere dal 2/02/2025; il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2/08/2025 (ad eccezione dell'articolo 101); che l'articolo 6, paragrafo 1, e i corrispondenti obblighi si applicano a decorrere dal 2/08/2027.

L'art. 113 è stato tuttavia modificato dall'art. 75-*quinquies* del Regolamento (UE) 2026/1744 (cd. *Digital Omnibus sull'IA* pubblicato in GUUE il 24 luglio 2026 ed entrato in vigore il 27 luglio 2026), che ha previsto:

che i capi I e II del regolamento IA si applichino a decorrere dal 2/02/2025, ma ad eccezione dell'articolo 5, paragrafo 1, primo comma, lettere b-*bis*) e b-*ter*), e dell'articolo 5, paragrafi 1-*bis* e 1-*ter*, che si applicano a decorrere dal 2/12/2026;

che il capo III, Sezioni 1, 2 e 3, ad eccezione dell'articolo 6, paragrafo 5, si applichino a decorrere dal 2/12/2027, per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 2, e dell'allegato III, e dal 2/08/2028 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, e dell'allegato I.

Infine, gli articoli da 102 a 110 si applicano a decorrere dal 27/07/2026.

[204] Art. 21: "1. I sistemi di IA che, alla data di entrata in vigore del presente decreto, formano oggetto di rapporti contrattuali o sono in fase di sviluppo o di sperimentazione per finalità di polizia ovvero sono già in uso nell'attività di polizia, sono resi compatibili con le disposizioni del capo II del titolo I, da ciascuna Forza di polizia per quanto di rispettiva competenza, entro un anno dalla predetta data. 2. Per le disposizioni del titolo I la cui applicazione è prevista direttamente ovvero dipende dal regolamento IA, si osservano i termini di entrata in vigore e di compiuta attuazione dello stesso regolamento**.**

In sostanza, per i **sistemi ad alto rischio** di cui all'allegato III (fra cui quelli utilizzati nelle **attività di contrasto**), l'applicazione è stata spostata al **2/12/2027**.

Per i sistemi ad alto rischio integrati in **prodotti fisici** l'applicazione è stata spostata al **2/08/2028**.

Le altre norme sono già applicabili o di imminente applicazione (2/12/2026).

La *Relazione illustrativa* ricorda che la normazione contenuta del decreto legislativo prevede alcuni atti successivi attuativi.

In particolare:

- l'articolo 5 demanda a un regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta delle Autorità nazionali per l'intelligenza artificiale, di concerto con il Ministro dell'interno, la definizione delle modalità di coordinamento tra lo spazio di sperimentazione di cui all'articolo 57 del regolamento IA e le attività sperimentali di sistemi di IA per finalità di polizia disciplinate dal medesimo articolo;
- l'articolo 9, comma 5, demanda a un decreto del Ministro dell'interno, di concerto con il Ministro della giustizia, sentiti il Garante e le Autorità nazionali per l'intelligenza artificiale, l'individuazione dei requisiti tecnici minimi, delle misure di monitoraggio, sicurezza e notifica relativi ai sistemi di identificazione biometrica remota in tempo reale per finalità di prevenzione, di ricerca di persone scomparse o di vittime di specifici reati (art. 8), nonché nell'ambito delle indagini preliminari per i gravi delitti indicati nell'allegato II del regolamento sull'IA (art. 14, che innesta l'art. 359-*ter* nel codice di procedura penale);
- l'articolo 10, comma 11, invece, demanda a un decreto del Ministro dell'interno, sentito il Garante, la definizione delle modalità di trattamento e memorizzazione dei dati biometrici e delle misure di sicurezza relative alle tecnologie di intelligenza artificiale per il riconoscimento facciale *a posteriori* rispetto alla commissione di un fatto di reato (*post delictum*), integrabili, ove ricorrano esigenze di ordine e sicurezza pubblica, nei sistemi di videosorveglianza installati a norma di legge.

Tali rinvii, secondo la *Relazione illustrativa*, "*appaiono giustificati dalla necessità di demandare a fonti secondarie o ad atti tecnico-amministrativi la disciplina di profili ad elevato contenuto specialistico e suscettibili di rapido aggiornamento". I termini previsti per la loro adozione risultano, in linea generale, congrui rispetto alla complessità degli adempimenti richiesti*".

Come già evidenziato in precedenza, particolare attenzione dovrà essere prestata in sede di applicazione della disciplina ai decreti attuativi laddove, normando aspetti tecnici connessi ad alcune delle procedure di maggiore impatto sulla tutela dei diritti fondamentali della persona, vadano a introdurre vere e proprie disposizioni disciplinanti in concreto l'utilizzo dei sistemi, specie negli spazi di frequentazione pubblica e per attività di carattere amministrativo.

L'art. 22 introduce la "**Clausola di invarianza finanziaria**" secondo la quale le amministrazioni interessate dovranno provvedere alle attività previste dal decreto mediante

l'utilizzo delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

La norma appare particolarmente dissonante nel contesto di riferimento laddove, da un lato, si pone l'accento sulla necessità di prevedere formazione adeguata e sperimentazione per le forze di polizia, dall'altro si vincolano le attività al costo zero.

Si tratta di una materia sensibile, complessa e centrale delle nuove dinamiche relazionali e delle prospettive di tutela dei diritti che richiede strumenti adeguati di intervento e di necessaria copertura finanziaria.

(Redattori Maria Laura Paesano e Francesco Barracca)

Il Vice Direttore	Il Direttore Aggiunto	Il Direttore
(Antonio Corbo)	(Antonio Scarpa)	(Alberto Giusti)