BIELLE CONSULTING

Risk, Sustainability & Compliance

Bielle Consulting - Governance, Risk & Compliance Newsletter

N.1 - Novembre 2025

I. Executive Summary

Il mese di ottobre 2025 ha ridefinito tre aree chiave della responsabilità d'impresa, spostando il focus dalla compliance formale alla gestione sostanziale del rischio. Per il management e i Consigli di Amministrazione, l'agenda delle priorità è ora dominata da tre cambiamenti di paradigma.

1. **La Sicurezza sul Lavoro necessita sempre più di un sistema di gestione.** L'azione combinata del D.L. 159/2025 e delle recenti sentenze della Cassazione ha creato una "tenaglia": da un lato, il nuovo Decreto impone controlli amministrativi più stringenti, come il tracciamento dei *near miss* (mancati infortuni) e la patente a crediti. Dall'altro, la Suprema Corte, con la sentenza 325025/2025 **chiarisce** la responsabilità penale personale (il Preposto deve fare in modo di "impedire" l'infortunio, non solo "vigilare") e, con la sentenza 27321/2025 **sancisce** quella solidale (il Committente ha un "debito di sicurezza" per il PSC - Piano Sicurezza e Coordinamento - inadeguato). L'implicazione è che deve essere valutata l'adeguatezza delle deleghe di funzione e dei sistemi di gestione in materia di Salute e Sicurezza.
2. **L'Applicazione del Rischio 231 (Fisco e IA).** Il perimetro 231 è al centro dell'attenzione su due fronti critici. Il primo, e più clamoroso, è l'indagine che ha portato al **sequestro di 1,29 miliardi di euro nei confronti della holding di Campari, Lagfin**. L'accusa, che include la "dichiarazione fraudolenta mediante altri artifici" e la "responsabilità amministrativa delle persone giuridiche", è legata a una presunta evasione sulla "exit tax". **Questo sequestro record conferma l'elevata attenzione delle Procure nell'applicare la 231 a complesse operazioni di pianificazione fiscale**, consolidando il concetto che il rischio fiscale rientra nel più ampio rischio penale-societario con impatti patrimoniali immediati.
   Il secondo fronte è il futuro: con l'entrata in vigore della Legge 132/2025, **due reati presupposto del D.Lgs. 231/01, Aggiotaggio (Art. 2637 c.c.) rientrante nei Reati Societari e Manipolazione del mercato (Art. 185 TUF) rientrante nei reati di Market Abuse, vengono aggiornati per includere l'utilizzo dell'IA** si estende ai reati finanziari commessi *tramite* IA.
   Questo è solo l'inizio. Il Decreto prevede anche la delega al Governo per disciplinare l'impiego illecito dell'IA e definire, tra l'altro, "criteri di **imputazione della responsabilità** penale delle persone fisiche e **amministrativa degli Enti** " e "nuove fattispecie di reato": significa che ogni Modello 231 dovrà essere oggetto di valutazione e, con ogni probabilità, di revisione prevedendo protocolli specifici per l'utilizzo dell'IA.
3. **La "Tolleranza Zero" delle Authority.** Il Garante Privacy ha ripreso un'intensa attività ispettiva. La sanzione all'Ospedale Careggi per la gestione del dossier sanitario (basata su consenso errato e sistemi IT non conformi *by design*) e la maxi-sanzione da 420.000 euro a un'azienda per aver usato chat WhatsApp

private a fini disciplinari ne sono una dimostrazione. Questo approccio è speculare a quello adottato dall'UIF (Unità di Informazione Finanziaria), i cui ultimi dati mostrano un'attività di intelligence e ispettiva (migliaia di segnalazioni *cross-border*) che rende i controlli interni Antiriciclaggio (AML) un presidio non negoziabile.

II. IL FATTO DEL MESE: Rivoluzione sulla Sicurezza sul Lavoro (D.L. 159/2025) e Giurisprudenza

Il Decreto Legge 31 ottobre 2025, n. 159 è una risposta diretta all'emergenza infortuni, ma il suo impatto va ben oltre i cantieri, ridefinendo gli obblighi di vigilanza e formazione per tutte le imprese.

Le Misure del D.L. 159/2025

Il nuovo decreto introduce un pacchetto di misure volte a rafforzare la prevenzione e, soprattutto, l'accertamento delle responsabilità.

- **Tracciamento dei "Near Miss" (Mancati Infortuni):** Viene introdotto l'obbligo per le imprese (con più di 15 dipendenti) di adottare linee guida per l'identificazione, il tracciamento e l'analisi dei mancati infortuni. Questo non è un esercizio statistico, ma la creazione di una prova precostituita. Saranno definite dal Ministero del Lavoro le modalità attraverso cui le imprese dovranno comunicare i dati relativi ai *near miss* e le azioni correttive implementate/da implementare a seguito degli

stessi. Questo obbligo trasforma il Documento di Valutazione dei Rischi (DVR) da adempimento statico a sistema di *risk management dinamico* e *data-driven*.

- **Formazione RLS e Soggetti Accreditati:** Viene esteso l'obbligo di aggiornamento periodico per i Rappresentanti dei Lavoratori per la Sicurezza (RLS) anche alle imprese con meno di 15 dipendenti. In parallelo, si punta a un innalzamento qualitativo degli enti accreditati per la formazione. Questo elimina l'ultima "zona grigia" per le PMI, aumentando la pressione sulla formazione effettiva.
- **Controlli nei Cantieri:** Vengono introdotte misure specifiche per il settore edile, come il "badge digitale di cantiere" per il tracciamento dei lavoratori e sanzioni più severe per la "patente a crediti".
- **Potenziamento della Vigilanza:** Il decreto autorizza il potenziamento dell'organico dell'Ispettorato Nazionale del Lavoro (INL) e del Comando Carabinieri per la tutela del lavoro. Questo segnala un chiaro passaggio da un approccio preventivo a uno repressivo.

Le Sentenze della Cassazione

La giurisprudenza della Suprema Corte ad ottobre ha **chiarito** due pilastri della responsabilità penale.

- **Cass. Pen. 32520/25**: Il Preposto deve "Impedire", non solo "Vigilare"
  La Corte di Cassazione, con la sentenza del 1° ottobre 2025, ha chiarito che la posizione di garanzia del preposto (ai sensi dell'Art. 19 del D.Lgs. 81/08) non si esaurisce in una vigilanza passiva, ma richiede un intervento attivo per "impedire l'infortunio". La sentenza ha ritenuto responsabile un preposto per non aver interrotto una procedura di lavoro palesemente pericolosa.
  Questa sentenza rende obsolete la maggior parte delle deleghe di funzione. Se un CEO (Datore di Lavoro) delega un Preposto, ma la Cassazione afferma che il Preposto è responsabile solo se ha il potere di "impedire", sorge un problema critico. Se il Preposto non ha l'autonomia di spesa o il potere gerarchico di fermare i lavori, non può "impedire". Di conseguenza, la delega è inefficace e la responsabilità penale risale automaticamente al Datore di Lavoro/CEO. È necessaria una revisione immediata di tutte le deleghe per garantire che i poteri delegati siano effettivi e reali, non mere nomine formali.
- **Cass. Civ. 27321/25**: Il Committente e il "Debito di Sicurezza"
  Con un'altra pronuncia chiave, la Cassazione Civile ha sancito la responsabilità solidale del committente per un infortunio mortale causato da un Piano di Sicurezza e Coordinamento (PSC) palesemente inadeguato. La Corte ha chiarito che il committente ha un "debito di sicurezza" e una posizione di garanzia ex lege. Ciò significa che il committente non può esimersi dalla responsabilità semplicemente appaltando i lavori, anche se il PSC è redatto da professionisti esterni. La due diligence sulla sicurezza dell'appaltatore non è più un'opzione, ma

un obbligo di garanzia. La scelta di un contraente basata su un'offerta economicamente vantaggiosa che palesemente sottostima i costi della sicurezza (e presenta un PSC debole) espone il management del committente a corresponsabilità civile e penale.

L'Impatto Combinato delle Novità in materia di Sicurezza (Ottobre 2025)

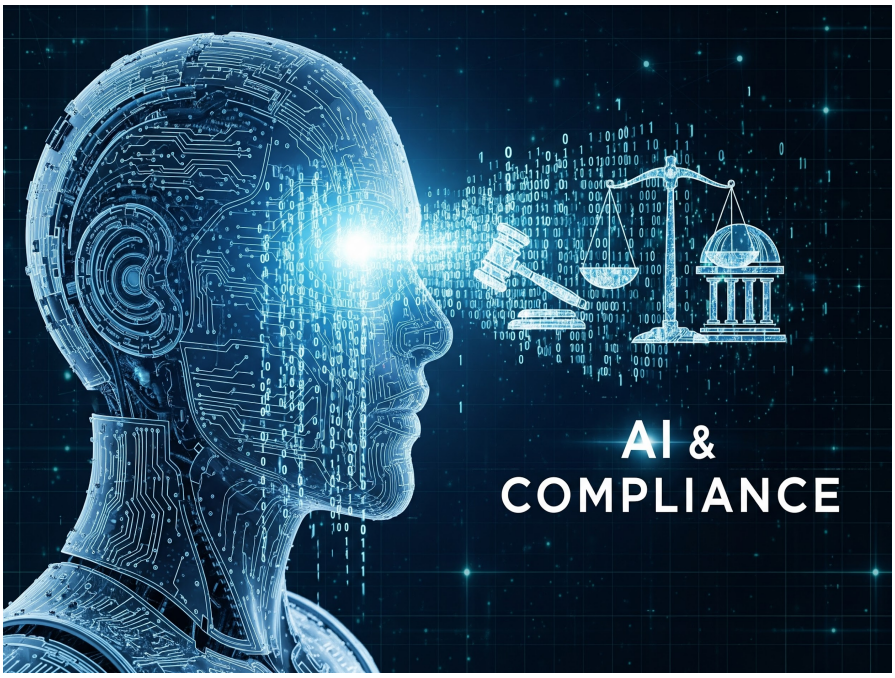
La seguente tabella riassume l'impatto strategico delle novità legislative e giurisprudenziali per il management.

Fonte	Soggetto Impattato	Il Nuovo Obbligo / Principio	Implicazione Strategica per l'Azienda
D.L. 159/2025	Datore di Lavoro / Management	Obbligo di tracciamento e analisi dei "Near Miss" (mancati infortuni).	Il registro Near Miss è una prova per il PM. Trasforma il DVR da documento statico a sistema di *risk management dinamico*. La mancata azione su un near miss registrato equivale a colpa grave in caso di futuro infortunio.
Cass. Pen. 32520/25	Preposto / Datore di Lavoro	Il Preposto deve *attivamente* "impedire" l'infortunio, non solo "vigilare".	La responsabilità penale risale al Datore di Lavoro se il Preposto non ha poteri *effettivi* (di spesa, di fermo lavori). La maggior parte delle deleghe di funzione è da riscrivere.
Cass. Civ. 27321/25	Committente (Azienda)	Il Committente ha un "debito di sicurezza" e responsabilità solidale per PSC inadeguato.	La *due diligence* sulla sicurezza dell'appaltatore diventa un obbligo di garanzia. Le gare al ribasso che trascurano la sicurezza espongono il management del committente a responsabilità diretta.
D.L. 159/2025	Datore di Lavoro (Tutte le imprese)	Obbligo di aggiornamento periodico RLS esteso alle	Eliminazione delle "zone grigie" per le PMI. Aumento dei costi di compliance e formazione, ma anche della consapevolezza dei

Fonte	Soggetto Impattato	Il Nuovo Obbligo / Principio	Implicazione Strategica per l'Azienda
		imprese \<15 dipendenti.	lavoratori, con potenziale aumento delle segnalazioni.

III. Perimetro 231: Il Rischio Fiscale, la Frontiera AI e il Rischio Ambientale

Il D.Lgs. 231/01 è un organismo vivente. Ottobre 2025 ha visto tre espansioni critiche: una verso il rischio fiscale (Caso Campari), una verso il futuro (Intelligenza Artificiale) e una che consolida il passato (Ambiente).



Caso Campari: Il Rischio Fiscale 231 e l'Ombra della "Exit Tax"

Il 31 ottobre, la Guardia di Finanza di Milano, su ordine della Procura di Monza, ha eseguito un maxi-sequestro preventivo da 1,29 miliardi di euro. L'obiettivo non è stato il Gruppo Campari, ma la sua holding di controllo lussemburghese, Lagfin.

Le accuse sono "dichiarazione fraudolenta mediante altri artifici" e, punto cruciale per gli amministratori, "responsabilità amministrativa delle persone giuridiche" (D.Lgs. 231/01).

L'indagine ruota attorno a una complessa operazione di fusione transfrontaliera del 2018, che secondo l'accusa avrebbe permesso di eludere la "exit tax" italiana su plusvalenze non dichiarate per oltre 5,3 miliardi di euro.

Questo caso segna un'escalation nell'applicazione della 231. Sebbene i reati tributari siano già inclusi nel novero dei reati presupposto, la Procura ha utilizzato la normativa per eseguire un sequestro di entità straordinaria. Per i CdA, questo significa che le strategie di pianificazione fiscale internazionale, se ritenute "artifici" elusivi, rientrano nei reati presupposto del DLgs 231/01 con il rischio di possibili sequestri di ingente valore e la responsabilità diretta dell'ente.

Intelligenza Artificiale e D.Lgs. 231/01 (Legge n. 132/2025)

La Legge n. 132/2025, in vigore dal 10 ottobre 2025, non si limita a recepire l'AI Act europeo, ma lo integra con severe norme penali e 231.

- **L'Aggravante Immediata:** L'uso dell'IA è ora un'aggravante specifica per reati 231 già esistenti, come l'Aggiotaggio (Art. 2637 c.c., previsto dall'Art. 25-ter 231) e la Manipolazione del Mercato (Art. 185 TUF, previsto dall'Art. 25-sexies 231).8
- **Il Rischio Futuro (La Delega):** Il punto cruciale è la delega al Governo (Art. 24 L. 132/25) per definire, entro 12 mesi, "nuove fattispecie di reato per omessa adozione di misure di sicurezza" e "criteri di imputazione della responsabilità" amministrativa degli Enti. Questa delega segna una rivoluzione. La legge si sta muovendo per trattare l'IA non come un semplice *strumento*, ma quasi come un "soggetto qualificato" interno. L'introduzione di un reato per "omessa adozione di misure di sicurezza" sull'IA potrebbe equiparare, di fatto, l'omesso controllo su un algoritmo all'omesso controllo su un dipendente. L'implicazione per il Modello 231 sarebbe rilevante; anche l'Organismo di Vigilanza (OdV) potrebbe dover *auditare* gli algoritmi, non solo le procedure umane, richiedendo valutazioni d'impatto specifiche per il rischio-reato.

Reati Ambientali e "Risparmio di Spesa" (L. 147/2025 e Cassazione)

La nuova Legge n. 147/2025 ha aggiornato l'elenco dei reati presupposto all'Art. 25-undecies (Reati Ambientali). In parallelo, una sentenza della Cassazione (Sent. 27669/25) ha stabilito che il "vantaggio" 231 per reati ambientali (es. gestione di discarica non autorizzata) non richiede un profitto diretto, ma si configura nel mero "risparmio di spesa" (es. costi di smaltimento evitati).

Il Modello 231 non può più limitarsi a presidiare la logistica (come la tracciabilità dei rifiuti), ma deve presidiare le *scelte di budget* e di *commessa* per assicurare che la compliance ambientale non venga compromessa da logiche di risparmio.

IV. Sostenibilità (ESG): Tra Semplificazione Tattica e Rinvio Strategico

Il reporting ESG sta affrontando il suo primo "reality check". Le notizie di ottobre mostrano un'apparente contraddizione: da un lato, l'Europa rallenta l'implementazione; dall'altro, i controllori alzano le aspettative sulla qualità.

Scenario UE: Il Rinvio degli Standard (CSRD Livello 2)

La Commissione Europea ha informato le autorità di vigilanza (EBA, EIOPA, ESMA) che posticiperà al 1° ottobre 2027 l'adozione di una serie di atti di Livello 2, inclusi gli standard ESRS per le imprese di paesi terzi (originariamente previsti per il 2026). La motivazione ufficiale è la riduzione degli oneri amministrativi e il miglioramento della competitività.

Primi Feedback sul Reporting (Fact-Finding ESMA del 14 Ottobre)

L'ESMA ha pubblicato un'analisi sulle prime pratiche di reporting 2024 (ESRS Set 1). I risultati sono preoccupanti:

- Solo il 60% delle aziende ha raggiunto l'obiettivo generale di trasparenza. La Valutazione di Doppia Materialità (DMA) è spesso "boilerplate", cioè formale e non sostanziale.
- I temi più trattati sono E1 (Clima), S1 (Forza Lavoro Propria) e G1 (Condotta Aziendale).22

Ai fini del DMA, l'ESMA richiede quindi di evitare descrizioni formali, e fornire spiegazioni sulla metodologia utilizzata, sulla soglia di rilevanza e sugli stakeholder coinvolti nelle valutazioni.

V. L'Agenda delle Authority: Privacy, Cybersecurity e AML

Garante Privacy: Interventi su dossier sanitario e chat private

1. Il Caso del Dossier Sanitario (Ospedale Careggi)

Con un provvedimento di agosto 2025, il Garante ha sanzionato l'Azienda Ospedaliero-Universitaria Careggi (80.000 euro) per la gestione illecita del dossier sanitario. Le violazioni non erano formali, ma sistemiche:

- **Mancanza di Consenso Specifico:** L'ospedale si basava su un "consenso orale generico per fini di cura", mentre il dossier sanitario, essendo un trattamento *ulteriore* rispetto alla singola prestazione, richiede un consenso specifico che non veniva raccolto.
- **Violazione della Privacy by Design (Art. 25):** Il sistema IT non permetteva all'interessato di oscurare *parzialmente* i dati (es. un singolo referto), ma consentiva solo l'oscuramento dell'intera cartella. Una progettazione "tutto o niente" che viola i principi di minimizzazione e controllo dell'utente.

La "sanzione" più rilevante non è quella di 80.000 euro, ma le misure correttive imposte, che obbligano l'azienda a una revisione totale delle procedure e degli applicativi. Questo intervento, unito ad altre sanzioni simili comminate ad una casa di cura privata, segnala un'azione ispettiva significativa sul settore.

2. L'Uso Illecito di sistemi di messaggistica e social media

Il Garante ha tracciato una linea netta sulla gestione "informale" dei dipendenti e dei clienti tramite app private di messaggistica, consolidando i limiti all'uso di tali dati.

- **L'inserimento nel gruppo (Marketing):** Un provvedimento (avvio di procedimento sanzionatorio) contro la società "Zena s.r.l.s." è nato dal reclamo di un cliente inserito in un gruppo WhatsApp a fini promozionali. Il Garante ha contestato la mancanza di una base giuridica valida, chiarendo che:
    - Il dato non poteva essere acquisito da un acquisto su piattaforme terze (es. Amazon) per finalità di marketing.

    - La creazione della chat ha comportato la **comunicazione dei numeri di telefono di tutti i partecipanti agli altri membri**, un trattamento invasivo che richiede un consenso specifico e informato.
    - È stato respinto il concetto di *opt-out* (il cliente che esce dal gruppo), in quanto l'informativa e il consenso devono essere **preventivi e inequivocabili**.
- **L'uso a fini disciplinari (Privacy sul lavoro):** Ancora più grave, una sanzione da 420.000 euro è stata comminata a una società che ha utilizzato "stralci virgolettati" di conversazioni private (WhatsApp e Messenger), inoltrate da terzi, per motivare contestazioni disciplinari e il licenziamento di una dipendente. Il Garante ha ravvisato una doppia violazione:
    - **GDPR (Mancanza di base giuridica e minimizzazione):** L'azienda, pur avendo ricevuto passivamente i dati da terzi, aveva l'obbligo di **astenersi dall'utilizzarli** poiché riguardavano comunicazioni private. È stata violata la presunzione di riservatezza e i principi di liceità e limitazione della finalità.
    - **Art. 8 Statuto dei Lavoratori:** L'uso dei contenuti delle chat private ha violato il divieto di indagini sulle opinioni del lavoratore, consolidando il principio che i dati estratti da canali privati (anche se involontariamente resi noti) non possono essere trasformati in prova disciplinare.

Cybersecurity (ACN) e NIS 2

Il contesto della minaccia è in crescita: l'Agenzia per la Cybersicurezza Nazionale (ACN) riporta un aumento del 40% degli attacchi cyber al settore sanitario nel 2025. In risposta, il 27 ottobre l'ACN ha pubblicato le Linee Guida sull'applicazione dei "criteri di premialità".

Questo crea un nuovo paradigma. Direttive come la NIS 2 25 impongono un livello *minimo* di sicurezza, che rappresenta un centro di costo. Le nuove Linee Guida ACN, invece, introducono un *premio* (punteggio extra) negli appalti pubblici per beni e servizi ICT per chi adotta misure di sicurezza *superiori* allo standard. Questo trasforma la cybersecurity da un costo obbligatorio a un *generatore di ricavi* e un vantaggio competitivo per vincere le gare.

Antiriciclaggio (UIF): L'Analisi dei Dati

Il 28 ottobre, l'UIF di Banca d'Italia ha pubblicato il Quaderno sull'antiriciclaggio relativo al I semestre 2025. I dati mostrano un'attività di intelligence intensa: 197 richieste dall'Autorità Giudiziaria, accertamenti ispettivi, 7.424 segnalazioni inviate alle FIU (Financial Intelligence Units) estere e, soprattutto, 25.547 segnalazioni ricevute dalle FIU.

Questi numeri (soprattutto le migliaia di segnalazioni *cross-border*) dimostrano che la vigilanza non è più nazionale, ma globale e *data-driven*. Il rischio per un'azienda non è più solo la "non compliance" (es. mancata Segnalazione di Operazione Sospetta), ma la "contiguità": essere la controparte commerciale di un soggetto segnalato in un'altra nazione. È da questo incrocio dati che nascono le ispezioni. L'adeguata verifica delle controparti (KYC/KYP) non è un formalismo, ma l'unica difesa contro l'essere trascinati in indagini di cui non si è diretti destinatari.

VI. Risk Management e Controlli Interni: Il ritiro del Corporate Governance Framework

A luglio 2025 il COSO (Committee of Sponsoring Organizations of the Treadway Commission) ha *ritirato* la bozza del suo nuovo framework di Corporate Governance (sviluppato con NACD - *National Association of Corporate Directors*), la cui pubblicazione era attesa per l'autunno 2025, per valutare i numerosi commenti ricevuti. Il framework originale, pubblicato a fine maggio 2025, mirava a fornire un quadro di riferimento per la governance aziendale e aveva avuto un periodo di consultazione pubblica esteso fino al 12 settembre 2025.

VII. Azioni Prioritarie Consigliate

Le evoluzioni di ottobre 2025 – dal D.L. 159/2025 alla nuova Legge sull'IA e gli esiti del caso Campari – non rappresentano semplici aggiornamenti normativi, ma delineano un mutamento del paradigma di governance. La responsabilità manageriale è in espansione, la funzione di vigilanza richiede proattività e i dati (come *near miss*, algoritmi e segnalazioni AML) sono diventati centrali nella gestione del rischio.

Per affrontare efficacemente questo scenario, Bielle Consulting raccomanda le seguenti verifiche e interventi immediati:

1. **Verifica di Validità delle Deleghe di Funzione (D.Lgs. 81/08):**
    - **Perché:** La Sentenza Cass. Pen. 32520/25 impone una riflessione critica: le deleghe di sicurezza conferite ai Dirigenti e Preposti sono adeguate?
    - **Azione suggerita: "Delega Check-Up"** per assicurarci che tali poteri non si trasformino in una potenziale risalita di responsabilità per il Datore di Lavoro e per il Consiglio di Amministrazione.
2. **Aggiornamento Strategico del Modello 231 (Integrazione Rischio AI, Fiscale, Ambientale):**
    - **Perché:** La Legge 132/25, l'indagine su Lagfin e la giurisprudenza sul "risparmio di spesa" rendono i Modelli 231 potenzialmente non adeguati/aggiornati.
    - **Azione suggerita:** sviluppare protocolli ad hoc per la governance dei futuri rischio-reato derivante dall'utilizzo di IA, per la corretta gestione delle operazioni fiscali straordinarie e per l'integrazione nei protocolli ambientali dell'analisi sui "costi evitati".
3. **Audit di Efficacia Privacy (GDPR "Health Check"):**
    - **Perché:** L'avviso del Garante Privacy relativo alle "verifiche sistematiche" richiede un'azione preventiva.
    - **Azione suggerita:** verifica dell'efficacia operativa delle procedure (come DPIA, Registro Trattamenti, ecc.), al fine sistemare eventuali non conformità al GDPR.

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