Giugno 2026

flash infopaper

Compliance & Risk Management

compliance normativa | anticorruzione

privacy | giurisprudenza

Compliance normativa

Anticorruzione

Privacy

Giurisprudenza

UIF: profili di rischio e obblighi SOS in materia di misure restrittive UE

Con la Comunicazione del 7 maggio 2026, l'Unità di Informazione Finanziaria per l'Italia (UIF) ha richiamato l'attenzione degli operatori sugli obblighi connessi al rispetto delle misure restrittive dell'Unione Europea, alla luce dell'entrata in vigore del D. Lgs. 211/2025, che ha attribuito rilevanza penale e ex d.lgs. 231/2001 alla violazione o all'elusione delle suddette misure.

Innanzitutto, ai fini della prevenzione dei reati di cui al d.lgs. 211/2025, l'UIF evidenzia che assumono rilievo i già previsti doveri derivanti dal d.lgs. 109/2007 a carico degli intermediari bancari e finanziari e degli altri soggetti obbligati (obbligo di congelamento di fondi e risorse detenuti, anche per interposta persona fisica o giuridica, da persone fisiche, giuridiche, gruppi o entità, designati, e i relativi obblighi di comunicazione). Inoltre, la UIF evidenzia come suddetti reati integrino ipotesi di attività criminose che, al ricorrere dei presupposti di cui all'art. 35 del D. Lgs. 231/2007, determinano l'obbligo di segnalazione di operazioni sospette (SOS). L'obbligo di segnalazione rimane però distinto e autonomo rispetto ai doveri di comunicazione relativi alle misure restrittive UE e presuppone sempre una valutazione adeguata e concreta del sospetto.

La Comunicazione individua diversi profili di anomalia e operatività a rischio, tra cui il ricorso a catene partecipative complesse e opache, operazioni di triangolazione di fondi tramite prestatori di servizi di pagamento attivi presso Paesi che non hanno applicato alcuna misura restrittiva, triangolazione di cripto-attività, utilizzo di conti di corrispondenza e IBAN virtuali (vIBAN) ovvero di strumenti di pagamento atti a dissimulare l'origine e la destinazione effettiva dei fondi, meccanismi di occultamento della localizzazione dei soggetti coinvolti tramite VPN, raccolte di fondi destinate ad aree di conflitto e attività di import/export di beni di lusso, prodotti petroliferi, macchinari industriali ad alto contenuto tecnologico e beni dual use.

Gli indici di anomalia sopra richiamati possono inoltre costituire utili elementi per l'individuazione delle c.d. red flags, rilevanti ai fini dell'attivazione di presidi di due diligence rafforzata secondo un approccio risk based, anche quali strumenti di prevenzione e controllo nell'ambito dei modelli organizzativi adottati ai sensi del d.Lgs. 231/2001.

La UIF invita pertanto tutti i destinatari a prestare la massima attenzione nella valutazione delle anomalie soggettive e oggettive rilevate, assicurando un'analisi concreta e complessiva dell'operatività. A supporto delle attività di segnalazione, è stato inoltre introdotto in via sperimentale il nuovo fenomeno "V01 – Operatività connessa con violazione di misure restrittive dell'Unione" ovverosia un codice di classificazione da utilizzare nelle segnalazioni di operazioni sospette quando il sospetto riguarda possibili violazioni o aggiramenti delle sanzioni.

Fonte: Comunicazione UIF 7 maggio 2026

ANAC e Società Consortili: Nuovi Confini tra Incompatibilità e Ruoli di Gestione

Nel Parere del 15 aprile 2026 (fasc. 1462/2026), a fronte di richiesta di un'amministrazione avente ad oggetto eventuali ipotesi di inconferibilità e incompatibilità in capo ad amministratori locali candidati per le cariche di presidente del C.d.A. di un'azienda speciale consortile, l'Autorità Nazionale Anticorruzione (ANAC) ha fornito importanti chiarimenti in merito ai confini tra cariche politiche locali e ruoli di vertice all'interno delle aziende speciali consortili.

Il primo elemento analizzato dall'Autorità riguarda il tema dell'inconferibilità. Nel dettaglio, l'Autorità specifica il venir meno del principale ostacolo al passaggio diretto da amministratore locale a esponente politico di un ente strumentale. La Legge n. 15 del 21 febbraio 2025 (di conversione del D.L. Milleproroghe), ha invero abrogato la sanzione della "inconferibilità" per gli ex amministratori locali che intendono candidarsi ai vertici di tali enti.

Esclusa l'inconferibilità, ANAC ha esaminato la speculare causa di incompatibilità (ex art. 11, comma 3, lett. a) del D.lgs. 39/2013), analizzando i due presupposti fondamentali per la sua applicazione nel caso delle aziende speciali:

1. la natura di "Amministratore" ed il peso dei poteri gestionali;
2. il meccanismo di nomina e sovrapposizione territoriale.

In merito al primo punto, ANAC ha evidenziato che le aziende speciali consortili per i servizi alla persona sono qualificate a tutti gli effetti come enti pubblici di livello comunale o provinciale. Tuttavia, per l'applicazione dei citati divieti, occorre considerare le concrete deleghe attribuite a:

- il Presidente del C.d.A. che esercita ampi poteri così come conferiti e previsti dallo Statuto, integra il requisito dell'esercizio di "amministrazione attiva" e poteri gestionali diretti. In questo caso, il Presidente rientra pienamente nella qualifica di "amministratore" ex D.lgs. 39/2013;
- per i Consiglieri del C.d.A. privi di deleghe gestionali dirette, al contrario, l'orientamento consolidato esclude l'applicazione della disciplina restrittiva.

Per quanto concerne il secondo punto, ANAC ha chiarito che l'incompatibilità sorge a causa della sovrapposizione sostanziale tra il territorio in cui il soggetto riveste la carica politica ed il territorio di operatività dell'azienda consortile. Invero, anche se la nomina formale spetta a un organo sociale (l'Assemblea), quest'ultima è composta dai Sindaci dei Comuni soci, della quale questi rappresentano la diretta espressione politica.

Allo scopo di evitare la sovrapposizione tra la figura del "controllore" (il politico che siede in Assemblea) e quella del "gestore" (il vertice del C.d.A.), ANAC ha ritenuto che sussiste l'incompatibilità per la carica di Presidente del C.d.A. qualora permangano i poteri gestionali previsti dagli statuti e vi sia coincidenza territoriale con le cariche politiche locali. L'incompatibilità può essere superata solo se l'Azienda adegua lo Statuto, limitando il ruolo del Presidente alla sola "alta amministrazione" e rappresentanza istituzionale. Per la nomina a semplice membro del C.d.A. senza deleghe, invece, non sussiste alcun ostacolo.

Fonte: Parere Anticorruzione approvato dal Consiglio dell'Autorità del 15 aprile 2026

Verifica dei requisiti dell'operatore economico: attività non delegabile ad operatori economici privati

L'Autorità Nazionale Anticorruzione (ANAC) ha condotto, nel febbraio 2026, un'ispezione presso un soggetto aggregatore regionale per esaminare potenziali criticità legate all'affidamento a operatori privati del servizio di verifica dei requisiti generali e speciali dei partecipanti alle gare pubbliche. Dall'ispezione è emerso che l'ente, a partire dal 2022, ha sistematicamente delegato a società esterne l'acquisizione presso gli uffici pubblici della documentazione necessaria (ad es., certificati penali, documentazione antimafia, carichi pendenti e regolarità fiscale) a comprova dei requisiti ex art. 94 e ss. del d.lgs. 36/2023. Tale prassi è stata giustificata dall'ente con l'elevato volume di procedure gestite a fronte di una carenza di personale interno specializzato, derivante dalla trasformazione dell'ente da agenzia informatica a centrale di committenza.

L'Autorità, a seguito dell'ispezione, ha rilevato talune violazioni di carattere normativo e operativo, quali:

1. esternalizzazione dell'attività di verifica dei requisiti di carattere generale: ANAC ribadisce che la verifica dei requisiti è un'attività provvedimentale riservata alla stazione appaltante e non può essere delegata a privati. Secondo il Codice dei Contratti Pubblici (artt. 15, 17, 62 e 99), tale compito spetta esclusivamente al RUP o ai responsabili di fase, in quanto volto a garantire l'affidabilità morale e professionale dell'appaltatore;
2. funzionalità della Piattaforma di Approvvigionamento Digitale (PAD) in uso presso il soggetto aggregatore: sono emerse carenze nella trasmissione dei dati alla Banca Dati Nazionale dei Contratti Pubblici (BDNCP) ed è stata riscontrata l'assenza di dati relativi all'aggiudicazione e all'esecuzione per alcuni Codici Identificativi di Gara (CIG);
3. criticità afferenti ai singoli affidamenti: l'analisi di specifici contratti ha rivelato ulteriori irregolarità, come:
    - in un caso è stato affidato il servizio al gestore uscente senza adeguata motivazione;
    - in una circostanza, la società incaricata di verificare i requisiti ha partecipato e vinto una gara indetta dallo stesso ente, finendo per acquisire autonomamente la documentazione sui propri requisiti;
    - un servizio è stato qualificato come "fornitura", applicando conseguentemente in modo illegittimo il criterio di aggiudicazione del prezzo più basso anziché quello dell'offerta economicamente più vantaggiosa, omettendo altresì l'indicazione del CCNL.

L'Autorità, dichiarando illegittimi gli affidamenti e il *modus procedendi* adottato, ha invitato l'ente a:

- cessare il ricorso a privati per la verifica dei requisiti, internalizzando l'attività;
- potenziare le competenze interne attraverso l'assunzione di personale specializzato;
- garantire la trasparenza, assicurando il corretto flusso di dati verso la BDNCP tramite la propria piattaforma digitale (PAD).

Fonte: Delibera n. 116 del 1° aprile 2026

Trattamenti antifrode nelle applicazioni di pagamento: sanzione del Garante per accesso illecito ai dati dei dispositivi, carenze di base giuridica e violazione dei principi di privacy by design

Il Garante per la protezione dei dati personali – in data 17 aprile 2026 – ha adottato un provvedimento sanzionatorio nei confronti di un operatore attivo nel settore dei servizi di pagamento, accertando l'illiceità dei trattamenti di dati personali effettuati tramite applicazioni mobili utilizzate dalla clientela, nell'ambito di sistemi di prevenzione delle frodi informatiche. Il procedimento trae origine da un significativo numero di segnalazioni e reclami pervenuti all'Autorità a partire dall'aprile 2024, nei quali gli utenti rappresentavano l'introduzione, all'interno delle applicazioni, di una nuova funzionalità qualificata come necessaria per garantire la sicurezza delle operazioni. In particolare, agli utenti veniva richiesto di autorizzare l'accesso ai c.d. «dati di utilizzo» del dispositivo, con l'indicazione che, in caso di mancata attivazione, l'operatività dell'app sarebbe stata progressivamente limitata fino alla sua completa inibizione.

Nel corso dell'istruttoria, l'Autorità ha analizzato nel dettaglio il funzionamento della soluzione antifrode implementata, rilevando come essa comportasse la raccolta sistematica di un'ampia gamma di dati relativi al dispositivo dell'utente. Tra questi, assume particolare rilievo l'acquisizione delle informazioni relative alle applicazioni installate o in esecuzione, attraverso l'utilizzo di tecniche di *hashing* e di correlazione con identificativi univoci del dispositivo.

Secondo il Garante, tale trattamento si caratterizza per un elevato grado di invasività, in quanto le informazioni raccolte risultano idonee a rivelare, anche indirettamente, aspetti della sfera privata dell'utente. In particolare, l'elenco delle applicazioni installate può consentire di inferire abitudini, interessi, comportamenti e, in taluni casi, anche dati riconducibili a categorie particolari, quali informazioni relative allo stato di salute, all'orientamento religioso o politico, o alle preferenze personali.

Sotto il profilo giuridico, il provvedimento distingue chiaramente tra la fase di accesso ai dati presenti nel dispositivo – disciplinata dalla normativa e-Privacy – e la successiva fase di trattamento antifrode, soggetta al GDPR. Con riferimento alla prima fase, l'Autorità ha escluso la possibilità di invocare l'eccezione della «stretta necessità» per l'erogazione del servizio, rilevando come la configurazione adottata non fosse tecnicamente imprescindibile e come risultassero disponibili soluzioni alternative meno invasive, già diffuse nel medesimo settore. Tale valutazione ha condotto alla qualificazione del trattamento come illecito per violazione dell'art. 122 del Codice Privacy, in quanto effettuato in assenza di un consenso valido e liberamente prestato. In particolare, è stato evidenziato che la richiesta di autorizzazione tecnica imposta dal sistema operativo non può essere equiparata al consenso richiesto dalla normativa, sia per la mancanza di adeguata informazione sia per l'assenza di libertà nella scelta dell'utente.

Con riferimento alla fase successiva di trattamento, il Garante ha ritenuto non correttamente individuata la base giuridica. In particolare, è stata esclusa la possibilità di fondare il trattamento sull'adempimento di obblighi legali in materia di sicurezza dei pagamenti, in quanto tali norme non specificano né impongono i trattamenti concretamente effettuati. Al contempo, è stata rilevata l'assenza di un adeguato *legitimate interest assessment*, circostanza che ha impedito il ricorso al legittimo interesse quale base giuridica.

Il provvedimento evidenzia, inoltre, una pluralità di ulteriori violazioni, tra cui quella del principio di trasparenza, in quanto le informative fornite agli utenti non descrivevano in modo adeguato né la natura dei dati raccolti né le finalità e modalità del trattamento. Analogamente, è stata accertata la violazione dei principi di privacy by design e by default, per mancata effettuazione di una valutazione d'impatto specifica e per assenza di una valutazione comparativa delle soluzioni tecniche disponibili.

Fonte: Garante per la protezione dei dati personali, Provvedimento n. 237 del 17 aprile 2026.

Linee guida del Garante sull'utilizzo dei tracking pixel nelle comunicazioni e-mail

Il Garante per la protezione dei dati personali – con provvedimento n. 284 del 17 aprile 2026 – ha adottato le «*Linee guida in materia di utilizzo di tracking pixel nelle comunicazioni di posta elettronica*», offrendo un'interpretazione sistematica del regime normativo applicabile e chiarendo i presupposti di liceità dei trattamenti connessi all'utilizzo di tali strumenti.

Sotto il profilo tecnico, i tracking pixel consistono in immagini di dimensioni minime – spesso invisibili all'utente – che non risultano direttamente incorporate nel corpo del messaggio ma sono richiamate da server remoti al momento dell'apertura dell'e-mail. Tale meccanismo consente al mittente, o a soggetti terzi eventualmente coinvolti, di ricevere informazioni relative all'interazione dell'utente con il messaggio, tra cui l'avvenuta apertura, il numero di visualizzazioni, il tempo di permanenza e ulteriori dati tecnici (quali indirizzo IP, tipologia di dispositivo o caratteristiche del client di posta utilizzato), suscettibili di contribuire alla profilazione dell'interessato.

L'Autorità ha ricondotto tale fenomeno nell'alveo della disciplina prevista dall'art. 122 del Codice Privacy, sottolineando come il funzionamento dei tracking pixel integri una duplice operazione di accesso al terminale dell'utente: da un lato, l'inserimento (o archiviazione) di un elemento sul dispositivo; dall'altro, la successiva lettura di informazioni correlate al comportamento dell'utente. Tale qualificazione determina l'applicazione della direttiva e-Privacy, che si configura come disciplina speciale rispetto al GDPR e introduce un regime fondato su un divieto generale di trattamento, derogabile solo al ricorrere di condizioni tassative.

Nel delineare il quadro regolatorio, il Garante ha attribuito particolare rilievo al principio di trasparenza, evidenziando come l'impiego di strumenti occulti di tracciamento, non percepibili dall'utente, incida in modo particolarmente significativo sul rapporto fiduciario tra titolare e interessato. In tale prospettiva, la mancata conoscibilità dell'utilizzo dei tracking pixel è stata ritenuta suscettibile di determinare una violazione dei principi di correttezza e lealtà, rendendo necessario un innalzamento del livello qualitativo delle informazioni rese agli interessati.

Le Linee guida precisano che l'informativa deve essere fornita in modo chiaro, accessibile e comprensibile, potendo essere strutturata anche su più livelli e attraverso modalità diversificate, al fine di garantire un'effettiva consapevolezza. In tal senso, l'Autorità valorizza l'utilizzo di strumenti multicanale, inclusi elementi dinamici e interattivi, in grado di migliorare l'efficacia comunicativa dell'informazione.

Con riferimento ai presupposti di liceità, il Garante ha affermato che, in via generale, l'utilizzo dei tracking pixel richiede il previo consenso dell'interessato, che deve essere libero, specifico, informato e inequivocabile. Tuttavia, viene riconosciuta la possibilità di derogare a tale regola in presenza di specifiche circostanze, in particolare quando il tracciamento sia strettamente funzionale alla fornitura del servizio richiesto o alla sicurezza delle comunicazioni, ovvero quando venga effettuato per finalità statistiche in forma aggregata e anonimizzata, tale da non consentire l'identificazione individuale dell'utente.

Particolare attenzione è dedicata al coordinamento tra consenso al marketing e utilizzo dei tracking pixel. L'Autorità, in un'ottica di semplificazione e di riduzione dei fenomeni di affaticamento informativo (c.d. *consent fatigue*), ha ritenuto ammissibile la possibilità di un consenso unitario che ricomprenda entrambe le finalità, purché tale soluzione sia adeguatamente rappresentata e non comporti alcuna forma di condizionamento o pressione sull'interessato. Resta, comunque, imprescindibile la previsione di meccanismi di revoca, anche in forma granulare.

L'Autorità ha previsto un periodo transitorio di sei mesi dalla pubblicazione delle Linee guida, entro il quale i soggetti interessati dovranno adeguare i propri sistemi e processi alle indicazioni ivi contenute.

Fonte: Garante per la protezione dei dati personali, Provvedimento n. 284 del 17 aprile 2026.

Sequestro preventivo e responsabilità dell'ente: limiti al riesame e centralità dell'art. 5 D.Lgs. 231/2001 (Cass. Pen., Sez. II, n. 13414/2026)

La sentenza della Corte di Cassazione n. 13414 del 13 aprile 2026 trae origine da un provvedimento di sequestro preventivo disposto nei confronti della società Global Oro S.r.l., indagata per l'illecito amministrativo di cui all'art. 25-*octies* D.Lgs. 231/2001 in relazione a ipotesi di riciclaggio. La società proponeva ricorso per Cassazione, evidenziando in particolare l'insufficienza della motivazione in ordine al *fumus commissi delicti*, con particolare riferimento ai presupposti della responsabilità dell'ente e, in modo specifico, alla mancata individuazione dell'interesse o vantaggio richiesto dall'art. 5 D.Lgs. 231/2001. La contestazione di riciclaggio, così come ricostruita nel provvedimento genetico, si fondava sul presunto coinvolgimento della Global Oro S.r.l. in operazioni di "sostituzione del contante con l'oro", ritenute espressive di condotte di riciclaggio ai sensi dell'art. 648-bis c.p., in quanto funzionali a trasformare denaro di provenienza illecita mediante l'impiego nell'attività orafa. In tale prospettiva, la società era stata inserita, insieme ad altre imprese del settore, tra i soggetti economici utilizzati per tali operazioni, sulla base di elementi indiziari ritenuti sufficienti, in sede cautelare, a formulare un addebito provvisorio anche ai sensi dell'art. 25-octies D.Lgs. 231/2001.

La Corte di Cassazione ha accolto il ricorso affrontando, oltre a profili processuali, anche quello sostanziale della responsabilità dell'ente, richiamandone la struttura e i presupposti applicativi. In particolare, viene evidenziato il carattere autonomo della responsabilità rispetto al reato commesso dalla persona fisica. La Corte ha ribadito che la responsabilità ex D.Lgs. 231/2001 non può essere desunta in via automatica dalla mera commissione del reato presupposto, ma richiede la verifica di specifici elementi costitutivi. In particolare, sul piano oggettivo, è necessario accertare che il reato sia stato commesso nell'interesse o a vantaggio dell'ente, mentre sul piano soggettivo rileva la cosiddetta "colpa di organizzazione", da valutare alla luce del ruolo dell'autore del reato e dell'assetto organizzativo della società, ossia verificando se la condotta illecita sia stata posta in essere da soggetti inseriti stabilmente nella struttura dell'ente – in posizione apicale o sottoposta – e se l'organizzazione societaria, per come concretamente delineata, fosse carente sotto il profilo dei presidi preventivi, dei controlli interni e dei modelli di gestione del rischio-reato, così da consentire o agevolare la commissione del reato presupposto.

In questa prospettiva, anche il sequestro preventivo finalizzato alla confisca del profitto deve essere sorretto da una motivazione che tenga conto dell'intera fattispecie dell'illecito amministrativo. Non è sufficiente richiamare il coinvolgimento della società nei fatti di riciclaggio o il comportamento dei singoli dipendenti: è necessario esplicitare, sia pure in forma sintetica, gli elementi dai quali desumere la riconducibilità del fatto all'ente secondo i criteri previsti dalla normativa 231. Nel caso di specie, il provvedimento genetico si limitava a individuare il coinvolgimento della società nelle operazioni di riciclaggio, senza procedere a una specifica valutazione sull'esistenza di un interesse o vantaggio per l'ente né sui criteri di imputazione della responsabilità. Per tali ragioni, la Corte ha annullato senza rinvio sia l'ordinanza adottata nell'ambito del riesame sia il decreto di sequestro preventivo, disponendo la restituzione dei beni alla società.

Fonte: Cass. pen., Sez. II, Sent., -data ud. 1803.2026- 13.04.2026, n. 13414

Corruzione tra privati: la Cassazione amplia la rilevanza della violazione dei doveri di fedeltà e chiarisce la decorrenza del termine di querela (Cass. pen., Sez. V, sent. 14 aprile 2026, n. 13515)

La Corte di Cassazione penale, Sezione V, con la sentenza n. 13515 del 14 aprile 2026, affronta alcuni profili centrali della fattispecie di corruzione tra privati di cui all'art. 2635 c.c., soffermandosi in particolare sull'estensione della nozione di violazione degli obblighi di fedeltà del dipendente .

La vicenda trae origine da un sistema di dazioni indebite che avrebbe coinvolto un dipendente con funzioni direttive di una società appartenente al gruppo FCA e alcuni soggetti riconducibili a una società fornitrice operante nel settore dei trasporti. Secondo l'impostazione accusatoria, il dipendente, pur privo di poteri formali di rappresentanza o di spesa, avrebbe svolto un ruolo strategico nella valutazione tecnica dei fornitori e nel rilascio delle approvazioni delle forniture, favorendo stabilmente determinati operatori commerciali in cambio di somme di denaro occultate attraverso false fatturazioni emesse da una società riconducibile alla sua convivente more uxorio.

La Suprema Corte ha confermato la sussistenza del reato di corruzione tra privati, valorizzando l'evoluzione normativa che ha interessato l'art. 2635 c.c. a seguito della riforma introdotta dal D.Lgs. n. 38/2017. In particolare, la pronuncia ribadisce che, nel vigente assetto normativo, la fattispecie assume natura di reato di mera condotta e di pericolo, con conseguente irrilevanza dell'effettiva produzione di un danno patrimoniale per la società. La violazione dei doveri di fedeltà e correttezza è infatti ritenuta sufficiente ai fini dell'integrazione della fattispecie, anche in assenza di un concreto nocumento economico.

Di particolare interesse risultano le considerazioni svolte dalla Corte in ordine alla nozione di "obblighi di fedeltà". Richiamando la consolidata giurisprudenza civilistica in materia di obbligo di fedeltà del lavoratore subordinato ex art. 2105 c.c., integrato dai principi di correttezza e buona fede di cui agli artt. 1175 e 1375 c.c., la Cassazione ha sottolineato che il dipendente deve astenersi non soltanto da comportamenti concorrenziali o dalla divulgazione di informazioni riservate, ma anche da qualsiasi condotta idonea a creare situazioni di conflitto con gli interessi del datore di lavoro o a compromettere il rapporto fiduciario.

Nel caso concreto, la Corte ha ritenuto rilevante il fatto che il dipendente, in violazione del codice etico aziendale, non avesse comunicato la situazione di conflitto di interessi derivante dai rapporti economici intercorrenti con gli interlocutori commerciali favoriti nelle forniture. Secondo la pronuncia, il patto corruttivo si era concretizzato proprio nell'asservimento delle valutazioni tecniche e dei processi decisionali aziendali agli interessi dei fornitori coinvolti, mediante il sistematico favore accordato agli stessi nelle dinamiche commerciali interne.

La sentenza assume rilievo anche sotto il profilo del soggetto attivo del reato, chiarendo che la qualifica richiesta dall'art. 2635 c.c. può ricorrere anche in capo a soggetti non formalmente dirigenti, ma titolari di "funzioni direttive diverse", purché dotati di autonomia operativa e di un ruolo concretamente incisivo nei processi decisionali dell'impresa. Nel caso di specie, la Corte ha valorizzato il ruolo del dipendente quale responsabile del dipartimento tecnico incaricato di valutare il fabbisogno dei container e di indirizzare, attraverso il proprio giudizio tecnico, le successive procedure di selezione dei fornitori.

Fonte: Cass. pen., Sez. V, sent. 14 aprile 2026, n. 13515

Omicidio colposo e violazioni antinfortunistiche: responsabilità del datore di lavoro per omessa valutazione dei rischi, carente formazione e insufficiente vigilanza (Cass. pen., Sez. IV, Sent., -data ud. 30.01.2026- 21.04.2026, n. 14579)

Con la sentenza n. 14579 del 21 aprile 2026, la Corte di Cassazione è tornata a pronunciarsi sul tema della responsabilità del datore di lavoro nei procedimenti per infortuni sul lavoro, soffermandosi sulla posizione di garanzia datoriale con riferimento agli obblighi di valutazione del rischio, formazione dei lavoratori e vigilanza sull'utilizzo delle attrezzature di lavoro ai sensi del D.Lgs. 81/2008.

La vicenda trae origine dal decesso di un lavoratore irregolare addetto alla conduzione di mezzi meccanici agricoli, impegnato in operazioni di pulitura di un terreno in forte pendenza mediante l'impiego di un trattore cingolato collegato posteriormente a un'attrezzatura frangistoppie. Durante l'attività, il mezzo si ribaltava precipitando nel greto di un torrente provocando la morte dell'operatore per schiacciamento, a causa del mancato utilizzo del mezzo di protezione "Roll bar" di cui il trattore era dotato e dell'assenza di cintura di sicurezza.

Al datore di lavoro veniva contestato il reato di omicidio colposo aggravato dalla violazione delle norme in materia di prevenzione degli infortuni sul lavoro, ai sensi dell'art. 589, comma 2, c.p., in relazione all'art. 29, comma 1, D.Lgs. 81/2008, per aver omesso la corretta valutazione dei rischi derivanti dalle lavorazioni agricole svolte con mezzi meccanici su terreni scoscesi e per non avere predisposto un adeguato documento di valutazione dei rischi; agli artt. 36 e 37 del medesimo decreto, per non aver fornito al lavoratore adeguata e sufficiente formazione ed informazione su rischi dell'attività svolta; nonché all'art. 71, comma 7, D.Lgs. 81/2008, per aver consentito l'utilizzo di un'attrezzatura di lavoro che richiedeva, per il suo impiego, specifiche competenze tecniche e un adeguato addestramento.

La Suprema Corte ha ritenuto infondati i motivi di ricorso, confermando la penale responsabilità del datore di lavoro quale titolare di una posizione di garanzia ai sensi dell'art. 2087 c.c. e dell'art. 2, comma 1, lett. b) D.Lgs. 81/2008. Secondo la Cassazione, tale posizione non si esaurisce nella mera predisposizione formale delle misure di sicurezza, ma comprende anche l'obbligo di verificare concretamente che le attività lavorative siano svolte in condizioni di sicurezza e da personale adeguatamente formato. Particolare rilievo è stato invero attribuito alla circostanza che il lavoratore non avesse ricevuto un addestramento adeguato all'utilizzo del trattore cingolato in condizioni di particolare pericolosità, come quelli derivanti dall'operare in terreni scoscesi. Secondo i giudici di legittimità, tale omissione risultava causalmente collegata all'evento mortale.

La Cassazione ha inoltre valorizzato il fatto che il documento di valutazione dei rischi risultava aggiornato soltanto successivamente all'infortunio e privo di data certa antecedente all'evento lesivo. L'aggiornamento postumo del documento di valutazione dei rischi costituisce indice sintomatico della mancata preventiva individuazione e gestione del rischio lavorativo. Viene inoltre precisato che un DVR generico, non calibrato sulle concrete modalità di esecuzione dell'attività lavorativa, non soddisfa gli obblighi imposti dagli artt. 17 e 28 D.Lgs. 81/2008. La sentenza ribadisce, quindi, il principio secondo cui la valutazione dei rischi deve essere preventiva, specifica e aderente all'effettiva organizzazione del lavoro, non potendo ridursi a un adempimento meramente formale. Sul punto assume dunque rilievo il tema della cosiddetta "data certa", disciplinato dall'art. 2704, comma 1, c.c., secondo cui la data della scrittura privata non autenticata è opponibile ai terzi solo nei casi previsti dalla legge o quando ricorra un fatto idoneo a dimostrarne con certezza l'anteriorità. In applicazione di tali principi, l'art. 28, comma 2, D.Lgs. 81/2008 stabilisce che il DVR deve essere munito di data certa oppure attestato mediante la sottoscrizione del datore di lavoro e, ai soli fini della prova della data, anche del RSPP, del RLS e del medico competente, ove nominato.

Alla luce delle considerazioni illustrate, pertanto, la Corte di Cassazione ha dichiarato inammissibile il ricorso, confermando integralmente la condanna pronunciata nei precedenti gradi di giudizio.

Fonte: Cass. pen., Sez. IV, Sent., -data ud. 30.01.2026- 21.04.2026, n. 14579

CONTATTI

BDO Advisory Services S.r.l.
Viale Abruzzi, 94
20131 Milano
Tel. 02 58 20 10

ras@bdo.it

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

Audit | Advisory | Digital | Tax | Law

Il Flash Info Paper viene pubblicato con l'intento di tenere aggiornati i clienti sugli sviluppi in ambito Risk & Compliance. Nonostante l'attenzione con cui è stata preparata, la presente pubblicazione deve essere considerata soltanto come un'indicazione di massima e non può, in nessuna circostanza, essere associata, in parte o in toto, ad un'opinione espressa da BDO. Non si deve fare affidamento sulla pubblicazione per trattare situazioni specifiche e non si deve agire, o astenersi dall'agire, sulla base delle informazioni ivi contenute senza un parere professionale specifico. Si prega di rivolgersi alla società membro di BDO della propria area geografica per discutere di queste questioni tenendo conto delle proprie particolari circostanze. La redazione di questo numero è stata completata il 3 giugno 2026.

www.bdo.it