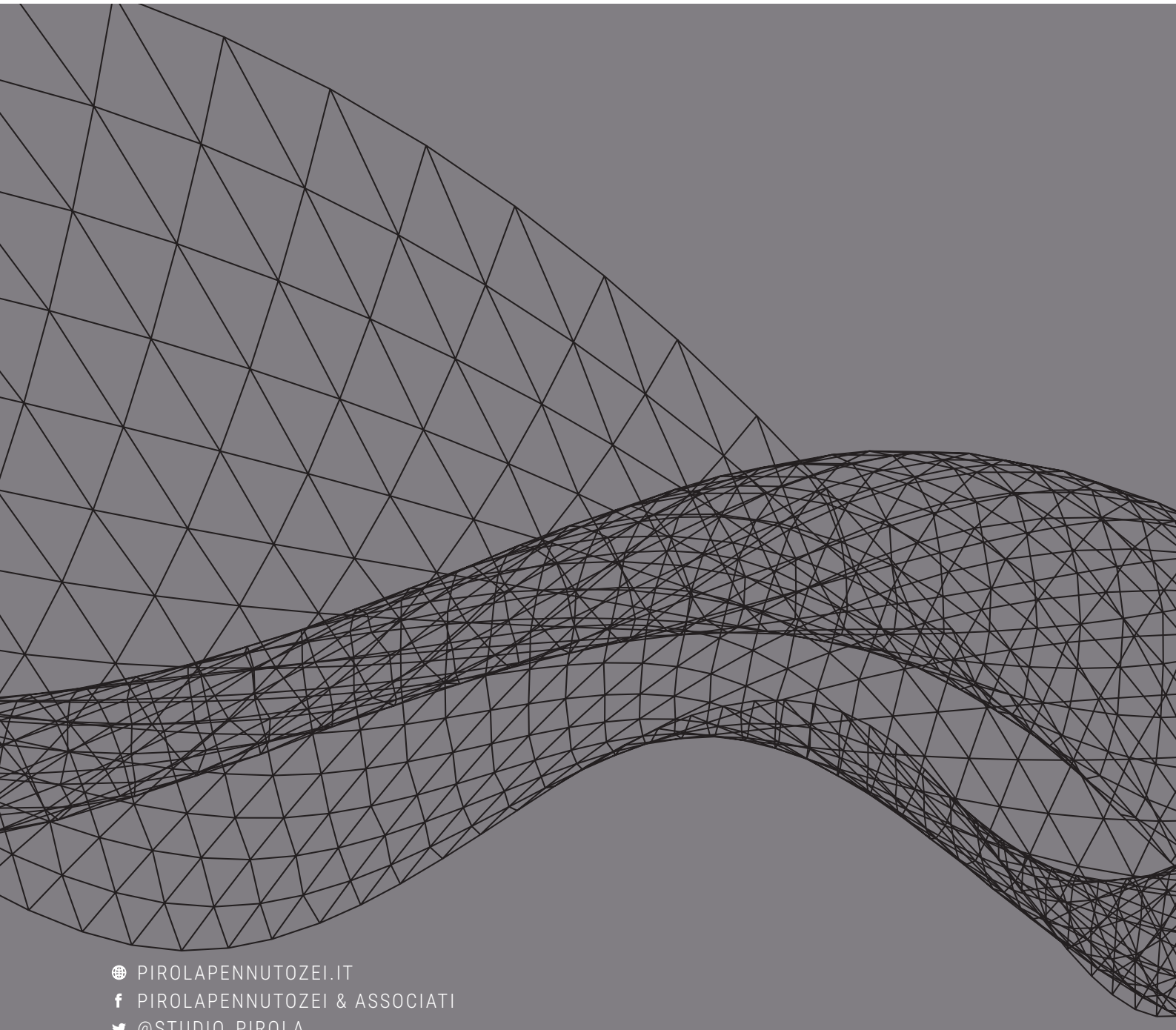
Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

COMPLIANCE

NEWSLETTER / AGOSTO 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 ↑

NORMATIVA

1.1
Nuovo Codice Privacy: Pubblicato in Gazzetta Ufficiale il D.lgs. 101/2018

Il nuovo codice della privacy, che adegua la normativa italiana alle disposizioni del Regolamento Generale sulla protezione dei dati N. 2016/679, è stato pubblicato in Gazzetta Ufficiale in data 4 settembre 2018 ed entrerà in vigore a far data 19 settembre 2018.

Il Decreto in commento prevede che, per un periodo transitorio, continuino ad essere efficaci i provvedimenti e le autorizzazioni generali del Garante, nonché i Codici deontologici vigenti.

Dalla lettura della norma si evince, anche, che il sistema sanzionatorio penale è stato arricchito con l'introduzione di nuove fattispecie di reato. Inoltre è affidato al Garante per la protezione dei dati personali il compito di dettare delle specifiche regole per l'applicazione delle sanzioni amministrative e promuovere modalità semplificate di adempimento degli obblighi per le PMI.

1.2
Il Brasile approva la nuova legge sulla privacy ispirata ai principi del GDPR

Il 14 agosto 2018 il Brasile ha approvato la legge No. 13,709 in materia di protezione dei dati personali al fine di regolamentare il trattamento degli stessi nel settore pubblico e privato.

Ai sensi della nuova normativa, gli enti pubblici e privati potranno trattare solo i dati personali che sono strettamente necessari per l'erogazione dei propri servizi. I destinatari della norma saranno sottoposti al controllo da parte della neo costituita Autorità Nazionale per la protezione dei dati e possono essere soggetti a sanzioni che raggiungono fino a 50 milioni di real brasiliani.

Con riferimento all'entrata in vigore della norma in commento, il Legislatore ha previsto che le società e gli enti pubblici potranno beneficiare di un periodo di 18 mesi per adeguarsi alle nuove regole. Esaminando la norma si ritrovano i principi enunciati nel Regolamento generale sulla protezione dei dati (GDPR). In particolare, il Legislatore Brasiliano ha fatto propri i principi fondamentali alla base del GDPR tra cui, in

particolare, liceità, correttezza, responsabilità, non discriminazione, limitazione delle finalità e trasparenza sull'uso dei dati personali.

1.3

D. Lgs. 65/2018: Sicurezza della rete e dei sistemi informativi

A far data dal 24 giugno scorso è entrato in vigore il D. Lgs. n. 65/2018 in materia di sicurezza delle reti e dei sistemi informativi che ha recepito la Direttiva (UE) n. 1148/2016 del Parlamento Europeo e del Consiglio, nota come Direttiva NIS.

In particolare, tra gli obiettivi del provvedimento legislativo vi è quello di "*promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali; migliorare le capacità nazionali di cyber security; e rafforzare la cooperazione a livello nazionale e in ambito UE*".

A ciò si aggiunga che il decreto in esame individua le Autorità competenti NIS per settore e i rispettivi compiti, nonché il gruppo di intervento per la sicurezza informatica in caso di incidente (i.e. CSIRT) che svolge i compiti e le funzioni del *Computer Emergency Response Team* (CERT) nazionale. Tale ultimo soggetto è quello che è chiamato a definire le procedure per la prevenzione e la gestione degli incidenti informatici.

PRASSI

2.1

Garante Privacy: attività ispettiva per il periodo luglio-dicembre 2018

Con deliberazione del 26 luglio 2018, il Garante per la Protezione dei dati personali ha approvato il piano ispettivo per il secondo semestre del 2018. Mediante tale deliberazione, il Garante ha inteso indirizzare l'attività ispettiva condotta dall'Ufficio del Garante, anche per mezzo della Guardia di Finanza, per il periodo luglio-dicembre 2018.

Con riferimento al contenuto della deliberazione, è stato statuito di indirizzare le attività ispettive verso i soggetti che effettuano trattamenti di dati personali particolarmente rilevanti, quali società o enti che gestiscono banche dati di grandi dimensioni, istituti di credito e società che svolgono attività di *telemarketing.*

Si legge nel comunicato che le attività ispettive avranno ad oggetto la verifica del rispetto degli obblighi di informativa, la corretta acquisizione del consenso da parte degli interessati, nonché il periodo di conservazione dei dati.

Giova sottolineare che l'anzidetta attività ispettiva sarà condotta, da un lato, nei confronti di soggetti individuati sulla base di reclami o segnalazioni e, dall'altro lato, su iniziativa della stessa Autorità, avuto riguardo ai trattamenti maggiormente rilevanti sotto il profilo della rischiosità e delle dimensioni dei trattamenti.

2.2

GPS e flotta aziendale: la parola al Garante Privacy

Con provvedimento n. 396 del 28 luglio 2018 il Garante della protezione dei dati personali si è espresso in merito ad una segnalazione effettuata da un dipendente avente ad oggetto l'implementazione da parte della società di un dispositivo GPS installato sui veicoli aziendali. In particolare, in tale sede la società non aveva rilasciato in favore dei dipendenti assegnatari del veicolo aziendale alcuna informativa e/o policy atta a delineare le caratteristiche di tale sistema GPS.

Si precisa che stante l'uso promiscuo della vettura aziendale, il sistema di geolocalizzazione istallato permetteva al datore di lavoro di trattare i dati relativi all'ubicazione del dipendente anche al di fuori dell'orario di lavoro. Il predetto sistema di geolocalizzazione consentiva, inoltre, al datore di lavoro di effettuare un'attività di monitoraggio su base continuativa dell'attività del dipendente, con una periodicità della rilevazione di circa 120 secondi.

All'esito dell'attività istruttoria condotta dall'Autorità è emerso che le operazioni di trattamento dei dati personali effettuate dalla società, titolare del trattamento, presentassero dei profili di non conformità alla disciplina dettata in materia di protezione dei dati personali. Infatti, è stato rilevato che il sistema di geolocalizzazione implementato fosse in contrasto con i principi di necessità, pertinenza e non eccedenza sanciti dal D.lgs. 196/2003 (i.e. Codice Privacy) e dal Regolamento Europeo n. 679/2016 (i.e. RGPD).

Pertanto, il Garante ha disposto a carico della società il divieto di trattare ulteriormente gli anzidetti dati personali. Inoltre, il Garante ha ingiunto al fornitore del servizio di geolocalizzazione di provvedere, da un lato, ad informare previamente i clienti rispetto alla possibilità di modificare le impostazioni standard del dispositivo e, dall'altro lato, di configurare, sin dalla fase di progettazione, il dispositivo mediante un sistema di localizzazione proporzionato rispetto al diritto alla riservatezza degli interessati, con particolare riferimento alla periodicità della rilevazione dell'ubicazione dell'interessato.

GIURISPRUDENZA

3.1

D. Lgs. 231/2001: sì al patteggiamento in virtù dell'adozione di un Modello "*riparatorio*"

Disposta la sola sanzione amministrativa nei confronti di una società, imputata per l'illecito amministrativo ex art. 25 del D. Lgs. 231/2001, in accoglimento del patteggiamento concordato tra le parti. Questa la conclusione cui è addivenuto il Giudice dell'Udienza Preliminare presso il Tribunale di Roma con sentenza del 20 marzo 2018 a seguito delle indagini relative ad ipotesi di corruzione che avevano evidenziato come l'ente imputato non avesse predisposto un Modello di organizzazione, gestione e controllo, idoneo ad impedire le condotte corruttive alla base delle ipotesi di reato, incorrendo pertanto nell'illecito contestato.

L'integrale restituzione del prezzo e del profitto del reato, il risarcimento del danno, così come la documentata eliminazione delle carenze organizzative di cui all'imputazione mediante l'adozione di un Modello "*riparatorio*" da parte dell'Ente hanno portato all'applicazione di una pena in misura ridotta.

Sul punto preme ricordare che l'art. 63 D. Lgs. 231/2001 consente l'accesso al rito del patteggiamento nell'ambito dei procedimenti "*231*" nei casi in cui: (i) per l'illecito amministrativo sia prevista la sola sanzione pecuniaria; (ii) per l'imputato del reato presupposto il giudizio sia definito o definibile con patteggiamento; (iii) non sia in concreto erogabile una sanzione interdittiva definitiva.
Nel caso di specie, il Giudice ha accertato come tali presupposti fossero rispettati.

La pronuncia in parola non appare particolarmente innovativa; cionondimeno contribuisce al consolidamento dell'orientamento giurisprudenziale finalizzato a valorizzare aspetti ulteriori a quelli normativamente previsti per consentire all'ente di evitare un processo ed accedere al patteggiamento.

3.2

***Whistleblowing:* nessuna tutela per il dipendente che commette un reato per raccogliere informazioni**

Con sentenza n. 35792 del 26 luglio 2018 la Cassazione ha statuito che il dipendente che accede abusivamente ad un sistema informatico per raccogliere prova di supposti illeciti sul luogo di lavoro

commette il reato di cui all'art. 615-*ter* c.p. (accesso abusivo al sistema informatico) e non può invocare la tutela riservata ai *whistleblower.* In tal senso, la Suprema Corte chiarisce come la *ratio* della nuova disciplina sul *whistleblowing* (legge 179/2017) non sia finalizzata ad ispirare le capacità investigative dei dipendenti pubblici i quali, dunque, possono segnalare esclusivamente fatti o notizie di cui siano venuti a conoscenza a causa del rapporto di lavoro.
Nel caso di specie, il dipendente, al fine di dimostrare la vulnerabilità del sistema informatico adottato dal datore di lavoro, aveva impiegato l'*account* e la *password* di un collega per accedere al sistema e creare un falso documento di cessazione del rapporto di lavoro per un soggetto mai impiegato.

Imputato dunque per il reato di cui all'art. 615-*ter* c.p., il ricorrente si era difeso sostenendo l'irrilevanza penale della propria condotta facendo valere, quale causa di giustificazione, l'adempimento del dovere, fondato sul vincolo di fedeltà che lega il pubblico dipendente all'amministrazione e derivante dagli artt. 54 e 54 *bis* del D. Lgs. 165/2001. La Suprema Corte, tuttavia, ha respinto la tesi difensiva argomentando come "*la normativa citata si limiti a scongiurare conseguenze sfavorevoli, limitatamente al rapporto di impiego, per il segnalante che acquisisca, nel contesto lavorativo, notizia di un'attività illecita". Non istituisce invece "alcun obbligo di attiva acquisizione delle informazioni, autorizzando improprie attività investigative, in violazione dei limiti posti dalla legge*".

Ne deriva che la condotta del dipendente non può essere in alcun modo scriminata ed il reato mantiene ogni profilo di antigiuridicità presupposto della condanna.

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 | AGOSTO 2018

RIFERIMENTI NORMATIVI, PRASSI E GIURISPRUDENZA AL 31 AGOSTO 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