



**BIELLE  
CONSULTING**

---

Risk, Sustainability & Compliance

Bielle Consulting - Governance, Risk &  
Compliance Newsletter

N.4 Aprile 2026

## **Indice**

I. Executive Summary	3
II. IL FATTO DEL MESE: Il "Caso Intesa" e il Crollo della Governance dei Dati	4
III. Agenda Authority & Governance: Focus su Antitrust e Antiriciclaggio	5
V. Focus ESG e Risk Management	6
V. Giurisprudenza e Sicurezza: L'Inchiesta Ceva e l'Autonomia della Responsabilità 231	7
VI. Azioni Prioritarie Consigliate	8

## I. Executive Summary

A seguito degli eventi di marzo 2026 le priorità assolute per il Board sono quattro:

1. **Privacy Accountability sotto Stress:** Il Garante ha irrogato sanzioni per complessivi **49,4 milioni di euro** a Intesa Sanpaolo nel solo mese di marzo. I provvedimenti colpiscono i sistemi di monitoraggio degli accessi ai dati PEP (Persone Politicamente Esposte) e la mancanza di trasparenza nei trasferimenti massivi di clientela verso banche digitali.
2. **Repressione Strategica del Greenwashing:** Con la pubblicazione del **D.Lgs. 30/2026** (9 marzo), le dichiarazioni ambientali generiche sono vietate se prive di evidenze scientifiche accessibili. Il rischio è l'**annullamento dei contratti** con i clienti che avevano fatto affidamento sulle dichiarazioni e pesanti sanzioni pecuniarie per pratiche commerciali scorrette.
3. **Responsabilità di Filiera e Frodi IVA:** L'inchiesta su **Ceva Logistics** (sequestro di **27,3 milioni** il 3 marzo) consolida per i grandi committenti il rischio di "colpa di organizzazione" nella gestione della catena di fornitura (filiera) anche in presenza di Modelli 231.
4. **Governance Operativa dell'AI:** Il 5 marzo la Commissione ha pubblicato il secondo progetto del **Codice di Buone Pratiche** sulla trasparenza, rendendo il **watermarking** (marcatura digitale) obbligatorio entro il **2 novembre 2026** per tutti i contenuti sintetici. Parallelamente, il pacchetto **Digital Omnibus**, in fase di negoziazione, propone lo slittamento degli obblighi per i sistemi ad alto rischio al 2027.

## II. IL FATTO DEL MESE: Il "Caso Intesa" e il Crollo della Governance dei Dati



Attraverso due provvedimenti coordinati, il Garante Privacy ha colpito l'assetto dei controlli interni della prima banca italiana, evidenziando che l'innovazione tecnologica non può eludere il principio di *accountability*.

### I Pilastri della Sanzione (€49,4 mln totali):

- **Operazione Isybank (€17,6 mln - 12 marzo):** Accertata la profilazione illecita di 2,4 milioni di clienti trasferiti alla banca digitale senza **base giuridica idonea**. Le comunicazioni tramite "archivio app" in periodo estivo sono state giudicate inadeguate a garantire la prevedibilità del trattamento per l'interessato.
- **Data Breach PEP (€31,8 mln - 26 marzo):** Riscontrata l'incapacità dei sistemi di rilevare per oltre due anni gli accessi indebiti di un dipendente ai dati di 3.573 clienti, inclusi **soggetti pubblici e politicamente esposti (PEP)**. L'Autorità ha sanzionato la **mancata differenziazione dei controlli** basata sul rischio specifico degli interessati e la tardività nella notifica del breach.

**Messaggio per il CdA:** La Compliance va considerata non come un mero onere amministrativo, bensì come un elemento fondamentale per la stabilità economica dell'azienda. In seguito a questo specifico caso, le organizzazioni che trattano un elevato volume di dati particolari o sensibili sono tenute a implementare:

- Sistemi di allerta automatizzati per identificare e segnalare immediatamente accessi o interrogazioni non standard.
- Una rigorosa validazione legale di ogni fase del processo di *customer migration*.

### III. Agenda Authority & Governance: Focus su Antitrust e Antiriciclaggio



- **Antitrust: Maxi-Sanzione a Morellato (€25,9 mln):** Il 31 marzo l'AGCM ha sanzionato Morellato Spa per un'intesa verticale restrittiva della concorrenza attuata tra il 2018 e il 2025. La società ha imposto ai rivenditori limiti agli sconti massimi e il **divieto assoluto di vendita su marketplace terzi** (Amazon, eBay), mentre operava direttamente su tali canali. Chi non si adeguava subiva il blocco degli ordini: una strategia definita "illecita" dalla stessa società in comunicazioni interne acquisite dall'Autorità.
- **AGCM e UX Design:** Il 23 marzo l'Antitrust ha sanzionato **Trustpilot per 4 milioni di euro**. Sotto accusa l'uso di **dark patterns** (interfacce manipolative) che inducevano in errore sulla rappresentatività delle recensioni. La conformità legale deve ora includere la validazione delle interfacce utente (UX/UI Compliance).
- **UIF (Antiriciclaggio):** Pubblicata il 31 marzo la comunicazione sulla prevenzione di abusi legati a **agevolazioni e contratti pubblici**. Introdotti i codici fenomenologici **PA1 - Abusi relativi all'accesso e/o all'utilizzo di agevolazioni pubbliche** e **PA2 - Abusi relativi a contratti pubblici** per segnalare frodi basate su false identità digitali o attestazioni professionali contraffatte finalizzate all'indebita percezione di fondi pubblici.

## V. Focus ESG e Risk Management



**D.Lgs. 30/2026 e Marketing Ambientale:** In vigore dal 24 marzo, il decreto proibisce dichiarazioni ambientali generiche (es. "green", "amico della natura") se prive di una **metodologia scientifica verificabile** e accessibile (es. QR code). Le imprese hanno tempo fino a settembre 2026 per conformare il packaging, pena sanzioni AGCM fino al **4% del fatturato**.

### **AI Act: Il Doppio Binario di Marzo 2026:**

Il mese ha visto un'accelerazione sia sul fronte tecnico che su quello dei tempi di attuazione:

- **Codice di Buone Pratiche (5 marzo):** La Commissione ha rilasciato la seconda bozza delle linee guida sulla trasparenza (Art. 50). Diventa operativo l'obbligo di **watermarking** (tecnica di marcatura leggibile da macchina inserita nei contenuti generati o manipolati da sistemi di intelligenza artificiale, come testi, audio, immagini e video) entro il **2 novembre 2026** per tutti i testi, immagini e video generati da IA, per prevenire disinformazione e deepfake.
- **Mandato "Digital Omnibus" (13/26 marzo):** Consiglio e Parlamento UE hanno avviato le negoziazioni per posticipare le scadenze dei sistemi ad alto rischio (Allegato III) al **2 dicembre 2027**.
- **AI Literacy:** Resta fermo l'obbligo di alfabetizzazione del personale, con sanzioni applicabili già dall'**agosto 2025**.

## V. Giurisprudenza e Sicurezza: L'Inchiesta Ceva e l'Autonomia della Responsabilità 231



- **L'Inchiesta Ceva Logistics:** La Procura di Milano ha eseguito un sequestro d'urgenza di **27,3 milioni di euro** nei confronti della multinazionale.
  - **Il Meccanismo:** Contestata una frode IVA tramite "società serbatoio" che omettevano sistematicamente il versamento di imposte e contributi, offrendo prezzi fuori mercato.
  - **La Responsabilità 231:** Alla società viene contestata la "**colpa di organizzazione**": la multinazionale non ha predisposto audit sostanziali sui fornitori privi di reale autonomia imprenditoriale. La Procura sottolinea che le condotte sono espressione di una **strategia aziendale** volta alla massimizzazione del profitto tramite l'indebita detrazione dell'IVA.
- **Cass. 8397/2026 (4 marzo): L'Inviolabilità della Responsabilità 231**
  - **Il Caso:** Grave infortunio a un tirocinante causato dalla mancanza di DPI e di un addestramento specifico.
  - **La Sentenza:** La Suprema Corte ha confermato la condanna dell'ente ex art. 25-septies 231 nonostante la **prescrizione del reato per la persona fisica**.
  - **Analisi Tecnica:** La Corte chiarisce che il Modello 231 è un sistema "autonomo" rispetto al D.Lgs. 81/08. L'ente risponde penalmente ogni volta che l'illecito deriva da un **risparmio di spesa** effettuato sulla sicurezza (in questo caso, i costi di formazione e DPI). La prescrizione del manager non salva la società se sussiste il vantaggio economico derivante dall'omissione organizzativa.

## VI. Azioni Prioritarie Consigliate

1. **Sventare Sanzioni Privacy su Dati PEP e Accountability:** avviare una revisione dei log di accesso ai dati dei clienti, soprattutto se si è in presenza potenziale di **persone politicamente esposte**. Il Board deve assicurarsi che vengano implementati **alert automatici** per interrogazioni anomale e piani di incident response che garantiscano la notifica al Garante entro le prime **24 ore**.
2. **Neutralizzare i Rischi Antitrust sulle Reti di Vendita:** alla luce del caso Morellato, effettuare una revisione urgente dei contratti di distribuzione, al fine di verificare e eventualmente rimuovere clausole che impongono sconti massimi o vietano la vendita tramite alcuni canali (es.: marketplace terzi), onde evitare sanzioni milionarie e danni reputazionali.
3. **Blindare la Supply Chain dalle Frodi IVA e "Colpa di Organizzazione":** alla luce delle contestazioni mosse dalla Procura nel caso Ceva, risulta fondamentale condurre approfondimenti specifici per verificare anche l'effettivo versamento dell'IVA da parte dei fornitori relativo alle specifiche commesse aziendali.
4. **Adeguare l'AI alla Trasparenza e al Watermarking:** in conformità al Codice di Buone Pratiche del 5 marzo, il Board deve incaricare le funzioni IT e Legal di verificare che ogni output di IA generativa destinato al pubblico (testi, audio, video) integri marcature leggibili da macchina entro il **2 novembre 2026**.
5. **Governare l'Obbligo di AI Literacy:** approvare immediatamente un programma di alfabetizzazione per tutto il personale che interagisce con sistemi IA. L'obbligo è sanzionabile dall'**agosto 2025** e costituisce un presidio essenziale contro la "colpa organizzativa" ex 231 per infortuni o decisioni automatizzate illecite.
6. **Bonificare il Marketing ESG dal Greenwashing:** avviare una gap analysis su tutti i claim ambientali ("eco", "green") presenti su packaging e siti web. Entro settembre 2026 ogni affermazione di sostenibilità deve essere supportata da un **fascicolo tecnico-scientifico** accessibile al consumatore tramite QR Code.
7. **Validare la Compliance delle Interfacce Utente (UX/UI):** alla luce della sanzione a Trustpilot, revisionare il design di siti e app per eliminare eventuali **dark patterns**. Verificare che le modalità di pubblicazione di recensioni e abbonamenti non siano manipolative o ingannevoli.

**Contattateci per ulteriori approfondimenti e per un assessment preliminare!**

### Studio Bielle Consulting Srl

 Via Thaon di Revel, 21 - 20159 Milano

 [info@bielleconsulting.com](mailto:info@bielleconsulting.com)

 +39 3481505622 - +39 3460875317