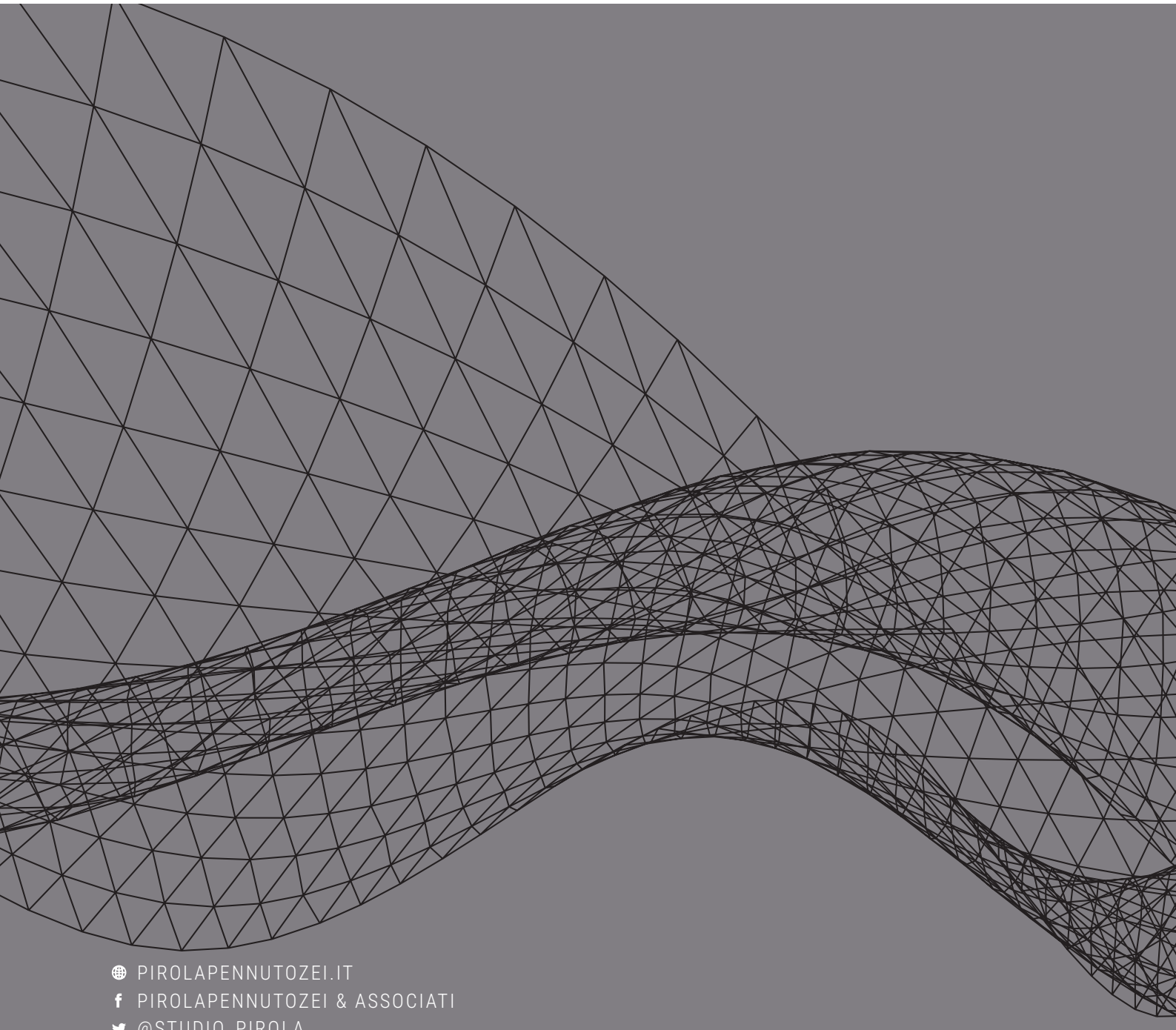
Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

COMPLIANCE

NEWSLETTER / MARZO 2018



PIROLAPENNUTOZEI.IT
PIROLAPENNUTOZEI & ASSOCIATI
@STUDIO_PIROLA
PIROLA PENNUTO ZEI & ASSOCIATI

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDICE

NORMATIVA

PRASSI

GIURISPRUDENZA

TORNA ALL'INDICE ↑

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDICE

NORMATIVA

1.1

GDPR, disco verde in Consiglio dei ministri

Il Consiglio dei Ministri del 21 marzo scorso ha approvato in esame preliminare uno schema di decreto legislativo, che ha dato attuazione all'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), pubblicata in Gazzetta Ufficiale il 6 novembre ed entrata in vigore il successivo 21 novembre.

Con tale provvedimento il Legislatore conferisce delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 in materia di trattamento dei dati personali delle persone fisiche e di libera circolazione di tali dati.

Il Consiglio dei Ministri è quindi intervenuto in attuazione della delega ricevuta dal Parlamento, scegliendo di abrogare, come espressamente disposto all'art. 101 dello schema di decreto approvato, l'attuale Codice per la protezione dei dati personali (D. Lgs. 196/2003). Tale scelta rappresenta la volontà di conferire maggiore chiarezza al *corpus* normativo in materia di protezione dei dati personali, ora costituito, da un lato, dalle disposizioni del Regolamento direttamente applicabili e, dall'altro, dalle disposizioni contenute nello schema di decreto legislativo approvato in via provvisoria.

Tra le disposizioni contenute nel provvedimento approvato dal Consiglio dei Ministri risultano di particolare interesse:

- l'art. 14, rubricato "*Attribuzione di funzioni e compiti a soggetti designati*", che prevede il potere del responsabile e del titolare del trattamento di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità, così potendo mantenere le funzioni attribuite a figure interne all'organizzazione che, ai sensi della previgente normativa, ma in contrasto con il Regolamento (UE) 2016/679, erano definiti "*incaricati*";
- gli artt. 88 e 93, che disciplinano secondo disposizioni rimaste immodificate rispetto alla previgente disciplina, le modalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale;

- l'art. 90, che disciplina la "*Conservazione dei dati di traffico per altre finalità*", che prevede un termine di conservazione di 24 e 12 mesi rispettivamente per finalità di accertamento e repressione di reati;
- l'art. 97 sulle "*Autorizzazioni del Garante*", con il quale viene stabilito un termine di 90 giorni dalla data di entrata in vigore dello schema di decreto per la valutazione di adeguatezza delle autorizzazioni attualmente in essere in relazione al teso del Regolamento (UE) 2016/679. La medesima attività di riesame dovrà peraltro essere svolta anche in relazione ai provvedimenti resi nel corso del tempo dal Garante;
- l'art. 98, rubricato "*Altre disposizioni transitorie*", che reca una clausola interpretativa a valenza generale, con la quale si specifica che i richiami contenuti in norme di legge o regolamenti a disposizioni del D. Lgs. 196/2003 debbano essere riferiti alle corrispondenti disposizioni del Regolamento (UE) 2016/679.

Il Legislatore delegato è poi intervenuto anche in materia di sanzioni penali, optando per l'abrogazione di alcune di esse poiché sarebbero potenzialmente sovrapponibili a quelle amministrative dettate ai sensi del Regolamento (UE) 2016/679 e, quindi, in violazione del principio del "*ne bis in idem*".

PRASSI

2.1

Sicurezza sul lavoro: pubblicata la norma ISO 45001:2018

Con la pubblicazione avvenuta il 12 marzo scorso si è concluso l'*iter* di approvazione del nuovo *standard* della norma ISO 45001 sui sistemi di gestione per la salute e la sicurezza sul lavoro.

La norma ("*Occupational Health & Safety Management Systems – Requirements with guidance for use*") mantiene la stessa struttura degli standard dei sistemi di gestione ISO 9001 e ISO 14001; le aziende che sono certificate OHSAS 18001: 2007 dovranno tuttavia cambiare i loro sistemi di gestione per la salute e la sicurezza sul lavoro, adattandoli alla nuova ISO, entro marzo 2021.

2.2

Transparency International: guida alle migliori pratiche legislative sul ***whistleblowing***

Transparency International ha diffuso la prima Guida di supporto alle legislazioni nazionali in materia di *whistleblowing,* indicando le *best practice* adottate e una serie di principi basilari che non dovrebbero essere disattesi, fra cui, in primo luogo, l'efficace protezione dei segnalanti, elemento fondamentale per il corretto funzionamento del sistema.

Quello della tutela del segnalante, d'altra parte, è un concetto ormai ratificato in tutti i trattati internazionali: Convenzione delle Nazioni Unite contro la corruzione (articoli 8, 13 e 33); Convenzioni del Consiglio d'Europa in materia civile e penale sulla corruzione (rispettivamente articoli 9 e 22); Convenzione Inter-americana contro la corruzione (articolo III, paragrafo 8); Convenzione dell'Unione africana sulla prevenzione e la lotta alla corruzione (articolo 5, paragrafo 6); Convenzione araba contro la corruzione (articolo 10, paragrafo 6), trattati cui le varie legislazioni nazionali si sono conformate, pur con le inevitabili differenze legate agli aspetti giuridici (sostanziali e procedurali) propri di ogni sistema.

Nonostante ciò, "*ad oggi – spiega la Guida – nessuna legge sul whistleblowing è pienamente allineata con i 30 principi di Transparency International. Di fatto, tutte le leggi nazionali esistenti sulla protezione degli informatori hanno ancora lacune*".

Per quanto riguarda il caso italiano, la disciplina sul *whistleblowing,* pur molto recente, disattende una serie di punti importanti dell'istituto, sottoponendosi a numerose critiche. Il riferimento va ad esempio a un sistema perimetrato in ambito privato alle società con Modello "*231*", per i soli reati presupposto della responsabilità amministrativa degli enti e utilizzabile esclusivamente da "*apicali e sottoposti*".

Non è stato poi introdotto alcun sistema premiante (principio n. 23), né individuata un'autorità istituzionale di riferimento, com'è l'A.N.AC. per il mondo pubblico (principio n. 28).

2.3

Nuove Faq del Garante sul *Data Protection Officer* (DPO) in ambito privato

Dopo la pubblicazione delle Faq relative al *Data Protection Officer* (DPO) in ambito pubblico, avvenuta lo scorso 15 dicembre 2017, il Garante *Privacy* torna a pronunciarsi sul tema, fornendo nuove indicazioni per la nomina del DPO, questa volta in ambito privato.

Sono quindi state pubblicate lo scorso 26 marzo le risposte alle otto domande più frequenti formulate da parte degli operatori. Il Garante ha così cristallizzato il proprio orientamento in materia, anche in relazione ai principi che aveva chiarito il Gruppo di Lavoro ex art. 29 dei Garanti Europei.

La prima risposta serve a inquadrare la figura: si ribadisce che il DPO avrà funzioni di supporto e di controllo, consultive, formative e informative relativamente all'applicazione del Regolamento, coopererà con l'Autorità (il suo nominativo va, infatti, comunicato al Garante) e costituirà il punto di contatto anche rispetto agli interessati. Si tratta, quindi, di una figura complessa, con molte funzioni che dovranno essere necessariamente coordinare tra loro per dar vita a un quadro armonioso.

La seconda considerazione specifica i requisiti che questa figura deve avere. Non è, quindi, necessario che sia iscritto ad albi o che abbia ricevuto particolari attestazioni formali, ma deve conoscere normativa e prassi e le regole dell'ambiente nel quale si trova a lavorare. Deve, poi, agire in piena autonomia e indipendenza, senza ricevere istruzioni e riferendo direttamente ai vertici, ed essere dotato di un ufficio e di risorse per l'espletamento reale dei suoi compiti.

Il terzo punto riguarda il delicato aspetto dell'obbligatorietà della designazione. Secondo l'intendimento del Garante saranno i soggetti che come "*core business*", cioè come attività principale, pongono in essere trattamenti che richiedano il monitoraggio regolare e sistematico degli interessati su larga scala, o trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e reati, a dover nominare un DPO. A questo proposito vengono formulati una serie di esempi con riferimento alle categorie obbligate alla nomina, indicando istituti di credito, imprese assicurative, sistemi di informazione creditizia, società finanziarie, società di informazioni commerciali, società di revisione contabile, società di recupero crediti, istituti di vigilanza, partiti e movimenti politici, sindacati, CAF e patronati, società operanti nel settore delle "*utilities*" (telecomunicazioni, distribuzione di energia elettrica o gas), imprese di somministrazione di lavoro e ricerca del personale, società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione, società di *call center,* società che forniscono servizi informatici e società che erogano servizi televisivi a pagamento.

Quanto invece ai soggetti non obbligati alla nomina, nelle FAQ si fa cenno a trattamenti effettuati da liberi professionisti operanti in forma individuale, ad agenti, rappresentanti e mediatori operanti non su larga scala, ad imprese individuali o familiari, a piccole e medie imprese con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

Tuttavia, viene comunque suggerita, in un'ottica di responsabilizzazione, la nomina del DPO anche nel caso in cui il Titolare o il Responsabile del trattamento non siano gravati da tale obbligo, nell'ottica di garantire un più alto livello di sicurezza.

La quinta regola precisa come un gruppo imprenditoriale possa designare un unico *Data Protection Officer*, purché sia facilmente raggiungibile da ciascuno stabilimento, sia in grado di comunicare in modo efficace con gli interessati e, soprattutto, sia in grado di collaborare con le autorità di controllo.

Viene poi evidenziato come il ruolo di *Data Protection Officer* possa essere ricoperto da un dipendente del titolare o del responsabile, purché non in conflitto di interessi che conosca la realtà operativa in cui avvengono i trattamenti. Al contempo, l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento assegna a tale figura. La scelta tra DPO "*interno*" o "*esterno*" è quindi liberamente demandata alla volontà del Titolare o del Responsabile del trattamento.

Il *Data Protection Officer* scelto all'interno andrà nominato mediante uno specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. L'atto, da redigere in forma scritta, dovrà indicare espressamente i compiti attribuiti, le risorse assegnate per lo svolgimento dell'incarico, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Nell'esecuzione dei compiti, il *Data Protection Officer,* interno o esterno che sia, dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il Titolare o il Responsabile del trattamento che abbia designato un DPO resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla. La nomina di un DPO, infatti, non solleva il Titolare da alcuna responsabilità in relazione al trattamento dati effettuato, che rimane comunque sempre in capo ai vertici societari.

La settima risposta precisa come il ruolo di DPO sia compatibile con altri incarichi, a condizione che non sia in conflitto di interessi. In tale prospettiva appare preferibile, nota il Garante, evitare di assegnare il ruolo di *Data Protection Officer* a soggetti con incarichi di alta direzione (amministratore delegato, membro del consiglio di amministrazione, direttore generale, ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione *marketing,* direzione finanziaria, responsabile IT ecc.). Da valutare con attenzione, secondo il Garante, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione dell'incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

Quanto, infine, alla figura di "*persona fisica*" o "*persona giuridica*" in capo al DPO, le FAQ chiariscono come il Regolamento preveda espressamente che il *Data Protection Officer* possa essere anche un "*dipendente*" del Titolare o del Responsabile del trattamento, mentre, qualora il *Data Protection Officer* sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica.

2.4

Garante *Privacy,* no allo *spam* sulle Pec dei liberi professionisti

Il Garante per la *privacy* ha vietato a una società e ad un'associazione ad essa collegata l'invio senza consenso di e-mail promozionali a liberi professionisti, attraverso l'indirizzo di posta elettronica certificata.

Dalle verifiche è emerso che alcuni collaboratori volontari dell'Associazione e una società terza avevano reperito *on line* massivamente gli indirizzi Pec di avvocati e, in minor parte, di commercialisti, revisori contabili, consulenti del lavoro e notai, in violazione dei fondamentali principi di finalità, liceità e correttezza del trattamento dei dati personali.

La società aveva poi spedito agli indirizzi di più di 800.000 professionisti diverse e-mail, contenenti la notizia della pubblicazione di un bando di selezione per "*consulente reputazionale*", l'invito a partecipare ad un *webinar* e articoli relativi alla società mittente.

Oltre ad essere stati trattati senza consenso, gli indirizzi Pec erano stati reperiti in modo illecito dal registro Ini-Pec, l'Indice nazionale dei domicili digitali, dal sito www.registroimprese.it e dagli elenchi pubblicati da alcuni ordini provinciali. La normativa stabilisce, infatti, che l'estrazione di indirizzi di posta elettronica certificata contenuti nel registro delle imprese o negli albi o elenchi "*è consentita alle sole pubbliche amministrazioni per le comunicazioni relative agli adempimenti amministrativi di loro competenza*". In un caso le e-mail risultavano inviate anche dopo che il destinatario si era già opposto formalmente al trattamento dei suoi dati personali, esercitando i diritti previsti dal Codice *privacy.*

A nulla sono valse le giustificazioni addotte dalla società e dall'associazione, le quali, tra l'altro, si ritenevano esentate dalla richiesta del consenso preventivo sulla base della presunta natura "*istituzionale*" delle comunicazioni. Le *e-mail* infatti, come ha chiarito il Garante, avevano carattere promozionale, in quanto favorivano le attività dell'associazione connesse alla figura di "*consulente reputazionale*" e dunque avrebbero dovuto essere inviate nel rispetto delle regole previste dal Codice *privacy* e delle Linee guida del Garante in materia di attività promozionale e contrasto allo *spam*. L'Autorità ha vietato, di conseguenza, alla società e all'associazione l'ulteriore illecito trattamento dei dati dei professionisti e ne ha prescritto la cancellazione, riservandosi di valutare eventuali profili sanzionatori.

2.5
Vietato il controllo massivo e la conservazione illimitata delle email

L'autorità Garante per la Protezione dei Dati personali ha vietato ad una società il trattamento effettuato sulle email aziendali dei dipendenti in violazione della normativa sulla protezione dei dati e di quella sulla disciplina lavoristica.

L'Autorità ha accertato che la società trattava in modo illecito i dati personali contenuti nelle email in entrata e in uscita, anche di natura privata, scambiate dal lavoratore con alcuni colleghi e collaboratori. I dati raccolti nel corso di un biennio erano poi stati utilizzati per inviare una contestazione disciplinare cui era seguito il provvedimento del licenziamento del dipendente, poi annullato dal giudice del lavoro.

Nel disporre il divieto l'Autorità ha rilevato come la società non avesse fornito ai dipendenti alcuna informazione sulle modalità e le finalità di raccolta e conservazione dei dati, né con una informativa individualizzata, né attraverso la *policy* aziendale, attività in netto contrasto con l'obbligo della società di informare i lavoratori riguardo alle caratteristiche essenziali dei trattamenti effettuati. La società, inoltre, conservava in modo sistematico i dati esterni e il contenuto di tutte le email scambiate dai dipendenti non solo per l'intera durata del rapporto di lavoro, ma anche dopo la sua interruzione, violando così i principi di liceità, necessità e proporzionalità stabiliti dal Codice *privacy.*

Secondo il Garante la società, anziché mettere in atto un trattamento così invasivo, avrebbe dovuto predisporre dei sistemi di gestione documentale in grado di individuare selettivamente i documenti da archiviare. Il mancato rispetto di tali principi, comportando la conservazione estesa e sistematica delle mail, la loro memorizzazione per un periodo indeterminato, nonché la possibilità per il datore di lavoro di accedervi per finalità non indicate in modo chiaro e puntuale, " *… consente il controllo dell'attività dei dipendenti. Controllo vietato dalla disciplina di settore che non autorizza, verifiche massive, prolungate e indiscriminate. Il datore di lavoro infatti pur potendo controllare l'esatto adempimento della prestazione e il corretto uso degli strumenti di lavoro deve sempre salvaguardare la libertà e la dignità dei dipendenti.*"

Il Garante ha ritenuto, infine, non conforme alla legittima aspettativa di riservatezza della corrispondenza l'accesso della società alle email in ingresso sull'*account* aziendale dopo il licenziamento del lavoratore. Al cessare del rapporto di lavoro la casella di posta elettronica deve essere, infatti, necessariamente disattivata e rimossa e al suo posto si devono attivare eventuali account alternativi.

GIURISPRUDENZA

3.1

Whistleblowing: l'anonimato è solo riserbo sulle generalità

Con la sentenza n. 9047/2018, la Cassazione ha avuto modo di pronunciarsi per la prima volta in tema di *whistleblowing* dopo la pubblicazione della l. n. 179/2017. Benché la pronuncia interessi l'ambito pubblico, essa offre comunque utili spunti di riflessione anche per il settore privato.

Nel caso in esame, infatti, la Cassazione ha rigettato il ricorso cautelare presentato da un dipendente dell'Agenzia delle Entrate indagato per truffa aggravata, falso ideologico in atti informatici e corruzione per atti contrari a doveri d'ufficio, confermando il quadro accusatorio che traeva origine da una segnalazione anonima presentata da un collega.

A nulla è valso per il dipendente eccepire l'inutilizzabilità della denuncia in quanto non autografa. Nello specifico, l'indagato lamentava la validità dell'ordinanza cautelare fondata sulle dichiarazioni rese dal *whistleblower,* senza che questi avesse reso sommarie informazioni in qualità di testimone, in applicazione di quanto stabilito ai sensi dell'art. 203 primo comma c.p.p.

La Cassazione ha invece sottolineato come l'esposto fosse pienamente utilizzabile, perché l'autore era stato identificato, benché considerato dal GIP alla stregua di un anonimo. Infatti, il canale di *whistleblowing* di cui all' art.54-*bis* del D.lgs. 165/2001 (Testo Unico sul Pubblico Impiego) realizza un sistema che garantisce la riservatezza del segnalante nel senso che il dipendente che utilizza una casella di posta elettronica interna al fine di segnalare eventuali abusi non ha necessità di firmarsi, ma effettua pur sempre la segnalazione attraverso le proprie credenziali ed è quindi individuabile, seppur protetto.

Inoltre, il segnalante non era rimasto anonimo nel corso del processo penale e non poteva pertanto essere classificato come informatore, le cui dichiarazioni sono utilizzabili solo se cristallizzate in sommarie informazioni o esame dibattimentale.

Ne è quindi conseguita la conferma dell'ordinanza cautelare che ritiene sussistenti gravi indizi di colpevolezza a carico dell'indagato sulla base della segnalazione di un *whistleblower* che non abbia reso sommarie informazioni testimoniali nell'ambito del procedimento penale.

3.2

La tenuità del fatto non si estende all'ente

Con la sentenza n. 9072/2018 la Cassazione è intervenuta per chiarire se sussista la responsabilità dell'ente ex D. Lgs. 231/2001 anche nell'ipotesi in cui all'imputato venga riconosciuta la particolare tenuità del fatto. La questione, infatti, non trova espressa regolamentazione normativa.

A parere degli Ermellini, l'ente deve essere giudicato in ragione del principio di autonomia sancito dall'articolo 8 del Decreto, sia per la natura della causa di non punibilità.

D'altra parte la sentenza che applica questo istituto – scrivono i giudici – "e*sprime un'affermazione di responsabilità, pur senza condanna, e pertanto non può assimilarsi ad una sentenza di assoluzione, ma lascia intatto il reato nella sua esistenza, sia storica sia giuridica*".

Ne discende che, in tema di responsabilità "*231*", "*in presenza di una sentenza di applicazione della particolare tenuità del fatto nei confronti della persona fisica responsabile della commissione del reato, il giudice deve procedere all'accertamento autonomo della responsabilità amministrativa delle persone giuridiche nel cui interesse e nel cui vantaggio il reato fu commesso*".

Pirola
Pennuto
Zei
& Associati
studio di consulenza
tributaria e legale

Via Vittor Pisani, 20
20124 Milano

T. +39.02.669951
F. +39.02.6691800

info@studiopirola.com
www.pirolapennutozei.it

COMPLIANCE NEWSLETTER | MARZO 2018

RIFERIMENTI NORMATIVI, PRASSI E GIURISPRUDENZA AL 31 MARZO 2018.
LA PRESENTE NEWSLETTER ILLUSTRA LE PRINCIPALI NOVITÀ E ALCUNE QUESTIONI DI INTERESSE GENERALE, E RAPPRESENTA DUNQUE UNO STRUMENTO MERAMENTE INFORMATIVO, IL CUI CONTENUTO NON VA UTILIZZATO COME BASE PER EVENTUALI DECISIONI OPERATIVE.
PER ULTERIORI INFORMAZIONI, VI INVITIAMO A CONTATTARE IL VOSTRO PARTNER DI RIFERIMENTO O AD INVIARE UN'EMAIL A UFFICIOSTUDI@STUDIOPIROLA.COM