



BIELLE CONSULTING

Risk, Sustainability & Compliance

Bielle Consulting — Governance, Risk & Compliance Newsletter

N. 9 · OTTOBRE 2026

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



Periodo di riferimento

Analisi eventi: settembre 2026

Indice

1

I. Executive Summary — Le priorità per gli amministratori

2

II. Il Fatto del Mese — Art. 25-vicies: il reato da intelligenza artificiale è un rischio 231 vigente

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 per gli amministratori

1. L'intelligenza artificiale entra definitivamente nel catalogo 231.

Dal **30 settembre 2026** è in vigore il D.Lgs. 9 settembre 2026, n. 160, che introduce un nuovo reato presupposto legato ai sistemi di IA. Norma: **art. 25-vicies D.Lgs. 231/2001** e **art. 437-bis c.p.** Rischio: **fino a 1.000 quote** (massimo € 1.549.370) e **sanzioni interdittive**.

2. Dati "anonimi" e marketing: due ordinanze milionarie del Garante.

Sanzionate una banca dati sanitaria re-identificabile e notifiche commerciali proseguite dopo l'opposizione del cliente. Norma: **artt. 5, 9, 25 e 32 Reg. (UE) 2016/679** nel primo caso, **artt. 12 e 21 Reg. (UE) 2016/679** nel secondo. Rischio: **€ 7.000.000** e **€ 5.508.000**.

3. Asserzioni ambientali (*greenwashing*): le nuove regole sono applicabili.

Dal **27 settembre 2026** si applica il D.Lgs. 20 febbraio 2026, n. 30, che vieta le asserzioni ambientali generiche non dimostrate. Norma: **art. 2 D.Lgs. 30/2026** e **art. 27, co. 9, D.Lgs. 206/2005**. Rischio: **sanzione AGCM fino a € 10.000.000**.

4. Prodotti digitali: preallarme entro 24 ore e notifica entro 72 ore

Dall'**11 settembre 2026** i fabbricanti di prodotti con elementi digitali notificano vulnerabilità attivamente sfruttate e incidenti gravi. Norma: **art. 14 Reg. (UE) 2024/2847**. Rischio: **fino a € 15.000.000** o al **2,5% del fatturato mondiale annuo**.

5. Rendicontazione di sostenibilità 2026: va scelto lo standard.

Il Reg. delegato (UE) 2026/1563, pubblicato il **21 settembre 2026**, offre tre opzioni per l'esercizio 2026 e impone di dichiarare quella adottata. Norma: **art. 2 Reg. delegato (UE) 2026/1563**. Posta in gioco: **oltre il 60% di datapoint obbligatori in meno**, secondo la Commissione europea.



II. Il Fatto del Mese — Art. 25-vicies: il reato da intelligenza artificiale è un rischio 231 vigente

La Gazzetta Ufficiale n. 214 del 15 settembre 2026 ha pubblicato il **D.Lgs. 9 settembre 2026, n. 160**, che adegua la normativa nazionale al Reg. (UE) 2024/1689. Il decreto è **in vigore dal 30 settembre 2026** e non prevede alcun periodo transitorio per le imprese.

Il primo intervento è penale

L'art. 12 inserisce nel codice l'**art. 437-bis c.p.**, "Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi". È punito con la **reclusione da uno a cinque anni** chi omette le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi ad alto rischio, oppure le misure di sorveglianza umana, quando ne deriva un pericolo per la vita o per l'incolumità pubblica o individuale. Risponde anche l'utilizzatore professionale che omette intenzionalmente la sorveglianza umana.

Il secondo intervento riguarda gli enti

L'art. 15 introduce l'**art. 25-vicies D.Lgs. 231/2001**, "Reati commessi con l'uso di sistemi di intelligenza artificiale": **da 600 a 1.000 quote** per il delitto dell'art. 437-bis c.p. e **da 200 a 700 quote** per l'art. 612-quater c.p., che punisce la diffusione senza consenso di immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale (c.d. "contenuti sintetici") e idonei a indurre in inganno sulla loro genuinità. In entrambi i casi si applicano le sanzioni interdittive dell'art. 9, co. 2, lett. b), c), d) ed e), D.Lgs. 231/2001.

Il terzo intervento è civile

Su istanza del danneggiato, il giudice ordina l'esibizione di registri, documentazione tecnica e parametri di supervisione umana (art. 17). Quando il danno deriva dalla violazione di un obbligo del Reg. (UE) 2024/1689, **il nesso di causalità è presunto**, salvo prova contraria (art. 18). La conformità al regolamento, anche se certificata, non esclude di per sé la responsabilità (art. 19).



II. Il Fatto del Mese (segue)

Il calendario europeo non attenua il rischio

Dopo il Reg. (UE) 2026/1744, gli obblighi dell'AI Act per i sistemi ad alto rischio si applicano dal **2 dicembre 2027** (Allegato III) e dal **2 agosto 2028** (Allegato I). Il reato presupposto è invece già vigente, e il delitto dell'art. 612-quater c.p. è operativo dal 10 ottobre 2025: un contenuto sintetico diffuso nell'interesse dell'ente è oggi un rischio 231.

MESSAGGIO PER GLI AMMINISTRATORI

Gli amministratori sono chiamati a:

- **censire i sistemi di IA sviluppati, forniti o utilizzati**, distinguendo quelli ad alto rischio;
- **aggiornare *risk assessment* e Modello 231** con protocolli su sicurezza, sorveglianza umana e contenuti sintetici;
- **verificare tenuta documentale e coperture assicurative** rispetto al nuovo regime di responsabilità civile.



III. Agenda Authority e Sanzioni

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

La società alimentava una banca dati con le cartelle di circa un milione di pazienti, raccolte presso circa 800 medici e presentate come anonime. I dati erano re-identificabili e per 3.370 pazienti comprendevano elementi identificativi diretti. Il Garante l'ha qualificata titolare del trattamento fin dalla raccolta.

Impatto pratico per le imprese: chi acquista o valorizza dati "anonimizzati" verifica con test documentati il rischio di re-identificazione.

[GARANTE PRIVACY] — 3 settembre 2026 — € 5.508.000 (provv. n. 613, Banco Bilbao Vizcaya Argentaria S.A., succursale italiana)

La banca ha inviato almeno dieci notifiche commerciali in-app a un cliente che le aveva disattivate e si era opposto due volte: la revoca era registrata ma non sincronizzata con il CRM. Il procedimento nasce da un solo reclamo.

Impatto pratico per le imprese: un difetto di integrazione tra sistemi vale una sanzione milionaria; il diritto di opposizione va testato su ogni canale.

[GARANTE PRIVACY] — 18 settembre 2026 — avvio di verifiche (caso Revolut)

Dopo l'acquisizione illecita di dati personali nel caso Revolut Bank (che aveva ricevuto la richiesta dalla PEC riconducibile a un'autorità pubblica), il Garante ha avviato una verifica sulla sicurezza degli accessi delle banche italiane. Ai responsabili della protezione dei dati ha chiesto di cercare nei sistemi comunicazioni anomale provenienti dalla stessa casella PEC e, in caso di riscontro, di informare l'Autorità ai sensi dell'**art. 33 Reg. (UE) 2016/679**.

Impatto pratico per le imprese: una comunicazione ricevuta via PEC non è di per sé affidabile; le richieste di dati vanno autenticate prima dell'evasione.



III. Agenda Authority e Sanzioni (*segue*)

[CONSOB] – delibera n. 24106 del 26 agosto 2026, pubblicata il 28 settembre – € 1.150.000 complessivi

Quattro persone fisiche hanno acquistato azioni Falck Renewables nell'estate 2021 utilizzando l'informazione privilegiata sulla cessione del 60% del capitale e sulla conseguente OPA obbligatoria. Alle sanzioni si aggiungono interdizioni fino a 24 mesi e confische per **€ 906.731,43**.

Impatto pratico per le imprese: nelle operazioni straordinarie registro insider e perimetro degli informati vanno presidiati dal primo contatto.

[ANAC] – 15 settembre 2026 – € 10.000 (delibera n. 348)

Il Segretario generale di un Comune ha firmato due sanzioni disciplinari a carico di un dipendente autore di più segnalazioni; il giudice del lavoro le ha annullate come ritorsive. ANAC ha sanzionato personalmente il firmatario ai sensi D.Lgs. 24/2023.

Impatto pratico per le imprese: la responsabilità per la ritorsione è personale; ogni provvedimento verso un segnalante richiede una valutazione preventiva indipendente.

[AGCM] – Bollettino n. 36 del 21 settembre 2026 – avvio di istruttoria (PS13123, Perplexity AI, Inc.)

Il procedimento, avviato il 21 maggio 2026, riguarda pratiche commerciali e sei clausole dei Termini di Servizio aggiornati al 23 gennaio 2026. Sono sotto esame la facoltà di modificare prezzi e piani di abbonamento a sola discrezione del fornitore, anche con effetto immediato; l'esclusione di garanzie e responsabilità, comprese quelle per risposte inesatte o incomplete; l'arbitrato con rinuncia all'azione collettiva; la legge della California con foro a San Francisco. Per l'Autorità le clausole "appaiono vessatorie".

Impatto pratico per le imprese: chi offre servizi digitali ai consumatori deve riesaminare modifiche unilaterali, limitazioni di responsabilità e foro competente.

Sun	Tue	Mon	Wed	Thurs	Fri	Sat
	1	2	3	4	5	6
5	8	9	10	11	12	13
14	15	16	17	18	19	20
21	23	26	27	28	29	30

Court Filing

Client Meeting

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
7:20-9:30 pm	Brief Submission					12:00 - 11:00
7:28-19:03 pm	Discovery Review					10:00 - 10:00
7:28-29:25 pm	Discovery Review					11:00 - 12:10
05:25-06:25 pm	Hearing Preparation					16:00 - 12:00
29:03-09:09 pm	Hearing Preparation					25:00 - 12:00

IV. Aggiornamenti Normativi e Scadenze Operative

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).

D.Lgs. 20 febbraio 2026, n. 30

Dal **27 settembre 2026** sono vietate l'asserzione ambientale generica priva della prova di un'eccellenza riconosciuta delle prestazioni ambientali, l'etichetta di sostenibilità non basata su un sistema di certificazione o non stabilita da autorità pubbliche, e l'asserzione di impatto neutro, ridotto o positivo fondata sulla compensazione delle emissioni.

Reg. delegato (UE) 2026/1560

In vigore dal **24 settembre 2026**, fissa lo standard volontario di rendicontazione di sostenibilità. Dagli esercizi 2027 opera il limite alle informazioni che le imprese obbligate possono imporre ai partner fino a 1.000 dipendenti; le clausole contrarie non sono vincolanti (direttiva (UE) 2026/470).



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

Scadenze

Ottobre 2026

NIS2: i soggetti inseriti in elenco nel 2025 completano le misure di sicurezza di base entro diciotto mesi dalla comunicazione di inserimento (art. 42 D.Lgs. 138/2024).

10 novembre 2026

Entra in vigore il Reg. delegato (UE) 2026/1563 (ESRS semplificati), applicabile dagli esercizi 2027. Per l'esercizio 2026 va dichiarata la versione degli standard applicata.

2 dicembre 2026

Reg. (UE) 2024/1689 (AI Act), due novità introdotte dal Reg. (UE) 2026/1744. La prima riguarda chi fornisce sistemi di IA che generano testi, immagini, audio o video: i contenuti prodotti devono essere marcati in un formato leggibile da una macchina e riconoscibili come artificiali (art. 50, par. 2). Per i sistemi già sul mercato prima del 2 agosto 2026 il termine di adeguamento scade in questa data (art. 111, par. 4); la sanzione arriva a **€ 15 milioni o al 3% del fatturato mondiale annuo**. La seconda è un nuovo divieto: non si possono immettere sul mercato né usare sistemi di IA che generano immagini, video o audio realistici delle parti intime, o di atti sessualmente espliciti, di una persona riconoscibile senza il suo consenso (art. 5, par. 1, lett. b bis)). Il divieto colpisce i sistemi che hanno questa finalità o che non dispongono di misure adeguate a impedirla, e chi li usa a tale scopo; la sanzione arriva a **€ 35 milioni o al 7% del fatturato mondiale annuo** (art. 99)

30 dicembre 2026

Reg. (UE) 2023/1115 (deforestazione): applicazione per operatori grandi e medi; **30 giugno 2027** per micro e piccoli. Il Reg. delegato (UE) 2026/2102 ha ridefinito i prodotti interessati.



V. Framework e Prassi di Riferimento

EBA — Linee guida sulla gestione del rischio di terze parti (18 settembre 2026)

Coprono i servizi non-ICT e, una volta applicabili, abrogheranno le linee guida sull'*outsourcing* del 2019; la data di applicazione non è fissata.

Impatto pratico per le imprese: gli intermediari avviano il censimento degli accordi con fornitori.

IIA — *Third-Party Topical Requirement* (efficace dal 15 settembre 2026)

È parte obbligatoria degli standard di internal audit.

Impatto pratico per le imprese: gli audit sulle terze parti documentano la copertura di governance, rischi e controlli.

ISO 9001:2026 (16 settembre 2026)

Impatto pratico per le imprese: va pianificata la gap analysis dei sistemi certificati.

ENISA — *Threat Landscape 2026* (22 settembre 2026)

Nel 2025 il 73% delle organizzazioni prese di mira è un soggetto essenziale o importante ai sensi della NIS2.

Impatto pratico per le imprese: il piano di sicurezza deve dare priorità alla gestione delle vulnerabilità, alla resilienza al ransomware e alle dipendenze dai fornitori.



VI. Giurisprudenza d'Impresa

1

Cass. Pen., Sez. III, n. 34744/2026

Colpa di organizzazione: l'assenza del modello non basta, ma pesa

2

Cass. Pen., Sez. III, n. 34440/2026

Sequestro dell'azienda: il pericolo va motivato

3

Cass. Pen., Sez. V, n. 32893/2026

Finanziamenti pubblici: l'autodichiarazione sul procedimento 231

4

Cass. Pen., Sez. IV, n. 33423/2026

Trasportatori in stabilimento: il DUVRI segue l'interferenza, non il contratto

COLPA DI ORGANIZZAZIONE: L'ASSENZA DEL MODELLO NON BASTA, MA PESA — Rif.: Cass. Pen., Sez. III, n. 34744/2026

Il Caso: Due società sono condannate per l'illecito amministrativo dipendente dal reato dell'art. 640-bis c.p., commesso da una figura apicale per ottenere un contributo pubblico. Ricorrono sostenendo che la colpa di organizzazione sia stata desunta dalla sola mancata adozione del modello.

La Sentenza: Ricorsi inammissibili. L'assenza del modello ex artt. 6 e 7 D.Lgs. 231/2001 non è elemento costitutivo dell'illecito e la colpa di organizzazione va provata dall'accusa; qui lo era, per il deficit organizzativo complessivo e l'assenza di controlli contabili sul progetto finanziato.

Analisi Tecnica per gli amministratori: Vanno documentati i controlli effettivi sui processi che generano contributi pubblici.

SEQUESTRO DELL'AZIENDA: IL PERICOLO VA MOTIVATO — Rif.: Cass. Pen., Sez. III, n. 34440/2026

Il Caso: Il G.i.p. sequestra quote e complesso aziendale di una società ritenuta veicolo di una frode fiscale, cui è contestato l'illecito dell'art. 25-quinquiesdecies (Reati tributari) D.Lgs. 231/2001. Il Riesame annulla la misura; ricorre la Procura europea.

La Sentenza: Ricorso inammissibile. Resta ferma la decisione secondo cui il sequestro finalizzato alla confisca ex art. 53 D.Lgs. 231/2001 richiede una motivazione rigorosa sul pericolo di dispersione della garanzia patrimoniale.

Analisi Tecnica per gli amministratori: La tracciabilità delle operazioni sul patrimonio dopo la contestazione è un argomento difensivo decisivo in sede cautelare.



VI. Giurisprudenza d'Impresa (segue)

FINANZIAMENTI PUBBLICI: L'AUTODICHIARAZIONE SUL PROCEDIMENTO 231 — Rif.: Cass. Pen., Sez. V, n. 32893/2026

Il Caso: L'amministratore unico di una s.r.l., nella domanda di finanziamento agevolato, attesta l'assenza di procedimenti pendenti a carico della società ai sensi del D.Lgs. 231/2001, mentre un procedimento è in corso. La Corte d'appello conferma la sua responsabilità per il delitto di falso ideologico commesso dal privato in atto pubblico.

La Sentenza: Ricorso rigettato. È falso ideologico commesso dal privato in atto pubblico (art. 483 c.p.), anche se il requisito non era richiesto per ottenere il finanziamento.

Analisi Tecnica per gli amministratori: Ogni autodichiarazione su carichi e procedimenti dell'ente passa da una verifica legale preventiva e tracciata.

TRASPORTATORI IN STABILIMENTO: IL DUVRI SEGUE L'INTERFERENZA, NON IL CONTRATTO — Rif.: Cass. Pen., Sez. IV, n. 33423/2026

Il Caso: Nell'agosto 2013 un autotrasportatore, socio di una ditta di trasporti, muore nello stabilimento di un mangimificio durante il carico, investito da un carrello elevatore in retromarcia guidato da un dipendente del committente. Tra le imprese non c'era un appalto scritto, solo accordi verbali per singoli trasporti, però regolari. Il datore di lavoro committente è condannato per omicidio colposo (artt. 113 e 589 c.p.): nessuna informazione sui rischi, nessun DUVRI.

La Sentenza: Ricorso rigettato. Gli obblighi di informazione, cooperazione, coordinamento e DUVRI (art. 26, co. 1, lett. b), 2 e 3, D.Lgs. 81/2008) dipendono dalla concreta interferenza tra organizzazioni nello stesso luogo di lavoro, non dalla qualificazione civilistica del rapporto. Prassi consolidate ed esperienza dei lavoratori non sostituiscono le cautele dovute.

Analisi Tecnica per gli amministratori: Il censimento delle interferenze comprende vettori, manutentori e fornitori abituali, anche senza contratto scritto. Viabilità interna e aree di carico vanno regolate nel DUVRI, a presidio dell'art. 25-septies D.Lgs. 231/2001.



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

1

Portare l'intelligenza artificiale nel Modello 231

Il nuovo art. 25-bis del D.Lgs. 231/2001 richiede un aggiornamento del *risk assessment* che parta dall'inventario dei sistemi di IA in uso. I protocolli coprono sicurezza, sorveglianza umana e impiego di contenuti sintetici.

2

Mettere in ordine prove e polizze sui sistemi di IA

Con il nesso causale presunto, la difesa in giudizio dipende da registri, documentazione tecnica e tracce della supervisione umana. La copertura assicurativa va verificata alla luce delle nuove regole di responsabilità civile.

3

Verificare l'anonimizzazione prima di usare i dati

Un dataset dichiarato anonimo resta dato personale se è re-identificabile. Contratti con i fornitori, ruoli privacy e test tecnici vanno riesaminati.

4

Collaudare il diritto di opposizione su tutti i canali

La revoca del consenso al marketing deve propagarsi a CRM, app e fornitori esterni. Un test periodico documentato evita che un singolo reclamo diventi una sanzione di sistema.

5

Passare al vaglio ogni asserzione ambientale

Etichette, sito, cataloghi e offerte commerciali contengono spesso formule generiche ora vietate. Ogni affermazione va ricondotta a una prova verificabile o rimossa.

6

Organizzare la risposta agli incidenti sui prodotti digitali

Chi fabbrica prodotti con elementi digitali ha bisogno di un processo capace di preallarmare in 24 ore e di notificare entro 72 ore. Il processo va provato con una simulazione.

7

Scegliere lo standard di sostenibilità e rivedere i questionari ai fornitori

La scelta tra vecchi e nuovi ESRS per l'esercizio 2026 va deliberata e dichiarata. Le richieste informative alla filiera vanno riallineate al limite dello standard volontario.



BIELLE CONSULTING

Risk, Sustainability & Compliance

Governance, Risk & Compliance per le imprese italiane

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**