Bielle Consulting - Governance, Risk & Compliance Newsletter

N.3 Marzo 2026

I. Executive Summary **3**
II. IL FATTO DEL MESE: Il Nuovo Regolamento AGCM sul Rating di Legalità **4**
III. Agenda Authority & Governance: Focus su Privacy, Cyber e Antiriciclaggio **5**
IV. Focus ESG e Intelligenza Artificiale **6**
V. Giurisprudenza e Sicurezza: L'Estensione della Responsabilità dalla Fabbrica ai Clienti **7**
VI. Azioni Prioritarie Consigliate per il Board **9**

I. Executive Summary

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

1. **L'Aggressività e il Coordinamento delle Authorities:** L'**AGCM** ha pubblicato il nuovo regolamento sul Rating di Legalità: da metà marzo, il **mero esercizio dell'azione penale** bloccherà i finanziamenti e gli appalti. L'**ACN** ha blindato le notifiche degli incidenti informatici (NIS2) con tempistiche draconiane, mentre il Garante Privacy continua a sanzionare incessantemente la videosorveglianza illecita con multe fino al **4% del fatturato**.
2. **L'Estensione del Rischio 231 e il Controllo della Supply Chain:** La giurisprudenza di Cassazione (sent. 5357/2026) ha sancito che rimuovere protezioni antinfortunistiche per velocizzare la produzione è un reato compiuto a **vantaggio dell'ente**. Parallelamente, la Procura di Milano ha emesso decreti di Amministrazione Giudiziaria nei confronti di **due grandi piattaforme di food delivery** e ha successivamente esteso l'inchiesta ad alcuni **grandi clienti committenti**, imponendo loro di dimostrare la tenuta dei propri Modelli 231 sulla filiera per evitare l'accusa di "agevolazione colposa".
3. **ESG:** La **Direttiva Omnibus 1** ha sollevato molte PMI dagli obblighi CSRD innalzando le soglie (1.000 dipendenti, 450 mln €). Tuttavia, le grandi imprese soggette alla CSRD esigeranno comunque questi dati a cascata dalla loro catena di fornitura; è quindi vitale l'adozione del nuovo standard volontario **EFRAG VSME**.
4. Infine, l'uso dell'**Intelligenza Artificiale Generativa** impone un aggiornamento immediato dei controlli interni secondo il nuovo framework **COSO** rilasciato a febbraio.

II. IL FATTO DEL MESE: Il Nuovo Regolamento AGCM sul Rating di Legalità

Il provvedimento di maggiore impatto strategico-finanziario del mese è la riscrittura strutturale del **Rating di Legalità** da parte dell'AGCM (Delibera 31812 del 27/01/2026 pubblicata in G.U. il 10 febbraio 2026), in vigore dal **16 marzo 2026**. Il Rating non è solo reputazione, ma un asset finanziario per il credito e gli appalti.

L'inasprimento normativo dell'Articolo 5 (Cause ostative) cambia radicalmente la gestione del rischio legale: per i reati 231 e contro la P.A. (es. corruzione, truffa ai danni dello Stato), **la semplice richiesta di rinvio a giudizio (esercizio dell'azione penale)** da parte di un PM sarà sufficiente a bloccare o sospendere il Rating.

Diventano bloccanti a tutti gli effetti anche:

- Le misure prefettizie antimafia.
- I provvedimenti per **abuso di dipendenza economica** e **tutte** le violazioni definitivamente accertate per pratiche commerciali scorrette.
- Le omissioni comunicative: nascondere l'inizio di un procedimento all'AGCM comporta il **divieto di richiedere il rating per 18 mesi**.

III. Agenda Authority & Governance: Focus su Privacy, Cyber e Antiriciclaggio

Le Autorità indipendenti hanno alzato il tiro, sanzionando le prassi disinvolte nella gestione dei dati e dei lavoratori:

1. **Garante Privacy: Videosorveglianza e Rischio 4%:** Con il **Provv. n. 83 del 12 febbraio 2026 (Doc. Web 10225084)**, il Garante ha sanzionato un esercizio commerciale per l'uso di telecamere interne (che riprendevano i dipendenti) senza la preventiva autorizzazione dell'Ispettorato del Lavoro (ITL) e per la telecamera esterna che inquadrava indiscriminatamente il suolo pubblico in assenza di cartellonistica. Le aziende devono ricordare che la violazione dell'Art. 4 dello Statuto dei Lavoratori, in virtù del principio di liceità richiamato dal GDPR, espone a **ordinanze di ingiunzione**, **divieto di trattamento** e **sanzioni fino al 4% del fatturato globale**.
2. **ACN (Cybersicurezza): L'Era della Notifica Obbligatoria:** Con Determinazione Direttoriale 9 febbraio 2026 (GU 17 febbraio), l'ACN ha emanato la **"Tassonomia degli incidenti"** in attuazione della Legge 90/2024 e della Direttiva NIS2. Le aziende ("soggetti importanti" o "essenziali") hanno l'obbligo di notificare allo CSIRT Italia attacchi ransomware o data breach incrociando i nuovi criteri tecnici, entro tempi stringenti (pre-allarme entro 24 ore, notifica dettagliata entro 72 ore e relazione finale entro un mese dalla notifica).
3. **UIF (Antiriciclaggio) e il Rischio dei vIBAN:** Nel Quaderno n. 33 del 17 febbraio 2026, l'UIF ha lanciato l'allarme sull'uso dei **Virtual IBAN**. Strumenti utilissimi per automatizzare le riconciliazioni dei pagamenti, creano però enormi sacche di opacità e disintermediazione, innalzando il rischio di *Money Laundering*. L'UIF richiede a **società**

finanziarie e grandi piattaforme e-commerce di irrobustire i presidi KYC e l**e Segnalazioni di Operazioni Sospette (SOS)**.

4. **AGCM: Maxi-sanzione per i "Dark Patterns":** Con il Provv. PS12853, l'AGCM ha irrogato una sanzione di **9 milioni di euro** al gruppo eDreams per pratiche commerciali ingannevoli basate su interfacce manipolative (design visivo emotivo, finti conti alla rovescia, difficoltà di recesso) volte a forzare gli abbonamenti "Prime".
   L'UX/UI (User Experience/User Interface) Design è ora formalmente sotto il faro legale dell'Antitrust.

IV. Focus ESG e Intelligenza Artificiale

1. **Direttiva Omnibus I e la Pressione sulla Supply Chain:** Il 26 febbraio 2026 è stata pubblicata nella GU dell'Unione Europea la **Direttiva Omnibus I**, che alleggerisce la CSRD e la CSDDD innalzando le soglie di obbligatorietà (**1.000 dipendenti e 450 milioni di fatturato** per la CSRD, **5.000 dipendenti e 1,5 miliardi di fatturato** per la CSDDD). Tuttavia, le PMI non sono affatto "salve": i grandi gruppi scaricheranno sulla catena di fornitura l'onere della raccolta dei dati per rendicontare gli aspetti ambientali e sociali relativi alla loro produzione. Le PMI dovranno adottare tempestivamente lo standard **VSME dell'EFRAG** (per il quale a febbraio sono stati rilasciati nuovi moduli formativi e tool digitali) per non essere espulse dalle vendor list.
2. **Risk Management e AI (Il nuovo Framework COSO GenAI):** Il 23 febbraio 2026 il COSO ha rilasciato la guida *"Achieving Effective Internal Control Over Generative AI"*, che traduce i principi di controllo interno in una mappa "audit-ready" per governare i nuovi rischi tecnologici (come esposizione cyber, "allucinazioni" algoritmiche e deriva dei modelli

manipolati). Il framework individua 8 capacità specifiche dell'AI (es. elaborazione dati, giudizio, interazione) con relativi presidi di sicurezza.
Da considerare anche l'impatto in tema di compliance: d**elegare processi aziendali a un'Intelligenza Artificiale** senza un tracciamento rigoroso espone ad esempio le aziende alla "colpa organizzativa" ex **D.Lgs. 231/01**. Se un a**lgoritmo non supervisionato agevola frodi finanziarie, fughe di dati o decisioni illecite, l'ente ne risponde penalmente** per omessa vigilanza e carenza nei sistemi di controllo.

V. Giurisprudenza e Sicurezza: L'Estensione della Responsabilità dalla Fabbrica ai Clienti

I tribunali italiani non si accontentano della compliance meramente formale ("di carta") richiedendo sempre più interventi sostanziali da parte delle aziende. L'ambito della responsabilità si sta ampliando, estendendosi dalla singola negligenza sul luogo di lavoro fino alla colpa derivante dall'omissione di controllo sui partner commerciali.

Sentenza 1: Il "Vantaggio" 231 nella Ricerca della Massima Produzione (Cass. 5357/10 feb 2026)

Un operaio di un'acciaieria subisce lo schiacciamento del braccio in un macchinario. L'indagine rivela che il capo reparto aveva rimosso le protezioni antinfortunistiche per aggirare frequenti blocchi tecnici e velocizzare gli interventi manuali sul nastro. La **Cassazione** ha confermato la condanna dell'ente ex D.Lgs. 231, stabilendo che la rimozione delle sicurezze, se motivata dall'obiettivo di evitare fermi produttivi, configura automaticamente **l'interesse e il vantaggio economico** per la società (risparmio di tempo e incremento del profitto a discapito della sicurezza).

Sentenza 2: Infortuni, Delega di Firma e Sconti Negati (Cass. 7563/25 feb 2026)

Morte per schiacciamento da trattore agricolo con visibilità ostruita e avvisatore acustico scollegato. La Corte ha stabilito che la mera rappresentanza legale per le questioni fiscali, del lavoro e amminsitrative è solo una "delega di firma", lasciando **tutti i soci solidalmente responsabili** (omicidio colposo) per la totale assenza di segnaletica e viabilità interna. Inoltre, l'azienda si è vista **negare la riduzione della sanzione 231** poiché il risarcimento agli eredi non era stato "integrale" (mancavano le firme di accettazione di due eredi).

IL CASO DEL MESE: Piattaforme di Delivery, Caporalato e l'Estensione delle Indagini ai Grandi Clienti (Committenti)

L'evento giudiziario più significativo arriva dalla Procura di Milano (PM Storari). Dopo aver disposto il controllo giudiziario per **Foodinho Srl (Glovo),** a fine febbraio la Procura ha ordinato un decreto d'urgenza di controllo giudiziario anche per **Deliveroo Italia Srl.**

- **Le Accuse e l'Algoritmo:** Si contesta **il caporalato digitale a**i danni dei rider (circa 20.000 in Italia per Deliveroo, 40.000 per Glovo). Secondo l'accusa, i ciclofattorini percepivano paghe a cottimo sotto **i 4 euro l'ora** per turni massacranti, costantemente controllati, valutati e sanzionati da un algoritmo che fungeva da vero e proprio "caporale" tecnologico limitando la loro autonomia.
- **L'impatto Dirompente per il Business (La Filiera):** L'indagine non si è limitata alle piattaforme. I Carabinieri del Nucleo Tutela Lavoro hanno notificato un **ordine di esibizione documenti a sette grandi multinazionali clienti** della GDO e del food retail: **McDonald's, Burger King, KFC, Poke House, Carrefour, Esselunga e CRAI Secom**.
- **Il Rischio 231 per i Clienti:** Sebbene non ancora formalmente indagati, a questi marchi è stato intimato di consegnare i propri Modelli Organizzativi 231. La Procura vuole verificare se le procedure di *vendor management* di queste aziende committenti siano idonee a prevenire e non avallare lo sfruttamento. In assenza di audit e due diligence adeguati sui propri fornitori, i clienti rischiano un'imputazione per **"agevolazione colposa"** del caporalato operato da Deliveroo. L'outsourcing non scherma più la capogruppo dalle

responsabilità penali.

VI. Azioni Prioritarie Consigliate per il Board

1. **Proteggere il Rating AGCM e l'Accesso al Credito:** richiedere periodicamente i **certificati dei carichi pendenti degli apicali**: è imperativo notificare all'AGCM eventuali rinvii a giudizio prima che scadano i termini legali, al fine di evitare il divieto assoluto di accesso al rating (e ai finanziamenti connessi) per 18 mesi.
2. **Sventare Sanzioni Privacy fino al 4% del Fatturato:** avviare una **mappatura completa delle telecamere aziendali per censire tutti gli impianti di videosorveglianza**. Il Board, tramite il DPO, deve assicurarsi di aver richiesto e ottenuto l'autorizzazione dell'Ispettorato del Lavoro (ITL) per tutte le ottiche che inquadrano aree di lavoro, provvedendo inoltre ad apporre immediatamente i cartelli informativi a norma GDPR. In quest'ottica, **la DPIA (Valutazione d'Impatto sulla Protezione dei Dati) risulta necessaria per i sistemi di videosorveglianza**.
3. **Blindare la Supply Chain dal Caporalato:** alla luce del caso Delivery, occorre condurre una ***due diligence* sugli appaltatori**. **Esigere verifiche periodiche sulla tenuta e sull'efficacia dei Modelli 231 dei partner che offrono servizi e logistica**. È fondamentale **includere e attivare clausole risolutive espresse** in caso di violazione della dignità sul lavoro. Questo serve a proteggere la società committente da eventuali accuse di "agevolazione colposa".
4. **Mitigare le Sanzioni 231 su Sicurezza e Prassi Deviate:** l'OdV, in coordinamento con il RSPP, deve **varare un piano di ispezioni *unannounced* (a sorpresa)** direttamente nei reparti e sulle linee produttive. L'azienda deve **applicare la tolleranza zero**, prevedendo sospensioni e sanzioni disciplinari immediate **per chiunque bypassi le sicurezze dei macchinari utilizzando la giustificazione di dover "velocizzare la produzione"**.
5. **Evitare Maxi-Sanzioni Cyber in ambito NIS2: Aggiornare il piano di Incident Response aziendale**, mappando l'infrastruttura IT sui **nuovi standard normativi della Tassonomia ACN**. Va strutturato un p**rotocollo operativo in grado di qualificare un attacco e notificare l'incidente** grave allo CSIRT Italia tassativamente entro le prime **24 ore.**
6. **Rispondere ai Requisiti ESG:** Procedere con **l'adozione dello standard EFRAG VSME** per iniziare a raccogliere i dati di sostenibilità e **mantenere così la propria posizione competitiva all'interno delle filiere multinazionali**.
7. **Governare l'AI: aggiornare i protocolli del Modello 231 implementando i controlli del framework COSO GenAI**, per **arginare** e mappare i **rischi legali e operativi derivanti dall'uso dell'Intelligenza Artificiale** Generativa nei processi decisionali.

Contattateci per ulteriori approfondimenti e per un assessment preliminare!

Studio Bielle Consulting Srl

📍 Via Thaon di Revel, 21 - 20159 Milano

📪info@bielleconsulting.com

☎️ +39 3481505622 - +39 3460875317