



luglio 2024

# flash infopaper

*Compliance & Risk Management*

compliance normativa | anticorruzione

privacy | giurisprudenza

### ► Compliance normativa

- Il Parlamento ha approvato in via definitiva il DDL Cybersicurezza
- Pubblicato in GUUE il nuovo Pacchetto AML

### ► Anticorruzione

- Appalti: irregolarità negli affidamenti diretti ed elusione del principio di rotazione
- La sottoposizione a misura cautelare interdittiva dell'Amministratore di fatto impone una valutazione da parte della PA circa l'affidabilità dell'operatore economico senza però alcun automatismo
- ANAC: non è sufficiente una contestazione dall'Agenzia delle Entrate per essere esclusi da una gara d'appalto

### ► Privacy

- EDPS adotta i primi orientamenti sull'utilizzo di sistemi di IA generativa
- Garante Privacy: indicazioni su web scraping e IA generativa

### ► Giurisprudenza

- Per le Sezioni Unite non vi è alcuna continuità normativa tra il reato di millantato credito e quello di traffico di influenze illecite (Cassazione penale, Sez. Un., 15 maggio 2024, n. 19357)
- L'adozione di misure per la protezione dai rischi interferenziali e la responsabilità del committente e appaltatore (Cassazione Penale, Sez. IV, 6 maggio 2024, n. 17683)
- Amministrazione Giudiziaria: altra nota casa di moda colpita dalla misura di prevenzione (Tribunale di Milano, sez. Misure di Prevenzione, decreto n. 12 del 6 giugno 2024)





## Il Parlamento ha approvato in via definitiva il DDL Cybersicurezza

La Camera dei Deputati ed il Senato della Repubblica hanno approvato, rispettivamente in data 15 maggio e 19 giugno 2024, il disegno di legge recante “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e reati informatici”, il cui testo è stato pubblicato sulla Gazzetta Ufficiale in data 2 luglio 2024 (Legge 28 giugno 2024, n. 90, in vigore dal 17 luglio 2024).

La novella legislativa ha apportato molte modifiche al codice penale in materia di prevenzione e contrasto dei reati informatici, con conseguenti aumenti di pene e l'introduzione di una nuova fattispecie del delitto di estorsione mediante reati informatici (ex art. 629, comma 3, c.p.). Inoltre, la legge è intervenuta sul catalogo dei reati presupposto della responsabilità amministrativa degli enti (ex art. 24-bis, D.Lgs. n. 231/2001) e sulla relativa disciplina sanzionatoria con aumenti alle sanzioni tra duecento e settecento quote previste per i reati informatici e l'introduzione della sanzione da trecento a ottocento quote per il reato di estorsione informatica aggiungendo per quest'ultima anche l'applicazione delle sanzioni interdittive per una durata non inferiore a due anni.

La nuova disposizione normativa prevede l'obbligo di segnalazione di alcuni tipi di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico principalmente alle pubbliche amministrazioni: i soggetti interessati devono provvedere alla segnalazione degli incidenti/eventi di natura accidentale o intenzionale che determinano il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici, senza ritardo e comunque al massimo entro ventiquattro ore.

Inoltre, i destinatari della nuova norma, in caso di segnalazioni dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultano potenzialmente esposti, dovranno provvedere tempestivamente all'adozione degli interventi risolutivi indicati dalla stessa Agenzia.

Per quanto riguarda gli obblighi organizzativi, le pubbliche amministrazioni devono dotarsi di una struttura preposta alle attività di cybersicurezza e devono individuare il referente per la cybersicurezza, quale unico punto di contatto delle amministrazioni coinvolte con l'Agenzia per la cybersicurezza nazionale. Alle strutture preposte è assegnata la funzione di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica in loro uso rispettino le linee guida sulla crittografia adottate dall'Agenzia per la Cybersicurezza Nazionale e dall'Autorità Garante per la Protezione dei Dati Personali e non contengano vulnerabilità note. Per quanto riguarda la crittografia, la legge ne valorizza l'utilizzo quale strumento di difesa cibernetica e istituisce il Centro nazionale di crittografia presso l'Agenzia per la cybersicurezza nazionale.

Con riferimento all'Agenzia Cybersicurezza Nazionale (ACN), la legge disciplina termini e modalità per l'adozione del regolamento che stabilisce modi e tempi per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia. Inoltre, è stabilito uno specifico divieto di “pantouflage”: per due anni, i dipendenti ACN che abbiano partecipato, nell'interesse e a spese dell'ACN, a specifici percorsi formativi di specializzazione, non potranno assumere incarichi presso soggetti privati finalizzati allo svolgimento di mansioni in materia di cybersicurezza.

Da ultimo, con riferimento alle gare di appalto per l'acquisto di specifiche categorie merceologiche di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, saranno individuati da un DPCM, da emanarsi entro 120 giorni dalla pubblicazione del DDL, gli elementi essenziali di cybersicurezza. Inoltre, nell'ambito delle fasi di valutazione delle offerte di tali procedimenti di gara, sono previsti una serie di obblighi e facoltà (ad esempio non aggiudicare) in capo alle stazioni appaltanti, incluse le centrali di committenza, in relazione alla presenza degli elementi essenziali di cybersicurezza.

**Fonte: DDL Cybersicurezza, 19 giugno 2024**



## Pubblicato in GUUE il nuovo Pacchetto AML

In data 19 giugno 2024, è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il c.d. Pacchetto AML, approvato dal Consiglio Europeo in via definitiva lo scorso 30 maggio. Trattasi di un insieme di norme volto al contrasto del riciclaggio e del finanziamento del terrorismo, con la finalità da rafforzare la tutela dei cittadini e del sistema finanziario dell'UE.

In particolare, il Pacchetto AML risulta costituito da:

- Regolamento (UE) 2024/1624 c.d. Regolamento Antiriciclaggio “single rulebook”;
- VI Direttiva Antiriciclaggio;
- Regolamento (UE) 2024/1620, che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo - c.d. AMLA;
- Regolamento (UE) 2024/1623 circa i requisiti per il rischio di credito, il rischio di aggiustamento della valutazione del credito, il rischio operativo, il rischio di mercato e l'output floor.

Con riferimento al Regolamento Antiriciclaggio, vengono riunite tutte le norme relative al settore privato dei singoli Stati. In particolare, vengono introdotte delle misure di due diligence rafforzate e obblighi di controlli sull'identità dei clienti, con i relativi obblighi di segnalazione.

Inoltre, tali obblighi più stringenti vengono estesi anche a società di calcio professionistiche di alto livello, agenti di calcio, commercianti di beni di lusso e operatori con criptovalute. Da ultimo, si segnala l'imposizione del limite di 10.000 euro per i pagamenti in contanti.

La direttiva definisce modalità di collaborazione tra le unità di informazione finanziaria (FIU) e le autorità di vigilanza. Inoltre, si prevede che gli Stati membri implementino dei punti di accesso unico in merito alle informazioni provenienti da registri centralizzati dei conti bancari, a cui le sole FIU potranno accedere.

Da ultimo, il c.d. Pacchetto AML ha istituito l'AMLA, Autorità con compiti di supervisione diretta e indiretta sui soggetti obbligati. Si attribuisce all'AMLA, ad esempio, il compito di individuare e valutare i rischi e le minacce di riciclaggio e finanziamento del terrorismo in tutto il mercato interno, nonché i rischi e le minacce provenienti dall'esterno dell'Unione che incidono o sono suscettibili di incidere sul mercato interno. Inoltre, si occuperà di sostenere e coordinare lo scambio di informazioni tra le FIU e tra le FIU e altre autorità competenti. Si sottolinea, infine, come all'Autorità venga attribuito il compito di riferire alla Commissione i casi in cui rilevi che uno Stato membro abbia recepito la direttiva in modo errato e incompleto.

Il Regolamento dovrà essere applicato dopo 3 anni dalla sua entrata in vigore, mentre la Direttiva dovrà essere recepita dagli Stati membri entro 2 anni per talune parti, entro 3 per altre.

### Fonti:

- **Regolamento (UE) 2024/1624**
  - **VI Direttiva Antiriciclaggio**
  - **Regolamento (UE) 2024/1620**
  - **Regolamento (UE) 2024/1623**
-



## Appalti: irregolarità negli affidamenti diretti ed elusione del principio di rotazione

ANAC, come si legge dall'Atto del Presidente approvato dal Consiglio del 16 aprile 2024, rileva diverse irregolarità commesse dalla Stazione Appaltante "Biblioteca di Genova" nella gestione degli affidamenti diretti per i servizi di manutenzione. Nello specifico, sembrerebbe che la Stazione Appaltante abbia affidato, mediante affidamento diretto, diversi lavori di manutenzione allo stesso appaltatore nel triennio 2019-2021 violando la normativa al tempo vigente. La vigilanza sull'Appaltante è stata avviata a seguito di una segnalazione che comunicava come la stessa Società risultasse affidataria, senza interruzione, almeno dal 2019, di contratti annuali dei servizi di manutenzione impiantistica presso la Stazione Appaltante "Biblioteca di Genova". Nello specifico, le condotte che risultano violate a seguito della vigilanza risultano le seguenti:

- manipolazione del principio di economicità e del divieto di frazionamento artificioso degli affidamenti a seguito di una mancata programmazione dei servizi di manutenzione che ha avuto come conseguenza un'«estrema parcellizzazione degli appalti di manutenzione» con l'obiettivo di restare sotto la soglia dei 40.000 €;
- elusione del principio di rotazione di inviti e affidamenti. La Stazione Appaltante ha difatti affidato alla stessa controparte numerosi incarichi, tutti correlati alla medesima classe merceologica (come dimostrano gli incarichi affidati nello stesso anno per lo svolgimento del servizio di conduzione e manutenzione degli impianti elettrici, speciali di climatizzazione e idrici oltre che per altri lavori di manutenzione) per un ammontare, almeno nel 2022, di oltre 170.000 €, oltre il valore limite di 150.000 € previsto dalla normativa in essere;
- mancato coinvolgimento di altri operatori economici e mancata negoziazione con la controparte potenziale per i servizi oggetto dei diversi affidamenti. Nelle delibere di affidamento non vi è traccia dell'indagine sul mercato tra più operatori e della trattativa/negoziazione diretta con l'operatore economico;
- mancata verifica sulla congruità dei prezzi. L'istruttoria mostrava come nessuna delle determine a contrarre conteneva la motivazione del provvedimento, né chiariva come sarebbe stata accertata la congruità dei prezzi, peraltro non sempre dichiarata, né conteneva la prevista dichiarazione in ordine all'insussistenza delle cause di conflitto di interesse da parte di chi partecipa al procedimento a qualsiasi titolo.

In sostanza, le violazioni con riferimento al caso specifico sono tante. Al riguardo, il Presidente dell'ANAC invita a tenere in considerazione per i futuri affidamenti quanto sopra esposto al fine di evitare provvedimenti sanzionatori.

**Fonte: Atto del Presidente dell'ANAC 16 aprile 2024**

---



## La sottoposizione a misura cautelare interdittiva dell'Amministratore di fatto impone una valutazione da parte della PA circa l'affidabilità dell'operatore economico senza però alcun automatismo

Il Comune di Sellia Marina aggiudicava l'affidamento dei lavori di adeguamento sismico ed ampliamento della scuola di Viale Calabricata all'operatore economico Omissis S.r.l., primo classificato. Il secondo classificato impugnava la determina di aggiudicazione definitiva e il TAR inizialmente rigettava il ricorso, con la conseguenza che la stazione appaltante procedeva a stipulare il contratto con l'impresa prima classificata.

Tuttavia, il Consiglio di Stato, in riforma della sentenza del TAR, accoglieva il ricorso e la relativa istanza cautelare di sospensiva dell'atto impugnato e disponeva, come reintegra in forma specifica, il subentro nel contratto dell'impresa seconda classificata. L'impresa Omissis S.r.l., originariamente prima classificata, segnalava quindi con plurimi esposti all'ANAC che in capo all'amministratore di fatto dell'operatore economico subentrante era stata adottata dal GIP di Catanzaro la misura cautelare del divieto di contrarre con la PA. La stazione appaltante, pertanto, in risposta a una richiesta di chiarimento dell'Autorità, specificava che l'Ente aveva formalizzato in via prudenziale 3 richieste di comunicazione antimafia per l'impresa, sollecitando altresì la Prefettura di Roma.

L'Autorità, quindi, si è soffermata, nel caso in esame, sul tema relativo alla mancata valutazione dell'affidabilità dell'operatore economico da parte della Stazione Appaltante.

L'ANAC ha invero specificato che la sottoposizione a misura cautelare interdittiva costituisce causa di esclusione ex art. 80, co. 5 lett. d) D.Lgs. 50/2016 (applicabile al momento dei fatti). Si segnala che, nel predetto articolo, non si faceva riferimento all'amministratore di fatto. Tuttavia, il Consiglio di Stato già nel 2022 aveva chiarito che la perdita dei requisiti generali in capo all'amministratore di fatto può riversarsi sull'operatore economico, con la conseguente esclusione dalla procedura. Peraltro, il Nuovo Codice Appalti ha fatto rientrare tra i soggetti cui riferire le cause di esclusione anche l'amministratore di fatto.

L'art. 80, co. 5 lett. c) D.Lgs. 50/2016 prevede però che sia necessaria una valutazione discrezionale dell'amministrazione circa gli illeciti professionali gravi, che possono condurre all'esclusione, senza però automatismi. L'illecito professionale grave è definito dalla giurisprudenza come qualsiasi fatto tale da porre in dubbio l'integrità e l'affidabilità dell'operatore economico, senza la necessità dell'accertamento con sentenza irrevocabile. La stazione appaltante, pertanto, al di fuori delle cause di esclusione automatica, ha un apprezzabile margine di discrezionalità circa l'incidenza della condotta sull'affidabilità e integrità del concorrente.

L'ANAC, nel caso in esame, ha censurato il fatto che il Comune non abbia effettuato alcuna valutazione circa l'affidabilità dell'operatore a fronte della misura cautelare interdittiva applicata all'amministratore di fatto. Peraltro, ha ritenuto inutile l'interrogazione del Comune alla Prefettura, posto che l'applicazione della misura cautelare interdittiva non rileva ai fini della comunicazione antimafia, nella quale sono riportate solamente le interdittive ex D.Lgs. 159/2011.

**Fonte: Delibera ANAC 16 aprile 2024**

---



## ANAC: non è sufficiente una contestazione dall’Agenzia delle Entrate per essere esclusi da una gara d’appalto

L’Autorità Nazionale Anticorruzione (ANAC) si è espressa in merito al provvedimento di esclusione da una gara di appalto per servizi di pulizia operato dall’Assessorato Regionale dei Beni Culturali e dell’Identità Siciliana, nei confronti di un operatore economico oggetto di contestazioni fiscali da parte dell’Agenzia delle Entrate.

A subire il provvedimento di esclusione e ad inoltrare l’istanza singola di parere per la soluzione delle controversie ex articolo 211, comma 1 del decreto legislativo 31 marzo 2023, n. 36 è stata la società Pluriservices S.r.l., a causa della presenza a suo carico di contestazioni fiscali ritenute gravi dalla Stazione appaltante ai sensi dell’art. 95, comma 2, del d.lgs. 36/2023.

Secondo il citato articolo, la Stazione appaltante può escludere un operatore economico «se sussistono gravi violazioni, definitivamente accertate o comunque con sentenza di condanna passata in giudicato, degli obblighi relativi al pagamento delle imposte e tasse o dei contributi previdenziali». Tuttavia, l’ANAC, a fronte del valore contestato inferiore ai 35.000 euro, stabilisce nel proprio parere precontenzioso l’illegittimità dell’esclusione operata dalla Stazione appaltante. Infatti, l’art. 3 dell’Allegato II.10 del d.lgs. 36/2023 specifica che la violazione fiscale è considerata «grave» solo se l’importo contestato è pari o superiore al 10% del valore dell’appalto e, comunque, non inferiore a 35.000 euro e nel caso in questione, l’importo oggetto di verifica inferiore alla soglia minima, impedisce l’esclusione automatica dalla gara.

L’ANAC ha quindi accolto il ricorso di Pluriservices S.r.l., annullando la sua esclusione dalla gara, ribadendo che la Stazione appaltante ha sì il dovere di valutare con discrezionalità la gravità delle violazioni fiscali, tenendo tuttavia conto dei criteri stabiliti dalla normativa vigente.

**Fonte: Delibera ANAC n. 234 del 15 maggio 2024**

---



## EDPS adotta i primi orientamenti sull'utilizzo di sistemi di IA generativa

Il 3 giugno 2024 l'European Data Protection Supervisor (l'Autorità Garante Europea per la protezione dei dati personali, o anche solo «EDPS») ha pubblicato i suoi primi orientamenti relativi al rapporto tra utilizzo di sistemi di intelligenza artificiale generativa (GenAI) e protezione dei dati personali. Queste indicazioni intendono fornire consigli e istruzioni pratiche alle istituzioni, agli organi e agli organismi dell'UE, ma esprimono anche principi di portata generale applicabili all'utilizzo di sistemi di IA generativa da parte di pubbliche amministrazioni e aziende private.

In primo luogo l'EDPS definisce l'IA generativa come «un sottoinsieme di IA che utilizza modelli di apprendimento automatico specializzati, progettati per produrre una varietà ampia e generica di output, in grado di svolgere una serie di compiti e applicazioni, come ad esempio generare testo, immagini o audio». Il ciclo di vita di un sistema di IA generativa comprende molteplici fasi:

- 1) viene definito l'ambito di utilizzo del modello;
- 2) il modello viene addestrato attraverso datasets specifici e rilevanti per il futuro utilizzo del sistema;
- 3) la fase di training viene completata grazie all'uso di specifiche tecniche, per le quali è necessario l'intervento umano, che assicurano una maggiore precisione delle informazioni;
- 4) viene valutata l'effettiva funzionalità del modello attraverso l'uso di determinate metriche;
- 5) infine, il modello viene impiegato e implementato.

Dopo aver definito le caratteristiche ed il ciclo di vita di un sistema di IA generativa, l'EDPS fornisce delle indicazioni finalizzate ad un utilizzo di tale tecnologia conforme alle normative europee in materia di protezione dei dati personali. In particolare:

- è necessario stabilire se ed in quale fase dello sviluppo di un sistema di IA generativa è stato effettuato un trattamento di dati personali. Spesso vengono trattati dati personali nella creazione del dataset utilizzato per l'addestramento, nella stessa fase di addestramento durante la quale vengono inferite informazioni ulteriori e nella fase operativa del sistema attraverso l'input e l'output di nuove informazioni. Nel caso in cui il provider del sistema di IA generativa affermi che non vengono trattati dati personali (ad esempio adducendo l'anonimizzazione degli stessi) è importante richiedere a quest'ultimo evidenza dei controlli e delle procedure poste in essere a tale scopo;
- nella fase di implementazione del sistema di IA generativa è importante coinvolgere il DPO, il quale può fornire consigli e garantire un'assistenza indipendente in merito all'applicazione della normativa in materia di protezione dei dati personali alla fattispecie concreta. Per svolgere il suo ruolo in maniera efficace, il DPO, deve venire a conoscenza delle modalità di trattamento dei dati personali, del funzionamento del meccanismo di input-output e del processo decisionale implementato nel modello;
- in ogni fase del ciclo di vita del sistema di IA generativa nel quale vi sia un trattamento di dati personali è importante verificare la liceità di quest'ultimo, individuando la base giuridica maggiormente adeguata. L'EDPS consiglia di prestare particolarmente attenzione ai casi in cui i service providers di IA generative pongano come base del trattamento il legittimo interesse. Infatti, l'Autorità afferma che in questo caso il legittimo interesse dovrà rispettare i requisiti individuati dalla CGUE nella sentenza C-252/21, in particolare è necessario che il legittimo interesse del provider non contrasti diritti o libertà fondamentali dell'interessato. L'EDPS specifica che è onere dell'utilizzatore del sistema di IA generativa verificare che il provider abbia rispettato le condizioni per l'utilizzo del legittimo interesse come base legale;
- durante ogni fase del ciclo di vita del sistema di IA generativa è fondamentale rispettare il principio di minimizzazione dei dati personali. In particolare il titolare ha l'obbligo di limitare la raccolta indiscriminata di dati e, al contrario, deve trattare solo i dati personali strettamente necessari per il perseguimento delle finalità del trattamento;
- nello sviluppo e nell'utilizzo di sistemi di IA generativa è necessario rispettare il principio di esattezza dei dati. Tale principio implica: nella fase di sviluppo, l'obbligo di verifica della struttura e dei contenuti del dataset di addestramento ed il controllo dei dati di output; nella fase di utilizzo, la necessità di ottenere garanzie contrattuali e documentazione relativamente alle procedure seguite per assicurare l'esattezza dei dati impiegati.

Fonte: [https://www.edps.europa.eu/system/files/2024-06/24-06-03\\_genai\\_orientations\\_en.pdf](https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf)



## Garante Privacy: indicazioni su web scraping e IA generativa

Il 20 maggio 2024, l'Autorità Garante per la protezione dei dati personali ha adottato e pubblicato una nota informativa in materia di web scraping per finalità di addestramento di intelligenza artificiale generativa.

Con la predetta nota informativa il Garante intende fornire indicazioni in merito al fenomeno della raccolta massiva di dati personali dal web per finalità di addestramento dei modelli di intelligenza artificiale generativa e segnalare possibili azioni di contrasto ai gestori di siti internet e piattaforme online, quali titolari del trattamento dei dati personali oggetto di pubblicazione.

Il Garante, innanzitutto, definisce l'attività di web scraping: essa consiste nell'utilizzo di programmi informatici, che scandiscono sistematicamente il web (c.d. *web crawler*) al fine di raccogliere massivamente ed indiscriminatamente dati contenuti nelle pagine web e successivamente conservare e memorizzare i dati così raccolti al fine di analizzarli ed elaborarli.

L'attività di *web scraping* può avere varie finalità, la cui liceità deve essere necessariamente accertata caso per caso. Tra le finalità alla base del web scraping vi è anche l'addestramento di sistemi di intelligenza artificiale generativa: infatti gli sviluppatori possono creare dataset frutto di un'attività di *scraping*, oppure utilizzare *data lake* di terze parti creati a loro volta attraverso la medesima attività.

I gestori dei siti web, titolari del trattamento di dati personali resi disponibili al pubblico attraverso piattaforme online, potrebbero ritenere il web scraping di terze parti finalizzato all'addestramento di IA generativa incompatibile con le finalità e le basi giuridiche della messa disposizione del pubblico dei dati personali. In questo caso, in ossequio al principio di *accountability*, il titolare del trattamento dovrebbe porre in essere adeguate cautele per mitigare gli effetti dell'attività di *web scraping*.

Il Garante indica, nella nota informativa in oggetto, quali potrebbero essere le misure più idonee ad evitare il fenomeno del web scraping, con l'avvertenza che nessuna di esse è in grado di impedire tale attività al 100%. In particolare, il Garante suggerisce di:

- creare aree riservate a cui si può accedere solo previa registrazione, in modo tale da sottrarre i dati personali alla pubblica disponibilità;
- inserire, nei Termini di Servizio del sito web, clausole ad hoc che prevedano l'espresso divieto di utilizzare tecniche di web scraping. Tale cautela, essendo di natura strettamente giuridica, opera ex post (attraverso l'azione in giudizio da parte del gestore del sito web), ma può altresì costituire uno strumento di carattere special-preventivo;
- monitorare il traffico di rete in modo tale da individuare i flussi anomali di dati in ingresso e in uscita dal sito web;
- porre in essere qualsiasi tecnica in grado di limitare l'accesso ai *bot*, come, a titolo esemplificativo, l'inserimento di verifiche CAPTCHA, la modifica periodica del *markup* HTML e il monitoraggio dei file di *log*.

Fonte: <https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/10020334>

---



## Per le Sezioni Unite non vi è alcuna continuità normativa tra il reato di millantato credito e quello di traffico di influenze illecite (Cassazione penale, Sez. Un., 15 maggio 2024, n. 19357)

Con sentenza 15 maggio 2024, n. 19357, le Sezioni Unite penali della Corte di Cassazione hanno risposto al quesito: «se sussista continuità normativa tra il reato di millantato credito ex art. 346, secondo comma, c.p. (abrogato dalla L. 9 gennaio 2019, n. 3) ed il reato di traffico di influenze illecite ex art. 346-bis c.p. (modificato dalla sopra citata legge)».

La Seconda Sezione penale aveva rilevato l'esistenza di un contrasto giurisprudenziale in ordine alla questione della continuità normativa tra l'abrogato reato di millantato credito e il "nuovo" reato di traffico di influenze illecite, rimettendo il ricorso all'esame delle Sezioni Unite.

Secondo un primo orientamento, sussiste piena continuità normativa tra la fattispecie prevista dall'abrogato art. 346 c.p. e l'art. 346-bis c.p., con la conseguenza che il secondo ha "inglobato" la descrizione delle condotte sanzionate dal primo. Secondo tale indirizzo, salve talune differenze, la riformulata disposizione dell'art. 346-bis c.p. punisce le medesime condotte in precedenza descritte dall'art. 346 c.p. Si tratterebbe di un fenomeno di "fusione, mediante incorporazione" di due disposizioni incriminatrici, mediante la formale abrogazione della prima e la modifica del testo della seconda.

Un secondo orientamento esclude la continuità normativa, osservando che nella fattispecie del novellato art. 346-bis c.p. non è ricompresa la condotta di chi, mediante artifici o raggiri, riceve o si fa dare o promettere denaro o altra utilità «col pretesto» di dovere comprare il pubblico ufficiale o impiegato o doverlo comunque remunerare: condotta che integra, invece, il reato di truffa ex art. 640, comma 1, c.p.. Nonostante la manifestata volontà del legislatore del 2019 di realizzare una forma di abrogatio sine abolitione, non vi è una esatta corrispondenza tra la condotta in precedenza prevista dalla norma contenuta nell'abrogato art. 346, comma 2 c.p., e quella riformulata del "nuovo" art. 346-bis c.p.. in quanto non è stato riproposto il termine "pretesto" contenuto nella precedente ipotesi di reato, con conseguente assimilazione ad una particolare forma di truffa, tanto da far ritenere che nel millantato credito c.d. "corruttivo" restasse assorbita la fattispecie di cui all'art. 640 c.p.

Le Sezioni Unite hanno aderito al secondo orientamento, precisando che le condotte già integranti gli estremi dell'abolito reato di cui all'art. 346, secondo comma c.p. potevano, e tuttora possono, configurare gli estremi del reato di truffa (in passato astrattamente concorrente con quello di millantato credito corruttivo), purché siano formalmente contestati e accertati in fatto tutti gli elementi costitutivi della relativa diversa fattispecie incriminatrice.

In prima analisi, le Sezioni Unite hanno ricordato che il delitto ex art. 346 c.p., in entrambe le sue declinazioni (millantato credito cd. "semplice" di cui al primo comma; millantato credito cd. "corruttivo", di cui al secondo comma), considerava inesistenti sia il credito, sia l'influenza, sia la stessa relazione tra il millantatore e il pubblico agente e la disposizione era tutta "concentrata" sulla condotta dell'unico soggetto di cui era prevista la punizione ("millantando credito ... riceve, si fa dare o promettere ... con il pretesto ..."), a differenza della "vittima" del millantato credito, raffigurato come soggetto danneggiato perché tratto in inganno dalla vanteria di una inesistente relazione con il pubblico agente, i cui favori il millantatore si proponeva di "comprare". Le due figure di reato venivano tenute nettamente distinte, in quanto: nella prima fattispecie, il denaro e l'altra utilità erano ritenuti il prezzo della mediazione ed il fatto era considerato punibile anche in assenza di impiego, da parte del millantatore, di particolari forme di artifici o raggiri. Invece, nella seconda fattispecie, il denaro o l'altra utilità erano indicati come il prezzo di una possibile corruzione: dunque, il millantatore, che intendeva trattenere per sé il prezzo, lo chiedeva con il "pretesto" di dover comprare il favore del pubblico agente o di doverlo remunerare; presentandosi, così, come "strumento" di corruzione di un pubblico agente, con il quale egli non aveva alcuna relazione.



In seconda analisi, con riferimento al reato ex art. 346-bis c.p., le Sezioni Unite hanno ricordato che il delitto presuppone una relazione effettivamente esistente tra il mediatore, che si proponeva di sfruttarla per perseguire un fine illecito, ed il pubblico agente, i cui favori il privato intendeva acquistare promettendo la consegna o consegnando un prezzo. Le Sezioni Unite hanno precisato che tali elementi qualificanti avevano permesso di distinguere gli ambiti applicativi dell'art. 346-bis c.p. rispetto a quella dell'art. 346 c.p.. In conclusione, nella ipotesi di reato ex art. 346-bis c.p., entrambi i soggetti raggiungevano una intesa ed erano punibili, trattandosi di coautori in un reato normativamente plurisoggettivo; la mediazione era considerata "onerosa" o "gratuita", a seconda che il prezzo fosse richiesto per il mediatore oppure per il pubblico agente.

Secondo il parere delle Sezioni Unite, rispetto alle dichiarate intenzioni del legislatore di far confluire nel primo comma riformato dell'art. 346-bis c.p. con la contestuale abrogazione dell'art. 346 c.p. ad opera della Legge 3/2019, è da escludere che la voluntas legis possa costituire canone interpretativo dirimente per risolvere il quesito. In conclusione, il confronto tra le linee strutturali generali delle due fattispecie di reato poste a raffronto risulta più coerente con l'idea di una "discontinuità normativa" tra le considerate disposizioni incriminatrici e quindi le Sezioni Unite hanno ritenuto che la scelta del legislatore del 2019 di abrogare l'art. 346 c.p. e contestualmente di modificare il contenuto dell'art. 346-bis c.p., ha comportato un fenomeno di abolitio criminis con riferimento ai fatti di millantato credito c.d. "corruttivo", già previsti dall'art. 346, comma 2, c.p.

**Fonte: Cassazione penale, Sez. Un., 15 maggio 2024, n. 19357**

### **L'adozione di misure per la protezione dai rischi interferenziali e la responsabilità del committente e appaltatore (Cassazione Penale, Sez. IV, 6 maggio 2024, n. 17683)**

Il caso in oggetto muove dal ricorso per Cassazione del Legale Rappresentante di una Società committente di lavorazioni su strutture prefabbricate ritenuta responsabile - in cooperazione con l'Amministratore Unico della Società appaltatrice - in relazione ad un infortunio sul lavoro avvenuto durante operazioni di verniciatura di un pannello prefabbricato, dal quale conseguivano per il lavoratore lesioni da schiacciamento con prognosi superiore a 40 giorni.

Veniva contestato ad entrambi gli imputati la mancanza, nei propri documenti di valutazione del rischio, di indicazioni relative ai pericoli connessi alle operazioni svolte (che sarebbero state inserite nei DVR successivamente all'evento) nonché la mancata trasmissione al lavoratore coinvolto di adeguate informazioni e idonea formazione sui rischi per la propria salute e sicurezza, con specifico riguardo a quelli derivanti direttamente dalle mansioni a lui demandate.

La Corte territoriale ha ritenuto poi che in capo alla ricorrente fosse mancata altresì un'attività organizzativa di prevenzione del rischio concreto rispetto alle operazioni eseguite nei propri locali di lavoro e che costituivano l'oggetto della propria linea produttiva.

L'occasione descritta è gradita alla Corte per ribadire - in coerenza a quanto già espresso in precedenti pronunce - alcuni dei principi cardine nell'ambito della Salute e Sicurezza sui luoghi di lavoro (anche) in contesti di contratti di appalto di opere e/o servizi. Si fa riferimento, segnatamente:

- le norme antinfortunistiche sono destinate a garantire la sicurezza delle condizioni di lavoro, anche in considerazione della disattenzione con la quale gli stessi lavoratori effettuano le prestazioni;
- qualora in uno stesso luogo operino più lavoratori, dipendenti da diversi datori di lavoro, ciascuno di questi, anche se subappaltatore, è tenuto all'elaborazione del DVR (artt. 28 e 29 D.Lgs. 81/2008) e solo il datore di lavoro/committente è tenuto alla redazione del DUVRI (art. 26, co. 3 D.Lgs. 81/2008);



- ogni datore di lavoro (anche subappaltatore) deve osservare le disposizioni in materia di sicurezza sui luoghi di lavoro e deve adottare idonee misure di prevenzione e protezione contro tutti i rischi per la salute e sicurezza durante l'attività lavorativa, anche quando questi sono dovuti alle cd. interferenze con attività di altre imprese e anche quando l'organizzazione del luogo di lavoro resta sottoposta ai poteri direttivi dell'appaltatore (in caso di subappalto) o del committente;
- l'obbligo di adottare tali misure non trova un limite quando l'attività dei lavoratori di una ditta appaltatrice (o subappaltatrice) si svolge in un luogo nella disponibilità giuridica altrui (es., lavorazione presso stabilimento del committente);
- nell'ipotesi dei cd. rischi interferenziali, l'obbligo per ciascun datore di lavoro di adottare idonee misure di prevenzione e protezione contro tutti i rischi - e di occuparsi del coordinamento dei vari interventi - non può essere escluso dalla circostanza che la redazione del DUVRI è compito precipuo del solo datore di lavoro/committente. Al riguardo, l'art. 26 distingue tra obblighi di coordinamento/attuazione delle misure di prevenzione/protezione (anche in caso di interferenze) che gravano su tutti i datori di lavoro ed obbligo di elaborazione del DUVRI che incombe solo sul datore di lavoro/committente;
- il DUVRI costituisce il risultato di un'attività di cooperazione e coordinamento tra tutti i datori di lavoro coinvolti (a riprova del coinvolgimento di tutti i soggetti in caso di lavorazioni da interferenza);
- il committente è titolare ex lege di una posizione di garanzia che integra ed interagisce con quella di altre figure di garanti legali (es., datore di lavoro, dirigente per la sicurezza, preposto, etc.) e può nominare un responsabile dei lavori (con delega formale che ricomprenda anche il conferimento di poteri decisori, gestionali e di spesa) che gli consente di andare esente da responsabilità, entro i limiti conferiti e fermo restando la propria responsabilità per la redazione del piano di sicurezza, del fascicolo di protezione dai rischi e per la vigilanza sul coordinatore circa l'espletamento dell'incarico conferito, nonché sul controllo del rispetto delle disposizioni previste nel piano;
- rappresenta obbligo di diligenza del garante prevedere il rischio specifico e indicarlo nel DVR, con conseguente adozione delle misure appropriate a prevenirlo (la mancata adozione di tali misure, seppur previste nel DVR, non esonera da un giudizio di responsabilità).

La Corte, posto quanto sopra descritto, ha quindi confermato la decisione di condanna già emessa nel grado di appello e ribadito come il Legale Rappresentante della Società committente avesse omesso qualsivoglia previsione di idonee misure di sicurezza nel proprio ciclo produttivo che avrebbero, se previste e applicate, ragionevolmente prevenuto il verificarsi dell'evento.

**Fonte: Cassazione Penale, Sez. IV, 6 maggio 2024, n. 17683**

---



## Amministrazione giudiziaria: altra nota casa di moda colpita dalla misura di prevenzione (Tribunale di Milano, sez. Misure di Prevenzione, decreto n. 12 del 6 giugno 2024)

Con decreto n. 12 del 6 giugno 2024, il Tribunale di Milano - Sezione Misure di Prevenzione ha applicato la misura dell'amministrazione giudiziaria ad una nota casa di moda, per aver agevolato colposamente, mediante omessi controlli, condotte di caporalato realizzate da subappaltatori coinvolti nella catena di fornitura.

L'organo giudicante ha invero riscontrato elementi di similitudine con le situazioni che hanno condotto alla sottoposizione alla misura di prevenzione di altri due noti brand del luxury fashion.

In particolare, le indagini hanno fatto emergere come la produzione di borse fosse esternalizzata dalla casa di moda a imprese prive di un'adeguata capacità produttiva, le quali a loro volta subappaltavano la produzione ad opifici cinesi, ove veniva riscontrato:

- l'utilizzo e lo sfruttamento di manodopera irregolare e clandestina;
- il transito dei soggetti irregolari da un opificio all'altro;
- la presenza del medesimo committente della produzione in subappalto;
- la violazione delle norme in tema di salute e sicurezza sui luoghi di lavoro, nonché di condizioni abitative e ambienti di lavoro.

Con riferimento alla committente, è stata accertata una carenza di modelli organizzativi ai sensi del D.Lgs. 231/2001 e un sistema di internal audit fallace, elementi integranti i presupposti di cui all'art. 34 Cod. Antimafia, in quanto tali carenze e mancati controlli avrebbero colposamente agevolato la realizzazione del reato di cui all'art. 603 bis c.p. da parte delle società subappaltatrici.

Gli elementi di cui sopra hanno quindi consentito al Tribunale l'applicazione dell'amministrazione giudiziaria, disponendo che l'intervento dell'Amministratore debba essere finalizzato:

- ad analizzare i rapporti con i fornitori, in modo da evitare che la filiera produttiva si articoli in appalti e subappalti nei quali vengono realizzate condotte illecite;
- a rimuovere i contratti in essere con soggetti direttamente o indirettamente collegati a realtà imprenditoriali che realizzano condotte illecite;
- ad adottare un efficace Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001;
- a rafforzare i presidi di controllo interno e quelli relativi alle verifiche reputazionali dei fornitori.

**Fonte: Tribunale di Milano, sez. Misure di Prevenzione, decreto n. 12 del 6 giugno 2024**

---

## CONTATTI

Viale Abruzzi, 94  
20131 Milano  
Tel. 02 58 20 10

BDO Advisory Services S.r.l.  
[ras@bdo.it](mailto:ras@bdo.it)

BDO è tra le principali organizzazioni internazionali di servizi alle imprese.

Questa pubblicazione non può, in nessuna circostanza, essere associata, in parte o in toto, ad un'opinione espressa da BDO. Nonostante l'attenzione con cui è preparata, BDO non può essere ritenuta responsabile di eventuali errori od omissioni contenuti nel documento. La redazione di questo numero è stata completata il 01 luglio 2024.

BDO Advisory Services S.r.l., società a responsabilità limitata, è membro di BDO International Limited, società di diritto inglese (company limited by guarantee), e fa parte della rete internazionale BDO, network di società indipendenti. BDO è il marchio utilizzato dal network BDO e dalle singole società indipendenti che ne fanno parte.

© 2024 BDO (Italia) - Flash Info Paper - Tutti i diritti riservati.

[www.bdo.it](http://www.bdo.it)



Vuoi ricevere la TaxNews e altre notizie da BDO direttamente via email?  
Iscriviti alle nostre mailing list.

