

BIELLE CONSULTING

Risk, Sustainability & Compliance

Bielle GRC Newsletter

N. 10 · NOVEMBRE 2026

La newsletter mensile di riferimento per amministratori e Management su normativa, giurisprudenza e rischi d'impresa.

Periodo di riferimento

Analisi eventi: ottobre 2026

Indice

1	I. Executive Summary — Le priorità assolute per il CdA
2	II. Il Fatto del Mese — Il decreto che chiude l'architettura italiana dell'AI Act
3	III. Agenda Authority e Sanzioni
4	IV. Aggiornamenti Normativi e Scadenze Operative
5	V. Framework e Prassi di Riferimento
6	VI. Giurisprudenza d'Impresa
7	VII. Azioni Prioritarie Consigliate — Cosa devono fare gli amministratori oggi
8	Contatti



I. Executive Summary — Le priorità assolute per il CdA

1. L'AI Act ha ora un'autorità che sanziona.

Con il **D.Lgs. 7 ottobre 2026, n. 179** (in vigore dal **23 ottobre 2026**) l'ACN è autorità di vigilanza del mercato sui sistemi di IA e può irrogare sanzioni fino a **35 milioni di euro o al 7% del fatturato mondiale** per pratiche vietate e fino a **15 milioni o al 3%** per violazione degli obblighi di fornitori e utilizzatori (**art. 23, co. 1-2, D.Lgs. 179/2026**).

2. Le decisioni sul personale non possono essere "solo algoritmo".

L'**art. 41 D.Lgs. 179/2026** rende **nullo** il licenziamento e ogni decisione su costituzione, modifica o estinzione del rapporto adottata unicamente su base automatizzata; il consenso del lavoratore non sana nulla.

3. NIS2 passa dalla carta agli impianti.

Dall'11 ottobre due ondate di attacchi hanno manomesso da remoto i sistemi di refrigerazione connessi di supermercati in diversi Stati UE, Italia compresa, e di tre siti di stoccaggio plasma in Francia; l'ACN ha emesso due avvisi urgenti (**13 ottobre e 4 novembre 2026**) estesi a ospedali e laboratori, mentre dal 1° novembre sono operativi i poteri ispettivi (**artt. 34-38 D.Lgs. 138/2024**). Rischio: fino a **7 milioni di euro o l'1,4% del fatturato** per i soggetti importanti, **10 milioni o il 2%** per gli essenziali (**art. 38**).

4. Dati sanitari "anonimi" che non lo sono: 7 milioni di euro.

Il Garante ha sanzionato IQVIA Solutions Italy (**provv. n. 710/2026**) per una banca dati di un milione di pazienti ritenuta anonima dalla società e reidentificabile per l'Autorità: la qualificazione del dato è una decisione di *governance*, non un dettaglio tecnico (**artt. 5, 6, 9, 35 GDPR**).

5. La responsabilità 231 non si trasmette per contratto.

La Cassazione (Sez. II, **n. 38060/2026**) ha escluso la responsabilità dell'ente distaccante per il reato del dipendente distaccato: senza prova rigorosa di interesse, vantaggio e deficit di vigilanza ex **artt. 5-7 D.Lgs. 231/2001**, l'ente non risponde. Specularmente, il GUP di Torino ha affermato la responsabilità dell'ente per il suicidio di un lavoratore (**art. 25-septies D.Lgs. 231/2001**).

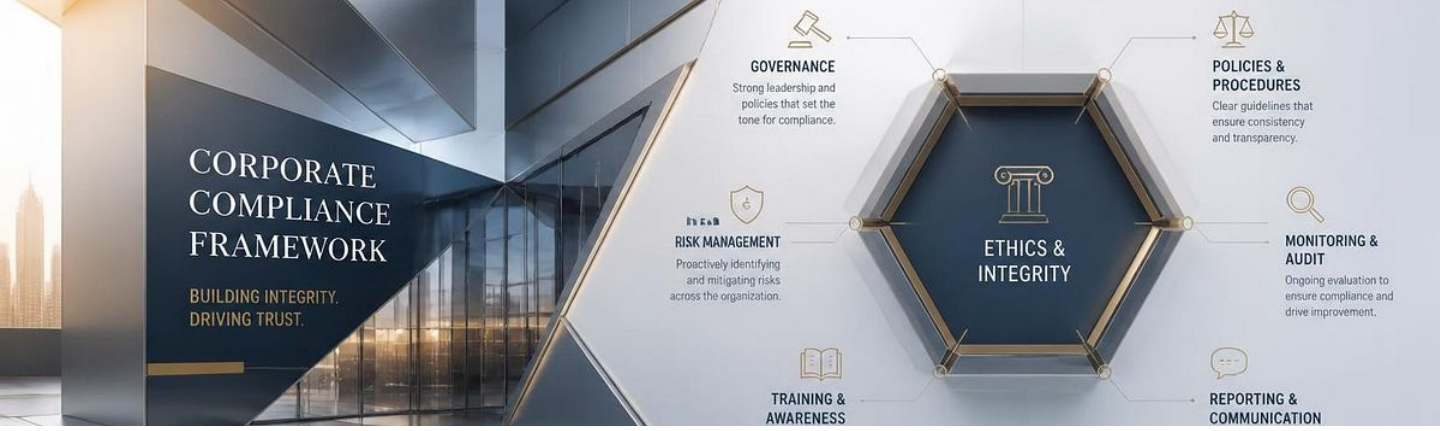


II. Il Fatto del Mese — Il decreto che chiude l'architettura italiana dell'AI Act

L'8 ottobre 2026 è stato pubblicato nella Gazzetta Ufficiale n. 234 il **decreto legislativo 7 ottobre 2026, n. 179**, secondo decreto attuativo della **legge 23 settembre 2025, n. 132**, dopo il **D.Lgs. 9 settembre 2026, n. 160** che aveva introdotto il reato di omessa adozione di misure di sicurezza nei sistemi di IA (**art. 437-bis c.p.**) e il nuovo **art. 25-vicies D.Lgs. 231/2001**. Il decreto è in vigore dal **23 ottobre 2026** e completa, a pochi giorni dalla scadenza della delega, il raccordo nazionale con il **Regolamento (UE) 2024/1689**.

Il primo blocco riguarda la *governance* pubblica

L'**AgID** è autorità nazionale di notifica (**art. 4**); l'**ACN** è autorità di vigilanza del mercato e punto di contatto unico con le istituzioni europee (**artt. 5 e 6**), con poteri di ispezione anche senza preavviso sulle prove in condizioni reali (**art. 15**). Banca d'Italia, CONSOB e IVASS vigilano sui sistemi ad alto rischio nei rispettivi settori; il Garante privacy conserva le competenze previste dall'**art. 74, par. 8, AI Act**.



II. Il Fatto del Mese *(segue)*

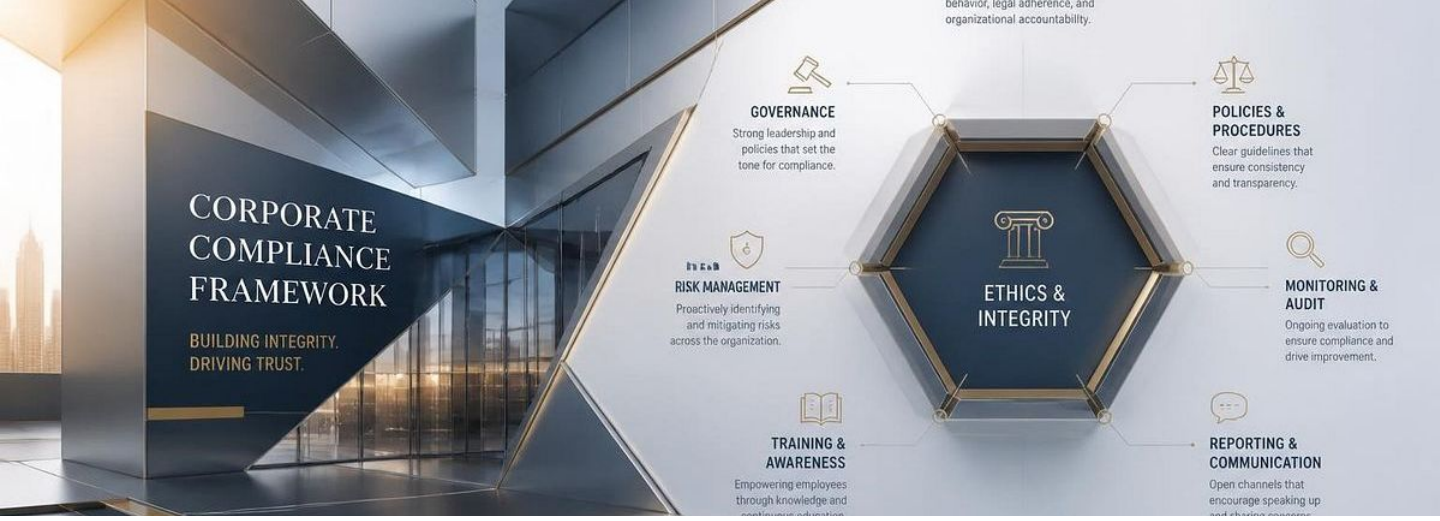
Il secondo blocco è sanzionatorio ed è quello che cambia il profilo di rischio delle imprese

L'**art. 23** riproduce i massimali europei: fino a **35 milioni di euro o il 7% del fatturato mondiale** per le pratiche vietate (**art. 5 AI Act**); fino a **15 milioni o il 3%** per la violazione degli obblighi di fornitori, importatori, distributori e *deployer* (tra cui gli **artt. 26 e 50 AI Act**, cioè obblighi degli utilizzatori e trasparenza); fino a **7,5 milioni o l'1%** per informazioni inesatte alle autorità. A questi si aggiunge un illecito di matrice nazionale: fino a **1 milione di euro o lo 0,5% del fatturato** per la violazione della valutazione d'impatto sui diritti fondamentali (**art. 27 AI Act**) e del diritto alla spiegazione delle decisioni individuali (**art. 86 AI Act**). L'**art. 22** consente, per violazioni di scarsa offensività, ordini di rimozione e la "dichiarazione pubblica" dell'infrazione: una sanzione reputazionale che per molte imprese pesa più di quella pecuniaria. L'**art. 24** impone la pubblicazione dei provvedimenti sanzionatori sul sito dell'autorità.

Il terzo blocco incide direttamente sui processi aziendali

L'**art. 41** stabilisce che le decisioni finali su costituzione, modifica o risoluzione del rapporto di lavoro, compresi provvedimenti disciplinari e valutazioni delle prestazioni, non possono essere adottate unicamente su base automatizzata; la decisione resta riservata a una persona fisica con potere effettivo; il lavoratore ha diritto a una motivazione intelligibile; il licenziamento in violazione è **nullo** e il consenso del lavoratore non costituisce eccezione.

L'**art. 42** porta l'IA dentro il **DVR**: i sistemi che incidono su organizzazione del lavoro, ritmi produttivi o processi decisionali rilevanti per la sicurezza vanno valutati ai sensi dell'**art. 28 D.Lgs. 81/2008**, con obbligo di informazione e formazione specifica. L'**art. 52**, infine, qualifica dati, algoritmi e metodi di addestramento come informazioni aziendali tutelabili ai sensi dell'**art. 98 c.p.i.**, a condizione che l'impresa adotti misure di segretezza adeguate.



II. Il Fatto del Mese *(segue)*

La finestra per le imprese

Il quadro, letto insieme al rinvio al **2 dicembre 2027** degli obblighi sui sistemi ad alto rischio dell'Allegato III (**Reg. (UE) 2026/1744**), consegna alle imprese una finestra di tredici mesi in cui le autorità sono già operative e il perimetro del sistema sanzionatorio è definito.

MESSAGGIO PER IL CDA

Gli amministratori sono chiamati a trattare l'intelligenza artificiale come un rischio d'impresa censito e governato, non come un progetto IT. Tre azioni:

- **Approvare un inventario dei sistemi di IA in uso**, con classificazione del rischio ai sensi dell'AI Act e indicazione del responsabile interno.
- **Rivedere i processi HR** che impiegano strumenti automatizzati, inserendo un passaggio decisionale umano documentato ai sensi dell'**art. 41 D.Lgs. 179/2026**.
- **Aggiornare DVR e Modello 231** integrando i rischi da IA (**art. 42 D.Lgs. 179/2026; art. 25-vicies D.Lgs. 231/2001**).



II. Il Fatto del Mese *(segue)*

Sintesi sanzioni e presidi operativi (D.Lgs. 179/2026)

Pratiche vietate (art. 5 AI Act / art. 23)

Fino a **35 milioni di euro o 7% del fatturato mondiale**

Obblighi fornitori e *deployer* (art. 23)

Fino a **15 milioni di euro o 3% del fatturato mondiale**

Informazioni inesatte alle autorità (art. 23)

Fino a **7,5 milioni di euro o 1% del fatturato mondiale**

Valutazione d'impatto e trasparenza (art. 23)

Fino a **1 milione di euro o 0,5% del fatturato** (artt. 27 e 86 AI Act)

Processi HR e divieto automazione esclusiva (art. 41)

Licenziamento o provvedimento **nullo**; obbligo di persona fisica con potere effettivo

DVR e tutela del segreto aziendale (artt. 42 e 52)

Integrazione obbligatoria nel DVR (art. 28 D.Lgs. 81/2008); algoritmi e dati tutelabili ex art. 98 c.p.i.



III. Agenda Authority e Sanzioni

[GARANTE PRIVACY] — 2 ottobre 2026 — Sanzione: € 7.000.000 (provv. n. 710 del 23 settembre 2026, IQVIA Solutions Italy S.r.l.)

Con il **provvedimento n. 710 del 23 settembre 2026**, reso noto il 2 ottobre, il Garante ha sanzionato IQVIA Solutions Italy Srl. La società aveva costruito, raccogliendo dati da circa 800 medici di medicina generale, una banca dati su un milione di pazienti (anno di nascita, sesso, diagnosi, prescrizioni, esami, vaccinazioni, localizzazione) utilizzata per studi commissionati anche da aziende farmaceutiche, qualificandola come anonima. Per l'Autorità il codice associato a ciascun paziente, unito alla granularità delle informazioni, consentiva la reidentificazione con mezzi ragionevoli: i dati erano quindi personali e relativi alla salute, trattati senza base giuridica e informativa adeguata (**artt. 6, 9, 13-14 GDPR**), senza limiti di conservazione (dati dal 2001), senza valutazione d'impatto (**art. 35 GDPR**) e senza misure di sicurezza adeguate (**art. 32 GDPR**). La società è stata ritenuta titolare fin dalla raccolta e ha **120 giorni** per adeguare il trattamento.

Impatto pratico per le imprese: la scelta di qualificare un dataset come "anonimo" va documentata con un test di reidentificazione e approvata dal DPO; chi acquista analisi di mercato basate su dati sanitari deve verificare la catena di liceità del fornitore.



III. Agenda Authority e Sanzioni *(segue)*

[ACN] 13 ottobre e 4 novembre 2026 — Avvisi urgenti sulla catena del freddo

Tra l'11 ottobre e il 2 novembre due ondate di attacchi hanno manomesso da remoto gli impianti di refrigerazione di supermercati in Francia (circa 700 punti vendita), Belgio, Paesi Bassi, Svezia e Italia (Coop e Conad in Sicilia e Veneto, una società di ristorazione toscana con notifica NIS) e di tre siti di stoccaggio plasma dell'Établissement français du sang, raggiunti **attraverso il fornitore delle apparecchiature**. Vettore: interfacce di telegestione esposte su Internet su controller spesso obsoleti, con sbrinamento forzato e soglie di temperatura alterate; nessuna rivendicazione, indagini in corso. Il bollettino ACN del **13 ottobre** fissa sei misure: **censimento** di controllori, gateway e sistemi di teleassistenza (inclusi i router dei fornitori); **separazione OT/IT** e nessuna funzione amministrativa esposta; teleassistenza solo via VPN con **MFA**; pulizia di account e password predefinite; verifica di soglie e allarmi; aggiornamento o sostituzione dei dispositivi fuori supporto. L'allerta del **4 novembre** estende i destinatari a **ospedali, laboratori e strutture che conservano materiali biologici**. La **Det. ACN n. 314287/2026** (dal **25 ottobre**) riordina intanto la piattaforma NIS: registrazione 2027 dal **1° gennaio al 28 febbraio**, verifiche automatizzate, **10 giorni** per integrare.

*Impatto pratico per le imprese: ogni impianto connesso — frigo, HVAC, building management, PLC, controllo accessi — è superficie d'attacco ex **artt. 23-24 D.Lgs. 138/2024**; un fornitore con accesso remoto va governato come un utente interno.*



IV. Aggiornamenti Normativi e Scadenze Operative

NIS2 — 31 ottobre 2026: fine della fase di adeguamento. Per i soggetti inseriti nell'elenco NIS nella primavera 2025, i **18 mesi** per adottare le misure di sicurezza di base (**art. 3 Det. ACN 379907/2025**; **artt. 23-24 D.Lgs. 138/2024**) sono scaduti al più tardi il **31 ottobre 2026**. Da novembre l'ACN esercita i poteri di verifica e ispezione, con sanzioni fino a **10 milioni di euro o il 2% del fatturato mondiale** per i soggetti essenziali.

Gli incidenti di ottobre e novembre chiariscono il perimetro dell'obbligo di notifica: la manomissione di una cella frigorifera che causa o può causare grave perturbazione operativa o perdita finanziaria è "incidente significativo" ai sensi dell'**art. 25 D.Lgs. 138/2024**, con preallarme al CSIRT Italia entro **24 ore**, notifica entro **72 ore** e relazione finale entro **un mese**; l'obbligo grava sui soggetti NIS della produzione e distribuzione alimentare all'ingrosso, non sul singolo punto vendita al dettaglio.

Tracking pixel nelle e-mail — 29 ottobre 2026. Dal 29 ottobre è richiesto il consenso preventivo, libero e specifico ai sensi dell'**art. 122 Codice privacy**, con informativa dedicata e revoca semplice. Sanzione applicabile: fino a **20 milioni di euro o il 4% del fatturato** (**art. 83, par. 5, GDPR**).

Norme vigenti e applicabili

Reg. (UE) 2024/2847 (*Cyber Resilience Act*)

Dall'**11 settembre 2026** si applica l'art. 14. Il fabbricante di prodotti con elementi digitali notifica al CSIRT il coordinatore e a ENISA le vulnerabilità attivamente sfruttate e gli incidenti gravi: preallarme entro **24 ore**, notifica entro **72 ore**, relazione finale entro 14 giorni dalla disponibilità di una misura correttiva o di attenuazione.

Reg. (UE) 2023/2854 (*Data Act*)

Riguarda i prodotti connessi, cioè i beni che raccolgono dati sul proprio utilizzo e li comunicano (macchinari, veicoli, elettrodomestici), e i servizi digitali necessari al loro funzionamento. Quelli immessi sul mercato dopo il **12 settembre 2026** devono essere progettati in modo che i dati generati siano, per impostazione predefinita, accessibili all'utente in modo facile, sicuro e gratuito, in un formato strutturato e leggibile da dispositivo automatico (art. 3, par. 1). Sono esclusi i prodotti di micro e piccole imprese (art. 7).



IV. Aggiornamenti Normativi e Scadenze Operative *(segue)*

Scadenze imminenti

31 dicembre 2026

Designazione del referente CSIRT per i soggetti NIS inseriti nel 2026.

1° gennaio – 28 febbraio 2027

Registrazione annuale sulla piattaforma NIS (**Det. ACN 314287/2026**).



V. Framework e Prassi di Riferimento

Assonime, Circolare n. 24 del 15 ottobre 2026 — "Intelligenza artificiale e governance societaria nella riforma del TUF".

L'associazione delle società per azioni legge le novità introdotte dal **D.Lgs. 27 marzo 2026, n. 47** (riforma del TUF, in vigore dal 29 aprile 2026): l'ingresso delle definizioni di "sistema di intelligenza artificiale" e "rischio informatico" nell'**art. 1 TUF**, il rafforzamento del ruolo del comitato controllo e rischi e dell'amministratore incaricato (**art. 147-sexies TUF**) e l'obbligo, dalle relazioni sul governo societario relative all'esercizio 2027, di informare sull'esistenza di una *policy* sull'uso dell'IA (**art. 123-bis, co. 2, TUF**). Assonime chiarisce che non esiste un obbligo generalizzato di adottare l'IA, ma che chi la usa deve ricondurla agli assetti adeguati ex **art. 2086 c.c.**: mappatura dei sistemi in uso, policy scritta, valutazione di figure dedicate (*AI governance officer*, comitato tecnologico), presidio su errori nei dati, discriminazioni algoritmiche, opacità degli output e uso non autorizzato di strumenti da parte del personale. La responsabilità decisionale resta in capo alle persone.

Impatto pratico per le imprese: la circolare, pur rivolta alle quotate, fornisce il benchmark che consulenti tecnici e giudici useranno per valutare l'adeguatezza degli assetti anche nelle non quotate; una policy IA approvata dagli amministratori è oggi il documento minimo difensivo.



VI. Giurisprudenza d'Impresa

1. **Cass. Pen. Sez. II, n. 38060/2026 (ud. 30 set, dep. 30 ott 2026)**
   Distacco del dipendente e responsabilità dell'ente: esclusa responsabilità dell'ente distaccante senza prova rigorosa ex artt. 5-7 D.Lgs. 231/2001.
2. **GUP Tribunale di Torino, sent. n. 1363/2026 (ottobre 2026)**
   Suicidio del lavoratore e colpa di organizzazione: responsabilità dell'ente ex art. 25-septies D.Lgs. 231/2001 per omessa valutazione stress da lavoro-correlato.

DISTACCO DEL DIPENDENTE E RESPONSABILITÀ DELL'ENTE — Rif.: Cass. Pen. Sez. II, n. 38060/2026, ud. 30 settembre, dep. 30 ottobre 2026

Il Caso: Una società era chiamata a rispondere ex D.Lgs. 231/2001 per una truffa aggravata commessa nell'ambito di un appalto pubblico. Il reato era riconducibile a un suo dipendente, distaccato presso una società consortile con funzioni di capo cantiere. I giudici di merito avevano escluso la responsabilità dell'ente distaccante per mancanza di prova; il Procuratore generale ha proposto ricorso.

La Sentenza: La Corte rigetta il ricorso. Il rapporto formale di lavoro e un vantaggio economico eventuale non bastano: occorre accertare in concreto i criteri di imputazione degli **artt. 5, 6 e 7 D.Lgs. 231/2001**, inclusa l'effettiva titolarità degli obblighi di direzione e vigilanza, e provare la responsabilità oltre ogni ragionevole dubbio.

Analisi Tecnica per il Board: I contratti di distacco e i rapporti consortili vanno rivisti per allocare espressamente i poteri di direzione e vigilanza; il Modello della distaccante deve prevedere flussi informativi dal distaccato e clausole 231 nei contratti con la consortile.

SUICIDIO DEL LAVORATORE E COLPA DI ORGANIZZAZIONE — Rif.: GUP Tribunale di Torino, sent. n. 1363/2026, ottobre 2026

Il Caso: Un autista, sottoposto per un periodo prolungato a condotte vessatorie sul luogo di lavoro, si è tolto la vita. Il giudice ha ricostruito il nesso tra le persecuzioni subite e il crollo psicologico del lavoratore, rilevando che il documento di valutazione dei rischi non considerava lo stress lavoro-correlato e che l'azienda non disponeva di presidi preventivi.

La Sentenza: Il GUP ha affermato la responsabilità del datore di lavoro, del preposto e dell'ente ai sensi dell'**art. 25-septies D.Lgs. 231/2001**, in relazione all'omessa valutazione del rischio da stress lavoro-correlato prevista dall'**art. 28, co. 1, D.Lgs. 81/2008** e all'assenza di un sistema di prevenzione.

Analisi Tecnica per il Board: La valutazione dello stress lavoro-correlato non è un adempimento formale: va aggiornata con indicatori reali (segnalazioni, assenze, turnover) e collegata al canale *whistleblowing* e all'OdV; il Modello deve prevedere un protocollo di gestione delle segnalazioni di molestie con tempi certi.



VII. Azioni Prioritarie Consigliate — Cosa devono fare gli amministratori oggi

1. Censire e classificare i sistemi di IA.
L'entrata in vigore del D.Lgs. 179/2026 rende sanzionabile l'uso non governato dell'intelligenza artificiale. Gli amministratori devono ottenere un inventario dei sistemi in uso, inclusi quelli adottati informalmente dal personale, con la classificazione del rischio e l'indicazione di chi ne risponde.

2. Garantire un decisore umano in ogni processo assistito dall'IA.
L'art. 41 D.Lgs. 179/2026 rende nulle le decisioni sul rapporto di lavoro adottate unicamente su base automatizzata, e **l'ambito HR** è quello in cui il rischio è più immediato: selezione, valutazione, provvedimenti disciplinari e licenziamenti assistiti da software vanno riprogettati per garantire una decisione finale umana motivata e tracciata. Il principio vale però per tutti i processi in cui l'IA produce raccomandazioni o decisioni — affidamento del credito ai clienti, selezione dei fornitori, controlli antifrode, risposte ai reclami — perché la sorveglianza umana è un obbligo del *deployer* ai sensi dell'**art. 26 AI Act**, la cui violazione è sanzionata fino a **15 milioni di euro o al 3% del fatturato** (**art. 23, co. 2, D.Lgs. 179/2026**).

3. Portare l'IA e lo stress lavoro-correlato nel DVR e nel Modello 231.
L'art. 42 D.Lgs. 179/2026 e l'art. 25-vicies D.Lgs. 231/2001 impongono di aggiornare valutazione dei rischi, formazione e protocolli; la sentenza torinese ricorda che il DVR incompleto sullo stress lavoro-correlato apre la strada alla responsabilità dell'ente.

4. Chiudere il cerchio NIS2, o aprirlo se si è rimasti fuori.
Per chi è in elenco dal 2025 la fase di adeguamento è finita: serve un fascicolo di evidenze pronto per un'ispezione ACN e un controllo dati sulla piattaforma prima di gennaio. Chi non si è registrato ma rientra negli **Allegati I-IV D.Lgs. 138/2024** deve provvedere nella finestra del **1° gennaio – 28 febbraio 2027**, verificando il perimetro e avviando la registrazione e il *gap assessment*.



VII. Azioni Prioritarie Consigliate (segue)

5. Censire e governare tutto ciò che è connesso in rete.

Gli attacchi alla catena del freddo sono passati da pannelli di telegestione raggiungibili da Internet e da accessi di manutenzione mai revocati: **nessuna azienda può proteggere ciò che non sa di avere**. Gli amministratori devono chiedere un **inventario completo di dispositivi, impianti e beni connessi** — frigo, HVAC, *building management*, PLC, router e piattaforme di telegestione dei fornitori — con responsabile e stato di supporto, e far **separare la rete degli impianti da quella gestionale**, senza interfacce amministrative esposte. Gli **accessi di terzi** (manutentori, installatori, teleassistenza) vanno trattati come utenze interne: account nominativi, **autenticazione a più fattori**, abilitazione a tempo, revoca a fine intervento; i **contratti di manutenzione** devono prevedere aggiornamenti, notifica di vulnerabilità e responsabilità in caso di compromissione.

6. Verificare l'anonimizzazione e i fornitori di dati.

Il caso IQVIA mostra che un dataset "anonimo" reidentificabile espone a sanzioni milionarie; chi tratta o acquista dati sanitari o profili dettagliati deve documentare il test di reidentificazione e la base giuridica del fornitore.

7. Rivedere distacchi, consorzi e deleghe.

La Cassazione premia chi documenta con precisione chi dirige e vigila sul personale distaccato: contratti di distacco, patti consortili e deleghe di funzione vanno allineati al Modello 231, con clausole che impongano flussi informativi all'OdV.



BIELLE CONSULTING

Risk, Sustainability & Compliance

Contattateci per ulteriori approfondimenti e per un assessment!

Sede

Via Thaon di Revel 21, 20159 Milano

Bielle Consulting Srl

Email & Web

info@bielleconsulting.com

www.bielleconsulting.com

linkedin.com/company/bielle-consulting

☎ Contatti

Simona Bellavia — **+39 348 150 5622**

Giacomo Leone — **+39 346 087 5317**