flash info paper

Compliance & Risk Management

agosto 2021

Il presente numero si propone di illustrare le principali novità in tema di compliance normativa in particolare ai sensi del D.Lgs. n. 231/2001, del Regolamento Europeo GDPR e in materia di anticorruzione.

In questo numero:

- Linee Guida Confindustria per la costruzione di modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01 – Aggiornamento 2021
- Modello organizzativo 231 inadeguato e non attuato (Tribunale di Vicenza, sezione penale, Sentenza del 17 giugno 2021 n. 348)
- Istituzione dell'agenzia per la cybersicurezza nazionale: il PNRR sostiene la cybersicurezza quale fondamento della trasformazione digitale
- EPPO – European Public Prosecutor's Office. La nuova procura europea
- Whistleblowing: le nuove linee guida ANAC
- Nuove linee guida del Garante per la protezione dei dati personali in tema di cookie
- Il Garante sanziona il Comune di Bolzano per controllo indiscriminato dei lavoratori
- L'interesse della società per il conseguimento di un indebito profitto ai danni dello Stato (Cass. pen. Sez. II, 15 giugno 2021, n. 23300)
- Responsabilità ex D.Lgs. 231/2001 in caso di estinzione fraudolenta dell'ente (Cass. pen. Sez. V, 5 luglio 2021, n. 25492)
- Limiti applicativi del D.Lgs. 231/2001 alle imprese individuali (Tribunale di Ravenna, Sentenza del 7 giugno 2021, n. 1056)

INDICE

vai agli argomenti di interesse!

D.LGS. 231/2001 E MODELLI ORGANIZZATIVI

LINEE GUIDA CONFINDUSTRIA PER LA COSTRUZIONE DEI MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO - AGGIORNAMENTO 2021

Nel mese di giugno 2021 Confindustria ha pubblicato l'aggiornamento del documento "*Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231*". La versione aggiornata, rivisitazione del testo risalente al 2014, recepisce le novità normative e gli orientamenti della giurisprudenza degli ultimi sette anni.

Le principali novità della PARTE GENERALE sono:

- *Principio di tassatività dei reati presupposto 231*: le Linee Guida evidenziano che il principio di tassatività dei reati presupposto è stato messo in discussione, a seguito dell'introduzione della fattispecie di autoriciclaggio (ex art. 648-ter.1 c.p.). Si fa quindi presente che la giurisprudenza ha valorizzato il dato letterale della norma che richiama genericamente qualunque "delitto non colposo" come fonte della provvista illecita da riciclare (con particolare riferimento alle violazioni fiscali), mettendo in discussione l'interpretazione che l'elenco dei possibili delitti non colposi possa comprendere esclusivamente quelli inclusi nel catalogo dei reati previsto dal decreto 231.
- *Interesse e vantaggio dell'ente*: le Linee Guida richiamano la giurisprudenza più recente in tema di legittimità al fine di poter interpretare in maniera corretta i concetti di "interesse" e "vantaggio" dell'ente.
- *Sanzioni interdittive*: le Linee Guida hanno aggiornato la tematica delle sanzioni interdittive, in considerazione delle modifiche apportate dalla legge 3/2019 (cd. Spazzacorrotti) che ha inasprito il trattamento sanzionatorio.
- *Sistema integrato di gestione dei rischi:* le Linee Guida sottolineano l'importanza di una compliance integrata, anche attraverso l'esecuzione di risk assessment congiunti, volta a migliorare l'efficacia e l'efficienza delle procedure al fine di ovviare a situazioni di sovrapposizioni di ruoli, duplicazioni di verifiche e di azioni correttive.
- *Sistemi di controllo ai fini della compliance fiscale*: in ottica di approccio integrato le Linee Guida auspicano la creazione di interazioni tra il Modello 231 ed altri strumenti di controllo aziendali al fine di mitigare il rischio fiscale. Tale approccio consentirebbe di integrare il sistema di controllo interno e minimizzare l'impatto derivante dall'adeguamento ai reati fiscali.
- *Comunicazione delle informazioni non finanziarie*: le Linee Guida richiamano il D.Lgs. 254/2016, il quale, recependo la Direttiva 2014/95/UE, prevede che alcune grandi imprese redigano la dichiarazione di carattere non finanziario c.d. DNF (informazioni sui temi rilevanti in materia ambientale, sociale, attinente al personale, al rispetto dei diritti umani, all'anticorruzione) al fine di rafforzare la trasparenza delle informazioni sull'attività di impresa.
- *Whisteblowing:* le nuove Linee Guida, richiamando la legge n. 179 del 2017 (recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato") evidenziano la necessità per le imprese dotate del modello organizzativo 231 di disciplinare le modalità di effettuazione delle segnalazioni e la loro relativa gestione prevedendo un eventuale procedura ad hoc. Le Linee Guida vogliono distinguere il profilo della riservatezza dell'identità del segnalante da quello dell'anonimato: "per garantire al denunciante una tutela adeguata, anche in termini di riservatezza dell'identità, è necessario che esso sia riconoscibile". Sotto il profilo dei possibili canali attivabili, si indica l'utilizzo di piattaforme informatiche anche gestite da terze parti indipendenti e specializzate, oltre che caselle di posta elettronica dedicate da aggiungersi al servizio postale ordinario ovvero nel deposito fisico presso cassette ad hoc. Il modello organizzativo deve innanzitutto indicare il "destinatario" delle segnalazioni: le Linee Guida valutano la scelta di indicare quale destinatario autonomo ed indipendente l'Organismo di Vigilanza coerente con i compiti a esso spettanti ed in ragione degli obblighi di informativa previsti dal decreto 231.
- *Autonomia e indipendenza dell'Organismo di Vigilanza*: le nuove Linee Guida sottolineano l'importanza dell'autonomia dell'ODV, prevedendo il "riporto" al massimo vertice operativo aziendale con la definizione di un budget annuale a supporto dell'attività. Inoltre, al fine di assicurare la necessaria autonomia e indipendenza è indispensabile che all'Organismo di Vigilanza non siano attribuiti compiti operativi e che il grado di indipendenza di questo venga valutato nella sua globalità.
- *Devoluzione delle funzioni di Organismo di Vigilanza al Collegio Sindacale*: le Linee Guida richiamando la nuova versione del Codice di Corporate Governance delle società quotate (31 gennaio 2020) che propone il tema della compatibilità di un OdV composto esclusivamente da membri esterni all'ente, purché sia assicurato – mediante il supporto delle funzioni aziendali e la cura di adeguati flussi informativi – un adeguato coordinamento con i soggetti coinvolti nel sistema di controllo interno e di gestione dei rischi, raccomandando di assicurare uno stretto coordinamento tra tutti i soggetti facenti parte del sistema di controllo interno.

Le Linee Guida hanno integrato la PARTE SPECIALE con presidi e protocolli dedicati alle nuove fattispecie di reato introdotte dopo il 2014 (es. autoriciclaggio, traffico di influenze illecite, reati tributari etc.).

Fonte:
Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231 – Giugno 2021

MODELLO ORGANIZZATIVO 231 INADEGUATO E NON ATTUATO (TRIBUNALE DI VICENZA, SEZIONE PENALE, SENTENZA DEL 17 GIUGNO 2021, N. 348)

È stata depositata il 17 giugno 2021 la sentenza del Tribunale di Vicenza, Sezione Penale, n. 348, con cui la Banca Popolare di Vicenza è stata condannata per i reati di aggiotaggio (ex art. 2637 c.c.), omessa comunicazione del conflitto d'interessi (ex art. 2629-bis c.c.) e ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (ex art. 2638 c.c.) previsti dall'art. 25-ter (Reati societari) del D.Lgs. 231/2001, co. 1, lett. r) e s).

La sentenza stabilisce che il Modello 231 predisposto da BPVi non supera il vaglio di idoneità (con conseguente colpa di organizzazione) sotto plurimi profili:

- assenza di una profilazione dei rischi specifici;
- assenza di indipendenza dei componenti dell'OdV (membro "interno"- Direttore Internal Audit - dipendente funzionalmente e gerarchicamente da soggetti su cui vigilare) o in conflitto di interessi (membri del collegio sindacale con significative interessenze con società collegate alla banca e beneficiari di ingenti retribuzioni) quindi privi di autonomia;
- inidoneità/assenza di flussi informativi (assenza di "procedimentalizzazione del flusso di dati provenienti dalle strutture aziendali afferenti le aree a rischio") necessari "per consentire l'esercizio autonomo del potere di vigilanza";
- assenza di presidi a garanzia della riservatezza del segnalante e a sua tutela.

Il Tribunale afferma poi che il Modello è rimasto nella realtà della banca un esercizio di stile e privo di effettiva attuazione:

- i verbali dell'ODV provano un'attività assolutamente inconsistente dell'OdV limitata a incontri con la funzione compliance ed il collegio sindacale e privo di programmazione di autonoma attività di verifica (delegata e appiattita su quella effettuata dall'internal audit - cioè l'organo dipendente dai controllati);
- assenza di attività formativa;
- mai effettuato alcun intervento sanzionatorio da parte dell'OdV.

In conclusione, un assetto organizzativo lacunoso e le carenze/assenze dei sistemi di controllo rendono inadeguati i presidi a fronte dei rischi, impedendo di fatto anche la loro identificazione e gestione.

Al contrario, sono elementi "premiali" nel giudizio di idoneità del modello e dell'attività di vigilanza – oltre che interessanti spunti operativi- la tracciabilità dell'attività svolta dell'OdV attraverso una sua regolare, completa ed accurata verbalizzazione e la comprovata indipendenza, nella pianificazione delle attività di verifica, da qualsiasi forma di ingerenza da parte di qualsivoglia organo di controllo o di vertice aziendale.

Fonte:
Tribunale di Vicenza, sezione penale, sentenza depositata in data 17 giugno 2021, n. 348

ISTITUZIONE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE: IL PNRR SOSTIENE LA CYBERSICUREZZA QUALE FONDAMENTO DELLA TRASFORMAZIONE DIGITALE

Con il D.L. n. 82/2021 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", pubblicato il 14 giugno 2021, in vigore dal 15 giugno 2021, prosegue la risposta normativa alla messa in sicurezza delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche dei soggetti pubblici e privati da cui possono dipendere malfunzionamenti, interruzioni, totali o parziali, di funzioni essenziali dello Stato e di servizi di pubblica utilità, con conseguente pregiudizio per la sicurezza nazionale.

Tale norma, infatti, segue il percorso delineato dapprima dalle disposizioni legislative del D.L. n. 105/2019, successivamente modificato dal D.L. n. 162/2019 (decreto "Milleproroghe" 2020), e successivamente da quelle attuative con il DPCM 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza, e con il D.P.R. 5 febbraio 2021, n. 54 (che adotta il regolamento approvato dal Consiglio dei Ministri, in data 29 gennaio 2021 - si veda Flash Info Paper marzo 2021, ndr), che ha definito procedure e modalità di valutazione delle acquisizioni, da parte dei soggetti inclusi nel perimetro di sicurezza cibernetica, di oggetti di fornitura e le procedure delle attività di verifica e ispezione.

Sulla spinta della necessità di dare attuazione al Piano Nazionale di Ripresa e Resilienza (PNRR), che prevede apposite progettualità nell'ambito della cybersicurezza, anche al fine di un adeguamento al quadro normativo europeo e di garantire un'unità giuridica dell'ordinamento nazionale, è stata istituita l'Agenzia per la cybersicurezza nazionale che opererà sotto la responsabilità del Presidente del Consiglio dei Ministri e dell'Autorità delegata, se istituita, quale ente di personalità giuridica di diritto pubblico e dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, il cui personale, rivestirà la qualifica di pubblico ufficiale.

L'art. 7 del D.L. n. 82/2021 sancisce le funzioni dell'Agenzia, tra cui quelle attribuite dal D.L. n. 105/2019 alla Presidenza del Consiglio dei Ministri, al Ministero dello Sviluppo Economico, incluse quelle attribuite al Centro di valutazione e certificazione nazionale, le attività di ispezione e verifica all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto di cui all'art. 1, co. 6, lett. c).

Inoltre, il Comitato Interministeriale per la Sicurezza della Repubblica (CISR) viene sostituito dal Comitato Interministeriale per la Cybersicurezza (CIC), istituito presso la Presidenza del Consiglio dei Ministri con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

Infine, l'Agenzia sostituisce anche il Dipartimento delle Informazioni per la Sicurezza, (DIS).

Di fatto, l'Agenzia diventa il principale interlocutore per i soggetti inclusi nel perimetro di sicurezza cibernetica che devono adempiere agli obblighi informativi previsti dal D.L. n. 105/2019 e la cui violazione, configura l'ipotesi di illecito ex D.Lgs. 231/2001 (reato di omessa comunicazione o comunicazione non veritiera di informazioni, dati, elementi di fatto rilevanti in materia di perimetro di sicurezza cibernetica nazionale).

A tal proposito, il D.L. n. 82/2021 stabilisce che tali obblighi di comunicazione (di cui all'art. 1, co. 6, lett. a), D.L. n. 105/2019) saranno efficaci al massimo dal 30 giugno 2022.

Il D.L. n. 82/2021 è stato preceduto dal DPCM 14 aprile 2021, n. 81, pubblicato in data 11 giugno 2021 ed in vigore dal 26 giugno 2021, recante il regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'art. 1, co. 2, lett. b), del D.L. n. 105/2019. Dal 1° gennaio 2022, i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, al verificarsi di uno degli incidenti avente impatto su un bene ICT, devono procedere alla notifica al CSIRT (Computer Security Incident Response Team, istituito presso il DIS). Il provvedimento contiene le tabelle di classificazione degli incidenti e le modalità di segnalazione.

Gli obblighi normativi mirano a garantire un monitoraggio costante dei livelli di sicurezza e misure di intervento immediate alle minacce provenienti dallo spazio cibernetico data la "straordinaria necessità ed urgenza di attuare misure tese a rendere il Paese più sicuro e resiliente anche nel dominio digitale".

Fonte:
Decreto-Legge n. 82/2021, pubblicato in G.U. il 14 giugno 2021

EPPO - EUROPEAN PUBLIC PROSECUTOR'S OFFICE. LA NUOVA PROCURA EUROPEA

La tutela degli interessi finanziari dell'Unione Europea è ormai da tempo argomento di grande attualità.

Con la c.d. Direttiva PIF (Direttiva UE 2017/1371), relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale, è stato già possibile evincere la volontà di adottare degli strumenti volti a contrastare le condotte fraudolente più gravi in ambito tributario e armonizzare il diritto penale degli Stati membri.

Inoltre, dal 1° giugno 2021, dopo una lunga fase preparatoria, è divenuta operativa la Procura europea («EPPO», da European Public Prosecutor's Office), incaricata di vigilare sull'utilizzo dei fondi europei e combattere corruzione e frodi a danno del bilancio dell'UE.

Fino ad ora, infatti, solo le autorità nazionali potevano indagare e perseguire i suddetti crimini (parliamo dei reati contemplati dalla Direttiva PIF), tuttavia, la loro competenza giurisdizionale si fermava al confine del loro Paese. Di fatto, dunque, le procure nazionali disponevano di strumenti limitati per combattere la grande criminalità finanziaria transfrontaliera.

La Procura europea ha sede a Lussemburgo ed è composta da due livelli: il livello centrale costituito dal procuratore capo europeo e da 22 procuratori europei (uno per Paese partecipante), ed il livello locale/decentrato, costituito dai procuratori europei delegati con sede negli Stati membri. Il livello centrale ha il compito di sovraintendere alle indagini e alle azioni penali svolte dai procuratori delegati a livello nazionale, i quali operano in completa indipendenza dalle rispettive autorità nazionali.

Si tratta, dunque, di una nuova procura indipendente dell'Unione Europea che agirà come unico organismo in tutti gli Stati membri partecipanti (ad oggi 22, tra cui l'Italia), operando di concerto con le autorità nazionali e con altri organismi e istituzioni dell'UE (quali OLAF, Eurojust ed Europol).

Fonte:
EPPO

ANTICORRUZIONE

WHISTLEBLOWING: LE NUOVE LINEE GUIDA ANAC

Il 9 giugno 2021, il Consiglio dell'Autorità Nazionale Anticorruzione (ANAC) ha approvato le nuove «Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del D.Lgs. 165/2001 (c.d. whistleblowing)».

Con le Linee Guida, l'ANAC ha voluto fornire indicazioni più precise sulle modalità di applicazione della normativa, rivolgendosi, difatti, alle pubbliche amministrazioni e ad altri enti privati sottoposti al controllo pubblico che sono obbligati a prevedere misure di tutela per il dipendente che segnala comportamenti illeciti.

Le Linee Guida si compongono di tre parti:

1) la prima parte chiarisce e fornisce indicazioni rispetto ai seguenti ambiti:
   - soggetti tutelati (dipendenti pubblici e dipendenti di enti privati che operano nel contesto lavorativo della pubblica amministrazione);
   - enti obbligati a garantire la tutela dei dipendenti autori di segnalazione (pubbliche amministrazioni, enti pubblici economici ed enti di diritto privato sopposti a controllo pubblico);
   - caratteristiche della segnalazione, ovvero il tempo e il luogo in cui si è verificato l'atto oggetto della segnalazione, la descrizione e/o altri elementi che permettono di individuare il soggetto autore dell'illecito;
   - oggetto della segnalazione, che deve indicare le «condotte illecite» di cui il segnalatore è venuto a conoscenza «in ragione del rapporto di lavoro», deve essere fatta per «tutelare l'interesse all'integrità della pubblica amministrazione»;
   - modalità e tempi delle tutele del segnalatore (tutela della riservatezza, da ritorsioni o discriminazioni);
   - esclusione dall'applicazione dell'istituto del whistleblowing e dal sistema di tutele ad esso connesso.
2) la seconda parte definisce il ruolo del responsabile della prevenzione della corruzione e della trasparenza (RPCT), le modalità di ricezione e gestione delle segnalazioni e fornisce indicazioni operative sulle procedure da seguire per il trattamento delle segnalazioni al fine di garantire sicurezza e riservatezza delle informazioni raccolte. Nella seconda parte, in sostanza, l'ANAC rafforza l'utilizzo di modalità informatiche per la ricezione e la gestione delle segnalazioni whistleblowing, avvalendosi di strumenti di crittografia per garantire la riservatezza del segnalante.
3) la terza parte illustra le procedure seguite da ANAC per la gestione delle segnalazioni e per la comunicazione delle misure ritorsive. All'ANAC è riconosciuto, inoltre, uno specifico potere sanzionatorio (ai sensi del comma 6 art. 54-bis).

Tali Linee Guida hanno «carattere transitorio», considerato che potrebbero essere modificate, in un secondo momento, per recepire i contenuti da adottare entro il 17 dicembre 2021 (come previsto dalla Direttiva 2019/1937 «riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione»).

Fonte:
Delibera numero 469 del 9 giugno 2021- ANAC

PRIVACY

NUOVE LINEE GUIDA DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI IN TEMA DI COOKIE

In data 10 giugno 2021 il Garante per la protezione dei dati personali ha aggiornato le precedenti linee guida in materia di cookie, al fine di rafforzare il potere decisionale degli utenti circa l'uso dei propri dati personali durante la navigazione. Innanzitutto alcune interessanti novità lato **informative**, atteso che:

- dovranno necessariamente riportare i vari tempi di conservazione dei dati degli utenti ed indicare eventuali altri soggetti destinatari di tali informazioni;
- potranno essere rese su più canali e con diverse modalità (ad esempio video, pop up, ecc.);
- ne è stata formalmente ribadita l'obbligatorietà con riferimento ai soli cookie tecnici.

Ulteriori chiarimenti sono stati forniti in tema di cookie di profilazione, in relazione ai quali è stata evidenziata la necessità di:

- richiedere apposito consenso attraverso un banner che sia ben distinguibile sulla pagina web;
- offrire agli utenti di proseguire la navigazione senza essere in alcun modo «tracciati» (ad es. chiudendo il banner attraverso un click sulla X- in alto a destra-).

In materia di acquisizione del consenso, il Garante ha altresì precisato che:

- lo «scrolling» – inteso come il semplice spostamento in basso del cursore – non può essere utilizzato come strumento esclusivo di acquisizione del consenso. È infatti necessario che esso sia inserito, dal titolare del sito, in un ampio contesto di alternative, dove la scelta dell'utente risulti inequivocabile e consapevole, al fine di evitare i c.d. «falsi positivi».
- i «cookie wall» – meccanismo vincolante attraverso il quale l'utente viene obbligato ad esprimere il proprio consenso alla ricezione dei cookie – sono illegittimi, salvo le ipotesi in cui il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalente senza prestare il proprio consenso;
- la ripresentazione del banner per l'acquisizione del consenso ad ogni nuovo accesso – agli utenti che in precedenza l'abbiano negato - lede la libertà degli interessati, prima o poi inducendoli a prestarlo pur di proseguire la navigazione in modo più «agevole». La scelta degli utenti dovrà dunque essere registrata e non più sollecitata, a meno che:
  1. non mutino significativamente le condizioni del trattamento;
  2. sia impossibile sapere se un cookie sia già memorizzato nel dispositivo;
  3. siano trascorsi almeno sei mesi.

Infine, il Garante raccomanda che i **cookie analytics**, usati per valutare l'efficacia di un servizio, siano utilizzati solo a scopi statistici.

Fonte:

Linee Guida - GDPD

IL GARANTE SANZIONA IL COMUNE DI BOLZANO PER CONTROLLO INDISCRIMINATO DEI LAVORATORI

In data 13 maggio 2021 il Garante per la protezione dei dati personali ha emanato un'ordinanza di ingiunzione nei confronti del Comune di Bolzano, in seguito ad un reclamo posto in essere da un dipendente avverso un provvedimento disciplinare con il quale gli era stato contestato dal proprio datore un utilizzo «extra lavorativo» del pc aziendale.

Il ricorrente lamentava:

- la violazione della disciplina della protezione dei propri dati personali da parte dell'Ente, a causa di un illegittimo monitoraggio del traffico di rete e dei singoli accessi ad internet;
- l'assenza di una specifica informativa dipendenti sulla gestione dei dati di navigazione.

Il Comune si era difeso rappresentando di aver fornito ai dipendenti – sia pur anteriormente all'entrata in vigore del GDPR – un'informativa generale sul trattamento dei dati personali e di averne poi predisposta un'altra, aggiornata.

Dall'attività istruttoria era però emerso che il Comune:

- non avesse in realtà pubblicato alcuna informativa aggiornata sul proprio sito web;
- facesse ricorso ad un sistema di controllo e filtraggio dei dati di navigazione dei dipendenti, memorizzandone i dati di dettaglio – anche non attinenti alla prestazione lavorativa - per un mese.

Tanto brevemente premesso, l'Autorità ha concluso l'istruttoria evidenziando che l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet non può portare al completo annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, neanche nei casi in cui il dipendente utilizzi i servizi di rete messi a disposizione del datore.

Oltre al pagamento della sanzione pecuniaria – pari ad 84 mila euro – è stato intimato al Comune di:

- adottare misure tecniche ed organizzative per anonimizzare il dato relativo alla postazione di lavoro dei dipendenti;
- cancellare i dati personali presenti nei log di navigazione web registrati;
- aggiornare lato privacy le procedure interne individuate e inserite nell'accordo sindacale.

Fonte:

Ordinanza ingiunzione nei confronti di Comune di Bolzano- GDPD

GIURISPRUDENZA

L'INTERESSE DELLA SOCIETÀ PER IL CONSEGUIMENTO DI UN INDEBITO PROFITTO AI DANNI DELLO STATO (CASS. PEN. SEZ. II, 15 GIUGNO 2021, N. 23300)

Una recente sentenza della Corte di Cassazione penale (Sez. II, Sent., [ud. 23 aprile 2021] 15 giugno 2021, n. 23300) ha ulteriormente sviluppato il principio cardine dell'interesse e vantaggio normato dal D.Lgs. 231/2001.

La vicenda giudiziale trae origine dalla condanna di una società per il delitto di riciclaggio commesso dai suoi amministratori avendo la stessa, secondo i giudici di merito, beneficiato dell'indebito profitto ottenuto dal reato (truffa ai danni dello Stato). In sede di ricorso, la società sosteneva la mancanza di responsabilità dell'ente, lamentando la mancata prova dell'interesse della società alla condotta illecita e l'invalidità del nesso tra la truffa e gli interessi della società stessa.

Giudicando infondato il ricorso, la Corte di Cassazione argomenta che il diretto interesse della società alla realizzazione della truffa è provato dal fatto che il ricavo del reato è stato impiegato dall'ente per la costruzione di un impianto industriale.

La difesa, inoltre, avanzava la tesi dell'attribuzione ai soci (imputabili del reato) di un interesse concorrente rispetto a quello della società. Anche per questa proposta, tuttavia, l'argomentazione è risultata infondata in quanto la sussistenza della responsabilità da reato dell'ente si concretizza qualora la persona giuridica abbia avuto un interesse anche solo concorrente con quello dell'agente alla commissione del reato presupposto (Cass., sez. VI, 22 maggio 2013, n. 24559). Dunque, l'interesse dell'autore del reato può anche solo coincidere con quello dell'ente, a cui potrà essere trasferita la responsabilità anche quando l'agente, perseguendo il proprio autonomo interesse, finisca per realizzare quello dell'ente (Cass., sez. V, 28 novembre 2013, n. 10265).

Tuttavia, l'interesse ha comunque un ruolo marginale in questa decisione, in quanto è stato accertato che la società abbia tratto vantaggio concreto dai finanziamenti illeciti, utilizzati per il completamento di nuove strutture.

Fonte:
Cass. pen. Sez. II, Sent., [ud. 23 aprile 2021] 15 giugno 2021, n. 23300; Cass., sez. VI, 22 maggio 2013, n.24559; Cass., sez. V, 28 novembre 2013, n. 10265.

RESPONSABILITÀ EX D.LGS. 231/2001 IN CASO DI ESTINZIONE FRAUDOLENTA DELL'ENTE (CASS. PEN. SEZ. V, 5 LUGLIO 2021, N. 25492)

Una recente sentenza della Corte di Cassazione penale (Sez. V, Sent., [ud. 27 aprile 2021] 5 luglio 2021, n. 25492) ha fatto chiarezza sull'applicazione della responsabilità ex D.Lgs. 231/2001 in caso di trasferimento fraudolento delle attività di una società, in favore di un altro ente.

La vicenda giudiziale, sottoposta al vaglio di legittimità della Corte di Cassazione, presentava una doppia condanna ex D.Lgs. 231/2001 di una società, successivamente oggetto di trasferimento e cessazione.

Approfittando dello scioglimento dell'ente a cui inizialmente era contestato l'illecito amministrativo, la difesa aveva chiesto sia l'estinzione dell'illecito sia la nullità della nomina del difensore di fiducia, in quanto il legale rappresentante era imputato del reato presupposto. Dunque, secondo la difesa, già i giudici di merito avrebbero dovuto ritenere estinto l'illecito, in quanto l'ente in discussione risultava essere sciolto.

La Corte di Cassazione ha, tuttavia, respinto il ricorso poiché, se la cessazione dell'attività d'impresa risulta fraudolenta e ha come fine quello di eludere l'applicazione del D.Lgs. 231/2001, l'illecito amministrativo non può considerarsi estinto. Sulla base di questo principio, la Cassazione ha dichiarato inammissibili i motivi di ricorso.

La giurisprudenza ha puntualizzato che "l'estinzione dell'illecito previsto dal D.Lgs. 8 giugno 2001, n. 231 consegue all'estinzione fisiologica e non fraudolenta dell'ente, giacché solo nel primo caso ricorre un caso assimilabile alla morte dell'imputato" (Cass. pen, Sez. 2, n. 41082 del 10/09/2019, Rv. 2771070). In questo caso, tuttavia, la cessazione dell'attività era finalizzata all'elusione dell'illecito e trova quindi applicazione l'art. 33 del D.Lgs. n. 231/2001 che prevede la responsabilità solidale del cessionario dell'azienda (Cass. pen. Sez. V, 5 luglio 2021, n. 25492).

In conclusione, l'ente non risulta quindi responsabile diretto del reato, bensì responsabile solidale, configurandosi in tal modo l'obbligo del pagamento della sanzione pecuniaria.

Fonte:
Cass. pen. Sez. V, Sent., [ud. 27 aprile 2021] 5 luglio 2021, n. 25492; Cass. pen. Sez. 2, n. 41082 del 10/09/2019, Rv. 2771070.

LIMITI APPLICATIVI DEL D.LGS. 231/2001 ALLE IMPRESE INDIVIDUALI (TRIBUNALE DI RAVENNA, SENTENZA DEL 7 GIUGNO 2021, N. 1056)

Nel testo della sentenza n. 1056 del 7 giugno 2021, il giudice unico del Tribunale di Ravenna ha verificato se la disciplina del D.Lgs. 231/2001 fosse applicabile alle imprese individuali.

Secondo il principio contenuto nell'art. 12 delle Disposizioni sulla legge in generale, l'interprete dovrebbe prediligere l'esegesi letterale del disposto normativo contenuto nell'art. 1 del Decreto, nella parte in cui si evince *«Il presente decreto legislativo disciplina la responsabilità degli enti»*. Il giudice ha concluso, seguendo il criterio dell'interpretazione letterale, che le imprese individuali sono escluse del novero dei soggetti destinatari della disciplina, in quanto trattasi di una categoria non definita dal punto di vista normativo a differenza delle società e delle associazioni.

Lo stesso legislatore aveva chiarito, all'interno della Relazione di accompagnamento al decreto, che la scelta dell'ente deve essere letta in sinergia con la espressa indicazione di soggetti nominati di guisa da *«indirizzare l'interprete verso la considerazione di enti che, seppur sprovvisti di personalità giudica, possano ottenerla»*. Quindi, il discrimine deve essere individuato in tutti quei soggetti giuridici meta-individuati che siano degli autonomi centri di imputazione di rapporti giuridici, destinatari degli atti compiuti dalla persona fisica che agisca nel loro interesse od a loro vantaggio.

In proposito, l'orientamento maggioritario della Corte di Cassazione sostiene che la disciplina prevista dal D.Lgs. 231/2001 non si applica alle imprese individuali, in quanto riferita ai soli enti collettivi (Cass. 18941/2012 e Cass. 18941/2004). Vi sarebbe, inoltre, una pronuncia isolata della Cassazione che sostiene la tesi contraria, ovvero le imprese individuali, ancorché non siano espressamente menzionate dall'art. 1 del Decreto, devono ricondursi alla generale categoria degli enti forniti di personalità giuridica, nonché di società e associazioni anche prove di personalità giuridica (Cass. 15657/2010).

Il Tribunale di Ravenna ha ritenuto condivisibile l'orientamento maggioritario della Cassazione, dovendo escludere che l'impresa individuale sia destinataria della disciplina ex D.Lgs. 231/2001, poiché essa si applica ai soli soggetti meta-individuati. Di fatto, nell'impresa individuale, imprenditore ed attività coincidono e, stante l'assenza di una scissione soggettiva tra persona fisica e soggetto meta-individuale, con l'applicazione all'impresa individuale del D.Lgs. 231/2001, si finirebbe per dar luogo ad una doppia punizione del medesimo soggetto per il medesimo fatto, con violazione del principio *ne bis in idem* sostanziale: la persona fisica sarebbe punito quale autore materiale del reato e quale titolare dell'impresa che si immedesima con lui.

Fonte:
Tribunale di Ravenna, Sentenza depositata in data 7 giugno 2021, n. 1056

Contatti:
BDO Italia S.p.A.
ras@bdo.it

Viale Abruzzi, 94
20131 Milano
Tel: 02 58 20 1

BDO è tra le principali organizzazioni internazionali di revisione e consulenza aziendale con oltre 91.000 professionisti altamente qualificati in più di 167 paesi. In Italia BDO è presente con circa 1.000 professionisti con una struttura integrata e capillare che garantisce la copertura del territorio nazionale.

www.bdo.it