I QUADERNI DEL GRUPPO ASLA DI **CORPORATE COMPLIANCE**

CORPORATE COMPLIANCE ROUND TABLES 2018

Atti del convegno con otto tavole rotonde con la partecipazione di ventiquattro esperti di diritto societario di sedici Studi Legali associati ad ASLA ai sensi del Decreto Legislativo n° 231 del 2001, un'occasione unica per diffondere la cultura del diritto d'impresa e la condivisione delle conoscenze più aggiornate in materia da parte dei professionisti dei propri Studi Membri

ASLA
Associazione Studi Legali Associati

I QUADERNI DEL GRUPPO ASLA DI **CORPORATE COMPLIANCE**

A CURA DI IRENE PICCIANO E ANTONIO BANA
CON TESTI DI ANDREA MANTOVANI, EVA REGGIANI, DEBORAH BOLCO, MARIANGELA PAPADIA, IRENE PICCIANO, EVA CRUELLAS SADA, EUGENIA GAMBARARA, MICAELA BARBOTTI, ROBERTO TIRONE, PIETRO ORZALESI, ANTONIO BANA, FRANCESCA CHIARA BEVILACQUA, GIACOMO GORI, PIETRO BOCCACCINI, FEDERICA DENDENA, GIULIO NOVELLINI, TOMMASO SALA, SIMONA CUSTER, ANGELA BERINATI, MARTA MARGIOCCO, CECILIA PONTIGGIA, TIZIANA BONESCHI, PIERO MAGRI, STEFANO CANCARINI, LAURA LIGUORI, LUIGI ZUMBO.

CORPORATE COMPLIANCE ROUND TABLES 2018

Atti del convegno con otto tavole rotonde con la partecipazione di ventiquattro esperti di diritto societario di sedici Studi Legali associati ad ASLA ai sensi del Decreto Legislativo n° 231 del 2001, un'occasione unica per diffondere la cultura del diritto d'impresa e la condivisione delle conoscenze più aggiornate in materia da parte dei professionisti dei propri Studi Membri

ASLA
Associazione Studi Legali Associati

Indice

CAPITOLO 1 di Stefano Cancarini, Federica Dendena, Laura Liguori, Giulio Novellini, Tommaso Sala e Luigi Zumbo

Data Protection Officer: guardiano od operatore della privacy?

Data Protection Officer: guardiano od operatore della privacy? Casi pratici aziendali nei primi sei mesi di applicazione del GDPR

SOMMARIO: 1. Il Data Protection Officer: origine ed evoluzione – 2. Obbligo di nomina – 3. Requisiti della designazione e di contatto – 4. Attività, conflitto di interesse e responsabilità – 5. (5) Caratteristiche specifiche del DPO in ambito privato e pubblico – 6. Designazione del DPO (interno o esterno alla realtà aziendale), tendenze di mercato circa il rapporto tra struttura privacy aziendale e DPO e tutela assicurativa

1. Il Data Protection Officer: origine ed evoluzione

Il Responsabile della Protezione dei Dati ("RPD"), nell'accezione inglese *Data Protection Officer* ("DPO"), è una figura di recente introduzione nel quadro normativo europeo sulla protezione dei dati personali, con il ruolo ibrido di agevolare e sorvegliare l'osservanza – da parte di titolari e responsabili – delle disposizioni del Regolamento (UE) 2016/679 ("GDPR") e delle norme nazionali di adeguamento. In particolare, al DPO sono attribuiti i ruoli di vigilanza e consulenza, nonché di punto di contatto per l'autorità di controllo (con cui coopera ai sensi dell'articolo 39, GDPR), gli interessati e i soggetti interni ed esterni all'organizzazione del titolare (o del responsabile).

Pur costituendo una novità nell'impianto di *governance* aziendale *post*-GDPR, la figura del DPO non è nuova nel panorama normativo europeo e internazionale.

Invero, nel contesto comunitario, già la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* ("Direttiva"), prevedeva la facoltà per gli Stati membri di introdurre nelle rispettive legislazioni nazionali la possibilità per i singoli titolari del trattamento di nominare un soggetto "*incaricato della protezione dei dati*", a cui demandare il compito di sorvegliare in maniera indipendente l'applicazione delle leggi di attuazione della Direttiva in ambito aziendale, garantendo il rispetto dei diritti e

delle libertà delle persone interessate, di cui solo alcuni Paesi, tra cui Germania, Francia e Svezia, hanno recepito la previsione in questione.

Sebbene il legislatore italiano abbia preferito non prevedere tale figura, anche in Italia si è sviluppato un vivace dibattito sulla figura del DPO, soprattutto grazie agli interventi del Garante per la protezione dei dati personali (il "Garante"), che già dal 2005 esortava le grandi e medie imprese ad adeguarsi a una "*visione della protezione dei dati attiva e dinamica*" come nei paesi in cui era ben conosciuta la figura del *Privacy Officer* [167]. Anche la dottrina e gli esperti del settore, peraltro, vedevano con favore l'introduzione di una figura con compiti e caratteristiche tipici dell'odierno DPO, soprattutto nelle aziende di rilevanti dimensioni [168].

La figura del "DPO" è stata introdotta anche per le istituzioni europee. Il Regolamento 2001/45/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2000, *concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati*, ha infatti previsto, all'articolo 24, la nomina da parte di "*ogni istituzione ed organismo della Comunità*" di un "*responsabile della protezione dei dati personali*" che in modo autonomo ed indipendente controllasse, *inter alia*, il rispetto della normativa in materia di data protection, tenesse un registro dei trattamenti e notificasse al Garante europeo della protezione dei dati personali quelli eventualmente qualificabili come "rischiosi".

Analogamente, oltreoceano, su impulso delle grandi realtà aziendali, il ruolo del c.d. *Privacy Officer* (o *Chief Privacy Officer*) ha trovato ampia applicazione già a partire dalla fine degli anni '90 [169]. A tale figura sono stati attribuiti principalmente ruoli di gestione dei rischi privacy e del potenziale impatto delle regole in materia di protezione dei dati personali [170].

2. Obbligo di nomina

L'articolo 37, paragrafo 1, GDPR, stabilisce che la designazione del DPO è obbligatoria, da parte di un titolare o responsabile, ogniqualvolta "*a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in*

167 Garante per la protezione dei dati personali, WP 106 - Relazione sull'obbligo di notifica da parte delle autorità di controllo nazionali, sull'utilizzo più appropriato di eccezioni e semplificazioni e sul ruolo degli incaricati per la protezione dei dati in ambito UE, del 18 gennaio 2005 [doc. web n. 1608212], disponibile a: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1608212; nonché, Garante per la protezione dei dati personali, Discorso del Presidente Francesco Pizzetti - Relazione 2005, del 7 luglio 2006 [doc. web n. 1303712], disponibile a: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1303712; Garante per la protezione dei dati personali, La protezione dei dati bussola nel futuro digitale. Intervento di Antonello Soro, Presidente del Garante privacy, del 21 ottobre 2015 [doc. web n. 4345757], disponibile a: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4345757

168 Tra gli altri, N. Bernardi, *Il Privacy Officer oggi nel contesto italiano*, in N. Bernardi, M. Perego, M. Polacchini, M. Soffientini (a cura di), *Privacy Officer. La figura chiave della data protection europea*, IPSOA, Milano 2013, p. 4

169 Sembrerebbe risalire al 1999 la nomina del primo CPO ad opera di una società californiana.

170 J. Brown, *Rise of the Chief Privacy Officer*, 2014, disponibile a: http://www.govtech.com/state/Rise-of-the-Chief-Privacy-Officer.html

trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

Nulla impedisce, ovviamente, la nomina di un DPO su base volontaria, nel qual caso dovranno comunque rispettarsi tutte le disposizioni in tema di posizione e poteri di tale figura. A questo proposito, il Gruppo di lavoro Articolo 29 ("WP29"), oggi *European Data Protection Board* ("EDPB") e il Garante, non hanno mancato di sottolineare l'importanza della figura del DPO all'interno di ogni organizzazione aziendale, sia per facilitare l'osservanza della normativa e "*aumentare il margine competitivo delle imprese"*, sia, conseguentemente, per assicurare il rispetto del *principio di accountability* previsto dal GDPR.

a) Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico

Il GDPR non stabilisce alcuna definizione di "autorità pubblica" o di "organismo pubblico". Sulla base delle indicazioni offerte dal WP29 nelle Linee-guida sui responsabili della protezione dei dati (RPD), dunque, queste espressioni devono essere interpretate alla luce del diritto nazionale [171]. In particolare, secondo il Garante, rientrano nella disciplina dell'articolo 37, paragrafo 1, lettera a), GDPR, non solo le amministrazioni dello Stato, le Regioni e gli enti locali, ma anche, *inter alia*, gli enti pubblici non economici nazionali, regionali e locali, le Università, le Camere di commercio, le aziende del Servizio sanitario nazionale e le autorità indipendenti [172].

Un'interpretazione estensiva della disposizione in esame è offerta anche dal WP29, che richiama come lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non sono necessariamente di esclusiva pertinenza di autorità o di organismi pubblici, potendo essere affidati in diversi ambiti (quali trasporti locali, regionali o statali, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive, istituti per l'edilizia popolare, organismi di disciplina professionale) anche a persone fisiche o giuridiche di diritto privato. In questi casi, le finalità del trattamento e la situazione in cui versano gli interessati sono assimilabili a quelle che si avrebbero ove ci si trovasse di fronte a un'autorità pubblica, stante la (quasi) totale assenza di discrezionalità per gli interessati in merito al "se" e al "come" del trattamento dei propri dati personali. In ragione di ciò, il WP29 raccomanda che gli organismi privati che svolgono funzioni pubbliche o esercitano pubblici poteri provvedano alla designazione di un DPO, al fine di garantire agli interessati l'ulteriore tutela offerta da tale figura [173].

171 *Ivi*, p. 8

172 Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico*, del 15 dicembre 2017 [doc. web n. 7322110], disponibile a: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

173 Article 29 Working Party, *Linee guida sui responsabili della protezione dei dati* (RPD), WP243.01, 5 aprile 2017, p. 8, disponibile a https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 Questa interpretazione risulta, peraltro, condivisa dal Garante nelle proprie Faq sul DPO (Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico*)

Più complessa, invece, la questione per le c.d. società *in-house*, che la dottrina prevalente ritiene comunque obbligate a procedere alla designazione di un DPO [174].

Discorso parzialmente differente riguarda, invece, le autorità giurisdizionali, che il GDPR esclude espressamente dall'obbligo di nomina del DPO. Tuttavia, il legislatore italiano è intervenuto integrando il Codice Privacy e prevedendo, all'art. 2-*sexiesdecies*, la designazione del DPO "*anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni*", peraltro in (potenziale) contrasto quindi con il dettato normativo europeo, come rilevato da parte della dottrina [175].

b) Il trattamento richiede il monitoraggio regolare e sistematico degli interessati su larga scala

La valutazione in merito all'obbligatorietà della designazione di un DPO in ambito privato necessita un certo sforzo interpretativo in quanto nel GDPR non si rinvengono le definizioni di "*attività principali*", "*larga scala*" (contenute nelle lettere b) e c)) e "*monitoraggio regolare e sistematico*" (di cui alla sola lettera b)).

Un primo chiarimento in merito alla portata dell'espressione "**attività principali**" è fornito dal considerando 97, GDPR, che specifica come "*le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*". Pertanto, sono da ritenersi escluse le attività ancillari in quanto meramente accessorie e di supporto [176]. Esulano, quindi, dal concetto di "attività principale" le prestazioni comuni a tutti gli organismi, quali, a titolo esemplificativo, la gestione delle retribuzioni del personale e la configurazione dei sistemi IT [177].

Altrettanto complessa risulta l'esatta definizione del concetto di "**larga scala**". Nel GDPR, le poche indicazioni di supporto sono contenute nel considerando 91, che fa riferimento a una "*notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un alto rischio*". Da parte sua, il WP29 indica, allo scopo di stabilire se un trattamento sia o meno effettuato su larga scala, di considerare i seguenti fattori: *(i)* numero di interessati, in assoluto o in percen-

174 A. Avitabile, *Il data protection officer*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, Bologna 2017, pp. 337-338

175 G. M. Pellos, *La figura del DPO nel regolamento n. 2016/679*, in G. M. Pellos (a cura di), *Il data protection officer (DPO). Il responsabile della protezione dei dati personali dopo il D.Lgs. 10 agosto 2018, n. 101,* Dike Giuridica Editrice, Roma 2018, p. 26.
Tuttavia, a parere di chi scrive, la tesi del conflitto tra norme non appare condivisibile, essendo l'antinomia soltanto apparente.

176 E. Pelino, *I soggetti del trattamento*, in L. Bolognini, E. Pelino, C. Bistolfi (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Busto Arsizio (VA) 2018, p. 164.

177 Gruppo di lavoro articolo 29 per la protezione dei dati, *op. cit.*, p. 9. Sul punto, in senso conforme, si veda anche, M. Iaselli, *Manuale operativo del D.P.O. (Data Protection Officer)*. Aggiornato al *d.lgs. del 10 agosto 2018, n. 101 in materia di privacy*, Maggioli Editore, Santarcangelo di Romagna (RN) 2018, p. 29; E. Bassoli, *La nuova privacy GDPR dopo il d.lgs. 10 agosto 2018, n. 101*, Dike Editrice Giuridica, Roma 2018 p. 87; G. B. Gallus, M. Pintus, *op. cit.*, pp. 180-181; G. M. Riccio, Art. 38. *Posizione del responsabile della protezione dei dati*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy,* Ipsoa, Milano 2018, p. 342.

tuale sulla popolazione di riferimento; *(ii)* volume e/o tipologia di dati trattati; *(iii)* durata e persistenza dell'attività di trattamento e *(iv)* portata geografica [178].

Anche l'espressione "**monitoraggio regolare e sistematico**" risulta priva di una precisa delimitazione nel corpo normativo. Secondo l'interpretazione del WP29, l'attività di monitoraggio dovrà essere contestualmente (e non alternativamente) regolare e sistematica [179], ove con l'aggettivo "regolare" si intende il trattamento *(i)* svolto in modo continuativo o a intervalli definiti; *(ii)* ricorrente o ripetuto a intervalli costanti; ovvero *(iii)* effettuato in modo costante o a intervalli periodici. Rientrano, invece, nella definizione di "sistematico" le attività poste in essere *(i)* per sistema; *(ii)* in modo organizzato, predeterminato o metodico; *(iii)* nel contesto di un progetto complessivo di raccolta di dati; ovvero *(iv)* nell'ambito di una strategia predefinita [180].

c) Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10

Il trattamento di categorie particolari di dati personali di cui all'articolo 9, GDPR, e quello di dati relativi a condanne penali e a reati di cui all'articolo 10, GDPR, sono requisiti alternativi e non cumulativi. Pertanto, risulta sufficiente il trattamento su larga scala, nell'ambito dell'attività principale [181] del titolare (o responsabile), di una sola di queste due categorie di dati personali per far scattare l'obbligo della designazione del DPO.

★★★

Si segnala, inoltre, che, con riferimento al settore privato, il Garante ha evidenziato che, "*ricorrendo i suddetti presupposti*" di cui alle lettere b) e c) dell'articolo 37, GDPR, sono tenuti a designare un DPO, tra gli altri, i seguenti soggetti: "*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 (i.e., 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; entità che erogano servizi televisivi a pagamento*" [182].

178 Article 29 Working Party, *op. cit.*, pp. 9-11.

179 G. M. Riccio, *op. cit.*, pp. 342-343.

180 Article 29 Working Party, *op. cit.*, p. 11.

181 Sui concetti di "attività principale" e "larga scala" si rimanda a quanto sopra esposto.

182 Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato, del 26 marzo 2018*, [doc. web n. 8036793], disponibile a: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793&zx=h34q1apw4hz4.

Tuttavia, a giudizio di chi scrive, stante la dubbia interpretazione del significato da attribuire al gerundio "ricorrendo", resta fermo che ogni titolare e responsabile, seppur rientranti in una delle categorie sopra elencate, devono comunque svolgere una seria valutazione circa l'applicabilità o meno dell'obbligo (o dell'opportunità) di nomina del DPO attraverso un'attenta analisi del dettato normativo alla luce delle caratteristiche oggettive della propria organizzazione, nel rispetto del principio di *accountability* [183].

3. Requisiti della designazione e di contatto

L'art. 37, comma 5, del GDPR recita che il DPO deve essere designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'articolo 39 del GDPR. È essenziale nella scelta del DPO tenere conto del fatto che "*il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento*" [184].

Con riferimento alle qualità professionali, l'articolo 37 del GDPR non specifica quali tra queste debbano essere prese in considerazione nella designazione di un DPO; tuttavia la conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati sono caratteristiche imprescindibili. Il DPO può documentare la propria esperienza professionale anche attraverso la partecipazione ad attività formative specialistiche (es.: master, corsi di studio e professionali) e il conseguimento dei relativi attestati specialistici.

Tuttavia, il Garante, in data 28 luglio 2017 [185], ha rappresentato come, allo stato attuale, le disposizioni non prevedono un albo dei DPO che attesti i requisiti e le caratteristiche di conoscenza, abilità e competenza previste dal GDPR, né richiedano che tali requisiti siano attestati attraverso specifiche certificazioni o percorsi formativi. Eventuali certificati rilasciati al termine di un percorso formativo, sebbene costituiscano un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, non equivalgono di per sé a una abilitazione allo svolgimento del ruolo, né possono sostituire la valutazione fatta dal titolare o dal responsabile del trattamento sui requisiti del DPO, che intende designare.

183 Le sanzioni di cui al Regolamento saranno argomento specifico di analisi nel contesto del commento agli artt. 83 e 84, GDPR. In questa sede, pare tuttavia opportuno anticipare che la violazione da parte di un titolare (o di un responsabile) dell'obbligo di designare un DPO è punita, ai sensi dell'articolo 83, paragrafo 4, lettera a), GDPR, con una sanzione amministrativa pecuniaria fino a 10 milioni di euro, ovvero, se superiore, fino al 2% del fatturato mondiale del gruppo cui appartiene l'organizzazione.

184 Cfr. considerando 97 del GDPR;

185 Cfr. Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali Doc-Web [7057222] del 28 luglio 2017: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7057222;

A conferma di quanto sopra, il TAR del Friuli Venezia Giulia con sentenza n. 287/2018 [186] ha ritenuto, nel caso di specie che la minuziosa conoscenza e l'applicazione della disciplina di settore – da parte del DPO - restano, indipendentemente dal possesso o meno di certificazioni, il nucleo essenziale e irriducibile della figura professionale, il cui profilo non può che qualificarsi come eminentemente giuridico.

Sotto altro profilo, secondo le Linee guida del WP29 [187], la capacità del DPO di assolvere i propri compiti deve essere considerata sia in relazione alle qualità personali e alle conoscenze dello stesso, sia in relazione alla posizione svolta all'interno dell'azienda o dell'organismo.

Inoltre, il livello di conoscenza varia in funzione della natura e dei dati e delle tipologie di trattamenti. Per cui, nel caso di trasferimento all'estero di dati personali oppure di trattamenti particolarmente complessi (es. i dati sanitari), dovrebbe essere designato un soggetto dotato di specifiche competenze.

Infine, sempre l'art. 37 del GDPR dispone che: il ruolo di DPO possa essere affidato ad uno dei dipendenti dell'azienda, ma anche esternalizzato a un fornitore di servizi (libero professionista o azienda); il DPO possa essere, altresì, una persona fisica o una persona giuridica; il DPO possa essere designato come responsabile per un gruppo di imprese, purché sia facilmente raggiungibile da ciascuno stabilimento ed in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo [188].

Con riferimento ai dati di contatto, l'art. 37, comma 7, del GDPR prevede che una volta designato il DPO occorra comunicare al Garante le generalità. Questa disposizione ha lo scopo di garantire che le autorità di controllo possano mettersi in contatto in modo facile e diretto, così come chiarito nelle Linee guida adottate dal WP29 [189] e stabilito in base all'articolo 39, comma 1, lettera e) del GDPR che afferma che il DPO funge da punto di contatto.

A tal proposito, il Garante ha messo a disposizione sul proprio sito un modulo, che permette la comunicazione diretta dei dati e del nominativo del DPO alla stessa [190]. I dati di contatto devono essere, inoltre, resi noti al personale interno della azienda e agli interessati, anche eventualmente pubblicandoli sul sito internet del titolare o responsabile del trattamento. Non è necessario, né in

186 Cfr. sentenza n. 287/2018 del TAR del Friuli Venezia Giulia: http://www.dirittoegiustizia.it/allegati/16/0000082282/TAR_Friuli_Venezia_Giulia_sez_I_sentenza_n_287_18_depositata_il_13_settembre.html

187 Cfr. Linee guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

188 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

189 Cfr. Linee Guida di cui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.6;

190 Cfr. Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati – RPD (art.37, par.7 del Regolamento (UE) 2016/679 - RGPD e art. 28, c. 4 del D.Lgs. 51/2018) https://servizi.gpdp.it/comunicazione-rpd/compilaModulo e relative FAQ: https://www.garanteprivacy.it/web/guest/regolamentoue/rpd/faq-relative-alla-procedura-telematica-per-la-comunicazione-dei-dati

ambito pubblico [191] né privato [192], pubblicare il nominativo del DPO. Sebbene ciò rappresenti con ogni probabilità una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso DPO stabilire se si tratti di un'informazione necessaria o utile in base alle specifiche circostanze.

Con la pubblicazione dei dati di contatto, il GDPR ha l'obiettivo di garantire che sia gli interessati sia le autorità di controllo possano mettersi in contatto con il DPO in modo facile e diretto senza l'intermediazione della struttura in cui opera. In tal senso deve essere, altresì, garantita la confidenzialità delle comunicazioni in maniera da evitare che gli interessati, ad esempio i dipendenti stessi della struttura, non siano dissuasi dal presentare eventuali reclami [193].

4. Attività, conflitto di interesse e responsabilità

Il DPO è un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR. Coopera con il Garante e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali [194].

Il DPO deve informare il titolare, il responsabile nonché se necessario i loro dipendenti sugli obblighi loro gravanti e che trovano fonte nel GDPR. Inoltre, l'art. 39 del GDPR dispone che egli debba informare i predetti soggetti anche in merito agli obblighi che potrebbero derivare dalla normativa comunitaria o da quella interna.

Oltre a quanto detto sopra, la lettera b) dell'art. 39 del GDPR dispone che il DPO sia tenuto a sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità [195].

In aggiunta, il DPO dovrebbe "*fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati* ["DPIA"] *e sorvegliarne lo svolgimento*". Tale previsione è eventuale dal momento che la lettera c) dell'art. 39 del GDPR stabilisce che questo avvenga su richiesta del titolare del trattamento, il quale non sarà tenuto a conformarsi alle indicazioni espresse dal DPO. Il WP29 rac-

191 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

192 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

193 Cfr. Linee Guida di cui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.6

194 Cfr. artt. 38 e 39 del GDPR; Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato, punto 1

195 Nel considerando 97 viene ulteriormente specificato che il titolare o il responsabile del trattamento dovrebbe essere "*assistito* [dal RPD] *nel controllo del rispetto a livello interno del presente regolamento*". Fanno parte di questi compiti di controllo svolti dal RPD, in particolare, la raccolta di informazioni per individuare i trattamenti svolti; l'analisi e la verifica dei trattamenti in termini di loro conformità, e l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

comanda che il titolare del trattamento si consulti con il DPO, anche, sulle seguenti tematiche: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al GDPR [196].

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal DPO è necessario che la documentazione relativa alla DPIA – come del resto tutti gli altri documenti – riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni del professionista.

Ulteriormente, in base all'articolo 39, paragrafo 2, il DPO deve "*considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*" (c.d. approccio basato sul rischio).

Infine, tra i compiti del DPO, si annoverano anche la cooperazione e il contatto con il Garante. In particolare, le lettere d) ed e) dell'art. 39 prevedono che il professionista funga da "punto di contatto" per l'autorità di controllo per questioni connesse al trattamento dei dati. In altri termini, il Garante potrà rivolgere a tale soggetto eventuali domande preliminari sulla gestione dei dati personali compiuta dal titolare e dal responsabile. In particolare, il DPO potrà essere coinvolto nell'eventuale consultazione preventiva di cui all'art. 36 del GDPR e nelle attività di ispezione da parte delle autorità.

L'art 38, comma 6, del GDPR consente al DPO lo svolgimento delle proprie funzioni, all'interno della struttura, a condizione che il titolare o il responsabile del trattamento assicuri che tali compiti e funzioni non diano adito ad un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un DPO può svolgere altre funzioni, l'affidamento di tali ulteriori compiti è ammesso solo a condizione che essi non creino situazione di conflitto. A tale riguardo, le linee guida dettate dal WP29 evidenziano che a seconda delle attività, delle dimensioni e della struttura dell'organizzazione, al fine della designazione del DPO, possa essere una buona pratica: *(i)* identificare le posizioni incompatibili con detta funzione, stabilire delle regole interne per evitare situazioni di conflitto di interesse, fornire una spiegazione generale sul conflitto di interesse; *(ii)* dichiarare che il DPO non versi in alcuna situazione di conflitto di interessi con riguardo alle sue funzioni; *(iii)* redigere regole interne a tale scopo onde evitare conflitti di interessi e *(iv)* individuare le qualifiche e le funzioni incompatibili con quella di DPO.

Sussistono situazioni di conflitto nei casi in cui il DPO rivesta ruoli manageriali di vertice, ad esempio come amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, dire-

196 Cfr. Linee Guida di cui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 4.2;

zione risorse umane o responsabile IT [197]; ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. A quest'ultimo proposito, anche in ambito pubblico, il Garante sottolinea che in linea di principio oltre ai ruoli manageriali di vertice, possono sussistere situazioni di conflitto di interesse rispetto a figure apicali dell'amministrazione investite di capacità decisionali in ordine alle finalità e ai mezzi del trattamento di dati personali posto in essere dall'ente pubblico, ivi compreso, ad esempio, il responsabile dei sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici)" [198].

Per quanto attiene invece alle responsabilità, l'art. 38, comma 3 del GDPR fissa alcune garanzie essenziali per consentire al DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile [199]. Ciò significa che il professionista, nell'esecuzione dei compiti attribuitigli ai sensi dell'art. 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Tuttavia, sia il titolare che il responsabile mantengono la piena responsabilità sull'osservanza della normativa in materia di protezione dei dati.

In tale contesto, nell'esecuzione dei compiti elencati dal GDPR, nonché degli altri compiti che potrebbero essere assegnati in via contrattuale per mezzo di relativo incarico di designazione, il DPO non è direttamente responsabile civilmente nei confronti di terzi, né possono essere a lui imputate eventuali sanzioni amministrative. Ciò non esclude, eventualmente, l'assunzione di responsabilità in sede contrattuale, per mezzo di manleve ed esoneri di responsabilità a favore del titolare o del responsabile.

Allo stesso modo, non sussistono responsabilità circa l'attività di sorveglianza: deve ritenersi che un'eventuale responsabilità professionale di tale soggetto debba poggiare su di un criterio di imputazione a carattere colposo e mai oggettivo [200].

L'articolo 38 comma 3 del GDPR prevede, inoltre, che il DPO non possa essere "*rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*".

197 Il pericolo del conflitto di interessi del DPO è stato affrontato dall'autorità bavarese per la protezione dei dati ("BayLDA") la quale ha sanzionato una società che aveva designato il proprio IT manager come responsabile della protezione dei dati. Quest'ultimo, infatti, avrebbe in pratica dovuto monitorare se stesso, verificando se le proprie attività di IT manager fossero conformi alla normativa in materia di protezione dei dati personali. V. https://www.lda.bayern.de/media/pm2016_08.pdf e Cfr. artt. 38 e 39 del GDPR; Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato.

198 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico, punto 7: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

199 Il considerando 97 aggiunge che i DPO "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*".

200 Cfr. Commentario GDPR e Normativa Privacy, a cura di Giovanni Maria Riccio, Guido Scorza, Ernesto Belisario, I Edizione, p. 351: anche se, "*a parere di chi scrive appare preferibile ritenere che un'eventuale omissione nella segnalazione della normativa pertinente […] così come delle misure adottate, non sia sufficiente a rendere responsabile, sempre a titolo di responsabilità professionale il DPO*".

Alla luce di quanto sopra, il GDPR ha creato una figura indipendente e di controllo dei trattamenti dei dati personali posti in essere dal titolare del trattamento; tuttavia il DPO non è immune da responsabilità, anche penali, nel caso di svolgimento non conforme delle sue attività al GDPR.

5. Caratteristiche specifiche del DPO in ambito privato e pubblico

L'art. 37, comma 1, lettere b) e c), del GDPR dispone che il DPO debba essere nominato in ambito privato quando "*le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*", ovvero nel caso in cui le attività principali consistano nel trattamento, su larga scala, di categorie particolari di dati personali o [201] di dati relativi a condanne penali e a reati.

Per poter comprendere l'effettiva portata di tali disposizioni è necessario compiere uno sforzo interpretativo alla luce dei considerando del GDPR e delle Linee Guida adottate dal WP29 [202] nelle quali si è cercato di definire con maggior chiarezza cosa si intenda per *(i)* "attività principali", *(ii)* "larga scala" e *(iii)* "monitoraggio regolare e sistematico".

In merito alle "attività principali", il WP29 [203] precisa che devono intendersi come ricomprese tra queste anche le operazioni essenziali per raggiungere gli obiettivi perseguiti a livello aziendale; afferisce, quindi, all'attività principale anche il trattamento di dati che costituisce una componente inscindibile delle attività svolte dal titolare o dal responsabile del trattamento. Il considerando 97 del GDPR, invece, si limita a stabilire che nel settore privato le attività principali riguardano quelle primarie del titolare ed esulano dal trattamento dei dati personali come attività accessoria.

Riguardo al secondo criterio, in entrambi i casi menzionati all'art. 37, comma 1, del GDPR si subordina l'obbligatorietà della nomina al trattamento di dati personali su "larga scala", eppure, tale concetto non è stato individuato in maniera

201 Seppur la traduzione del GDPR in lingua inglese riporti la congiunzione "e", non sussistono motivazioni di ordine sistematico che impongano l'applicazione simultanea dei due criteri (categorie particolari di dati e dati relativi a condanne penali e reati), dunque, il testo deve essere interpretato come se vi fosse la congiunzione "o", agli effetti già presente nella traduzione in lingua italiana. Cfr. in tal senso le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.5

202 In tale contesto la stessa Autorità Garante nelle Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato rimanda espressamente alle Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2

203 Cfr. le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.2

certa e predeterminata né dal legislatore europeo [204], né dal WP29 [205]. Quest'ultimo, pur affermando l'impossibilità di precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità [206], ha mostrato una possibile via interpretativa elencando i seguenti fattori come rilevanti: (i) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; (ii) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; (ii) la durata, ovvero la persistenza, dell'attività di trattamento, e (ii) la portata geografica dell'attività di trattamento.

In relazione al "monitoraggio regolare e sistematico", si può far riferimento al considerando 24 del GDPR che include nel "monitoraggio del comportamento degli interessati" tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale, ma la nozione di monitoraggio potrebbe assumere rilievo anche off line. Il WP29 [207] ha poi integrato l'interpretazione di questo criterio definendo da un lato la regolarità del monitoraggio come una attività svolta in modo continuativo, ovvero ripetuta ad intervalli costanti, periodici o per un arco di tempo definito e dall'altro la sistematicità dello stesso come una attività posta in essere in modo predeterminato, organizzato e metodico nell'ambito di un progetto complessivo di raccolta di dati.

Sulla base dei presupposti così interpretati si dovrà valutare l'obbligo di nomina del DPO in capo al titolare o al responsabile del trattamento; tuttavia, l'articolo 37, comma 4, del GDPR prevede che il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti tali categorie possano o, se previsto dal diritto dell'Unione o degli Stati membri, debbano designare un DPO anche in casi diversi da quelli appena descritti. In linea con questa previsione, il Garante ha raccomandato in via generale la designazione di un DPO in ossequio al principio dell'*accountability* [208].

Inoltre, il legislatore europeo ha esplicitamente previsto un altro caso di obbligatorietà della nomina del DPO laddove il trattamento sia effettuato da

204 Il considerando 91 del GDPR relativo alla valutazione d'impatto recita in particolare "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*"

205 Cfr. le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.3

206 Il Gruppo Articolo 29 ha affermato il suo impegno nel contribuire alla definizione di standard utili pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina obbligatoria del DPO. Cfr. le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.3

207 Cfr. le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.4

208 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali [209].

Ancora una volta non appare facile individuare l'effettivo ambito di applicazione di tale previsione in quanto il GDPR demanda l'inquadramento delle "autorità pubbliche" e degli "organismi pubblici" alle normative nazionali. Alla luce di ciò e della definizione di "ente pubblico" contenuta nella Direttiva n.2002/98/CE del 17 novembre 2003 [210], la disposizione in esame deve ritenersi applicabile oltre che alle autorità pubbliche di carattere nazionale, regionale o locale, anche agli altri diversi organismi di diritto pubblico previsti dalla relativa disciplina nazionale [211].

Laddove sia nominato un DPO in ambito pubblico, la costituzione di un apposito ufficio dovrà essere frutto di una valutazione di opportunità o di necessità [212] tenendo ben presente che il titolare e il responsabile del trattamento devono fornire le risorse necessarie affinché il DPO possa svolgere le sue funzioni [213].

Un'ulteriore problematica sorge in relazione allo svolgimento di funzioni pubbliche e all'esercizio di pubblici poteri da parte di soggetti di diritto privato sulla base di una concessione [214]. In questi casi i dati dell'interessato si trovano in una situazione molto simile a quella che si avrebbe se questi fossero trattati da un soggetto di diritto pubblico tanto che il WP29 [215], pur chiarendo che in tali contesti la nomina non sarebbe di per sé obbligatoria, raccomanda comunque la designazione di un DPO [216].

6. Designazione del DPO (interno o esterno alla realtà aziendale), tendenze di mercato circa il rapporto tra struttura privacy aziendale e DPO e tutela assicurativa

209 Cfr. Art. 37, comma 1, lettera a, del GDPR

210 Secondo la Direttiva nella definizione di "*ente pubblico*" devono includersi "*le autorità statali, regionali o locali, gli organismi di diritto pubblico e le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di diritto pubblico*"

211 Cfr. sia le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.1, che le Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

212 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

213 Indipendentemente dalla costituzione o meno di un ufficio, non possono essere designati più DPO per un unico titolare o responsabile del trattamento; ciò non esclude la possibilità di individuare figure di supporto. Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

214 Cfr. Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110

215 Cfr. le Linee Guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, WP 243 rev. 01 - punto 2.1.1

216 Tanto in ambito pubblico quanto in ambito privato emerge con chiarezza l'intento dell'autorità di estendere quanto più possibile la buona prassi della nomina del DPO indipendentemente dalla presenza di un obbligo in tal senso

La designazione del DPO e l'eventuale strutturazione del relativo "ufficio" o "dipartimento" [217] sono stati, e sono tutt'ora, temi molto dibattuti tra gli operatori in ambito privacy.

Circa la designazione del DPO, il dilemma che affligge i titolari e responsabili del trattamento è se identificare il soggetto che ricoprirà tale funzione tra coloro facenti parte della realtà aziendale o, al contrario, designare un soggetto esterno alla struttura.

In entrambi i casi vi sono aspetti positivi e negativi, i cui più rilevanti sono qui di seguito elencati e sintetizzati:

A) DPO Interno

- **PRO**: art. 37, paragrafo 6, del GDPR prevede espressamente che il DPO possa essere un dipendente del titolare o del responsabile del trattamento. A tal riguardo il vantaggio, dal punto di vista funzionale, è che la risorsa interna conosce in maniera specifica la struttura aziendale e i relativi processi; e
- **CONS**: svolgendo altre mansioni all'interno dell'azienda, la risorsa interna potrebbe incorrere in un possibile conflitto di interessi con quelle proprie dell'altro incarico.

B) DPO esterno

- **PRO**: si mitiga il rischio di conflitto di interessi; e
- **CONS**: il grado di conoscenza delle dinamiche aziendali è limitato e, nella maggior parte dei casi, il soggetto designato ricopre più incarichi, con la conseguente difficoltà di reperibilità e di riscontrare in tempi rapidi i riscontri richiesti.

Alla luce di quanto sopra, si osserva altresì che la possibilità di affiancare al DPO interno un soggetto/i esterno/i che integri(no) i rispettivi requisiti, tecnico e/o giuridici, è un compromesso che il mercato sta valutando.

Indipendentemente dalla designazione del DPO, interna o esterna alla realtà aziendale, è interessante evidenziare l'evoluzione del mercato circa l'adozione di una struttura aziendale finalizzata alla *compliance privacy*.

Successivamente alla piena applicabilità del GDPR, ovvero post 25 maggio 2018, la tendenza del mercato è stata quella di prevedere (i) la competenza della "*direzione legal – corporate and compliance affairs*" per la gestione delle relative tematiche privacy e (ii) la designazione del DPO (qualora obbligatoria ai sensi

217 Ciò vale soprattutto in caso di designazione di un DPO interno alla realtà aziendale.

del GDPR [218]), per la supervisione e consulenza relativa al trattamento dei dati personali. Tale scelta organizzativa è stata frutto di diversi fattori, quali:

- individuazione all'interno dell'azienda delle funzioni che avessero un certo *know-how* in materia, tale da garantire un presidio costante specialmente in fase di implementazione del dettato normativo;
- l'assenza, prima dell'entrata in vigore del GDPR, di orientamenti univoci circa l'adozione da parte delle aziende di strutture tecnico-organizzative sotto il profilo del presidio *privacy*, ivi inclusa la designazione di un soggetto responsabile alla protezione dei dati; e
- si preferiva attendere le tendenze di mercato per vedere, magari aiutati da qualche delucidazione in merito del Garante, quale sarebbe stato il modo migliore per organizzare la struttura aziendale in termini di compliance rispetto alla normativa *privacy*.

Alla luce di quanto sopra, infatti, la maggior parte degli operatori ha deciso di adottare strutture organizzative provvisorie, simili a quella sopra specificata, per affrontare al meglio la delicata fase di prima implementazione della norma. Successivamente, gli stessi avrebbero verificato l'opportunità di mantenere tali strutture o modificarle in base alla mole di lavoro che sarebbe scaturita, dalla prassi che anche le altre aziende avevano ormai consolidato nonché da eventuali pronunciamenti del Garante o delle autorità di controllo competenti.

Negli ultimi mesi è stato rilevato che le richieste di consulenza privacy hanno avuto un incremento significativo. La causa di tale fenomeno potrebbe essere imputata principalmente a due fattori (i) la diffusione nei contesti aziendali (e sociali) di una maggiore consapevolezza circa la normativa *privacy* e (ii) l'ingente e variegato numero di trattamenti di dati personali eseguiti da alcuni operatori.

Pertanto, alla luce di quanto sopra e tenendo altresì conto della necessità di riscontrare in tempi rapidi le richieste avanzate dai soggetti interessati, gli operatori hanno modificato le rispettive strutture adottando un presidio specifico e dedicato (quasi esclusivamente) alla gestione delle tematiche *privacy* con una diretta interazione con il DPO.

Nella maggior parte dei casi le "nuove" strutture sono caratterizzate dal ruolo preminente ricoperto dal dipartimento legale in ambito *privacy*. In ogni caso, per mitigare il rischio di conflitto di interessi tra la funzione legale e il ruolo del DPO (soprattutto se interno alla realtà aziendale), gli operatori separano la figura del DPO rispetto al dipartimento legale, ad esempio, affidando

218 Come previsto dall'art. 37 GDPR, la designazione del DPO è obbligatoria: "*Se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; Se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; Se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati*". Si consideri che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto comunitario. Inoltre, anche ove il GDPR regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29", così come il Garante della privacy italiano, incoraggiano un tale approccio "cautelativo".

tale ruolo al responsabile/dipartimento *compliance*. Infatti, tale separazione, oltre a limitare le sovrapposizioni di attività funzionali alla gestione delle tematiche privacy, potrebbe agevolare il processo di adeguamento al GDPR.

Inoltre, è ormai assodata l'importanza del presidio IT a supporto del DPO. In molti casi, tale presidio è stato garantito in passato dal *commitment* aziendale, ma, recentemente, molte aziende hanno formalizzato la presenza di tale figura direttamente nell'ufficio del DPO o comunque in un *team*, ufficiale e multidisciplinare (interno o esterno), che agirebbe a supporto ufficiale del medesimo DPO.

Infine, coloro che si apprestano ad assumere il ruolo di DPO necessitano sempre più di una tutela nell'eventualità di un proprio errore professionale. Infatti, seppur il DPO non risponda in via diretta e personale in caso di inadempimento da parte del titolare/responsabile del trattamento circa le previsioni del GDPR, è evidente che la responsabilità del DPO possa derivare dal rapporto contrattuale intercorrente tra il DPO e il titolare/responsabile del trattamento. Si pensi, ad esempio, alla sanzione comminata dal Garante al titolare per violazione di dati personali per finalità illecite e in rispetto alle quali il DPO aveva espresso il suo parere favorevole: in tal caso è prevedibile l'esperimento di un'azione contrattuale dal titolare avverso il DPO per risarcimento del danno causato dal suo operato.

Proprio per tali ragioni, si assiste alla recente diffusione di coperture assicurative a tutela dell'attività svolta dal DPO [219]. In ogni caso, il profilo della responsabilità del DPO e l'eventuale copertura assicurativa del suo operato è un aspetto molto delicato, soprattutto in questa fase di implementazione del GDPR, nella quale non sono ancora state riscontrate prassi consolidate a tal riguardo.

219 Nella maggior parte dei casi, tali prodotti assicurativi sono prestati nella forma cd. "claims made" (letteralmente "a richiesta fatta"), per la quale il sinistro coincide con la richiesta di risarcimento del danno avanzata dal terzo (per maggiori informazioni, cfr.: https://it.wikipedia.org/wiki/Claims_made)

CAPITOLO 2 di Deborah Bolco, Mariangela Papadia e Eva Reggiani

Gli attori della privacy: ruoli e responsabilità dentro e fuori dall'azienda.

Gli attori della privacy: ruoli e responsabilità dentro e fuori dall'azienda. Continuità o rottura col passato?

SOMMARIO: 1. Introduzione – 2. Il titolare del trattamento – 3 Il responsabile (esterno) del trattamento – 4 Il sub-responsabile del trattamento – 5 I soggetti designati – 5a: Il responsabile (interno) del trattamento – 5b: Gli incaricati del trattamento

1. Introduzione

L'entrata in vigore del Regolamento (EU) n. 2016/679 (il "GDPR"), pur ponendosi in sostanziale continuità con molte delle disposizioni contenute nella direttiva 95/46/CE (la "Direttiva") e nel decreto legislativo n. 196 del 30 giugno 2003 (il "Codice Privacy"), ha determinato una "rivoluzione copernicana" [220] nel quadro normativo europeo in materia di protezione dei dati personali su più fronti, comportando un radicale mutamento di prospettiva per quanto concerne la gestione del rischio connesso al trattamento di dati personali. In tale contesto, la corretta identificazione dei ruoli dei soggetti coinvolti nelle attività di trattamento dei dati personali gioca un ruolo fondamentale [221].

Nonostante le caratteristiche soggettive di titolare e responsabile del trattamento restino essenzialmente immutate rispetto al regime previgente, è pur vero che il GDPR ha imposto nuovi obblighi sia in capo a entrambe le

220 L'espressione è stata coniata da C. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, in Bloomberg BNA Privacy and Security Law Report* (2012) February 6 2012, consultabile al seguente link https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781

221 Cfr. il considerando n. 79 del GDPR il quale prevede che "*la protezione dei diritti e delle liberà degli interessati così come la responsabilità generale di titolari del trattamento e responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento*". Cfr. altresì A. D'Ottavio, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato – Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019, p. 145 e ss.. Tra l'altro, da un punto di vista generale, l'individuazione di chi operi come titolare o responsabile del trattamento rileva anche ai fini dell'individuazione dell'ambito territoriale di applicazione del GDPR (cfr. art. 3 del GDPR).

figure [222] sia per quanto concerne la regolamentazione dei rapporti (i) fra titolare del trattamento e responsabile del trattamento [223], (ii) fra contitolari del trattamento [224], nonché (iii) fra responsabile e sub-responsabile del trattamento [225].

Analizzeremo, dunque, le caratteristiche di ciascuna figura coinvolta nelle attività di trattamento di dati personali alla luce delle disposizioni del GDPR nonché del novellato Codice Privacy [226] al fine di identificare gli elementi di continuità e di discontinuità rispetto alla disciplina previgente in materia di protezione dei dati personali.

2. Il titolare del trattamento

Il titolare del trattamento costituisce *"il centro di imputazione delle decisioni in ordine al trattamento dei dati da esso effettuato"* [227] ed è colui il quale risponde in via generale dell'osservanza delle norme in materia di protezione dei dati personali [228].

Gli adempimenti che il GDPR attualmente impone al titolare del trattamento sono estremamente più onerosi rispetto a quanto era richiesto in precedenza, non soltanto in considerazione della maggiore particolarizzazione di obblighi già esistenti, ma anche (e soprattutto) alla luce della sostanziale traslazione sul titolare del trattamento delle valutazioni e analisi concernenti sia i rischi connessi alle attività di trattamento sia l'individuazione delle misure tecniche e organizzative idonee a mitigare tali rischi [229]. Sul punto, è stato rilevato

222 Tale mutamento di approccio è particolarmente evidente nel caso del responsabile del trattamento, in quanto il GDPR, a differenza della Direttiva, pone taluni specifici obblighi in capo ai responsabili del trattamento (*e.g.*, la tenuta del registro delle attività di trattamento ex art. 30 del GDPR e la nomina del *data protection officer*, qualora ricorrano i presupposti di cui all'art. 37 del GDPR oppure ciò sia imposto dal diritto nazionale). Sul punto, cfr. *infra* cap. 3.

223 Cfr. l'art. 28 del GDPR il quale indica i contenuti inderogabili minimi che il contratto (o altro atto giuridico) che vincola il responsabile del trattamento al titolare del trattamento deve contenere (v. *infra* cap. 3).

224 Cfr. l'art. 26 del GDPR il quale prevede che i contitolari del trattamento debbano stipulare un accordo interno (v. *infra* cap. 2).

225 Cfr. l'art. 28(4) del GDPR (v. *infra* cap. 4).

226 Cfr. il decreto legislativo n. 101 del 10 agosto 2018 recante "*disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

227 Cfr. L. Greco, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 252.

228 Cfr. il considerando n. 74 del GDPR il quale prevede che "*è opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche*".

229 Basti pensare, ad esempio, all'abrogazione dell'istituto della verifica preliminare ex art. 17 del Codice Privacy. Tale norma prevedeva che il titolare del trattamento dovesse consultare preventivamente il Garante per la protezione dei dati personali qualora il trattamento che si intendeva svolgere presentasse "*rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare*". All'esito di tale verifica preliminare, il Garante prescriveva le misure e gli accorgimenti che il titolare del trattamento avrebbe dovuto attuare per poter procedere al trattamento. Nel quadro attuale, invece, spetta in primo luogo al titolare

come il titolare del trattamento dovrebbe adottare quanto più possibile una "*visione integrata* [del trattamento] *che combin*[i] *competenze tecniche e informatiche con competenze giuridiche ed organizzative* […] [e] *che, nel valutare l'adeguatezza delle misure da approntare, impone al titolare di tenere in considerazione non solo le singole concrete attività di trattamento, ma più in generale 'la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*'" [230].

Venendo ora alla definizione di titolare del trattamento contenuta nel GDPR [231], essa si compone di tre elementi fondamentali [232]:

a) il soggetto ("*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo*");

b) la determinazione "[del]*le finalità e* [dei] *mezzi del trattamento*"; e

c) la circostanza che tale determinazione venga effettuata "*singolarmente o insieme ad altri*".

a) Il soggetto ("la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo")

Come precisato dal Garante per la protezione dei dati personali (il "Garante"), nel caso di persone giuridiche o enti (e a prescindere dalla forma giuridica adottata da queste ultime [233]), il titolare del trattamento è la persona giuridica o l'ente "*nel suo complesso*" poiché è a tale persona giuridica o ente che "*competono le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza*". Ciò in quanto la "*persona fisica*" cui fa riferimento la definizione normativa è quella che "*assum*[e] *individualmente la piena responsabilità*" dell'attività

del trattamento valutare, ai sensi dell'art. 35 del GDPR, il rischio inerente al trattamento e individuare autonomamente le misure tecniche e organizzative necessarie per mitigare tale rischio. Soltanto nel caso in cui, nonostante l'adozione di tali misure tecniche e organizzative, il rischio resti elevato, il titolare del trattamento dovrà consultare l'autorità (cfr. art. 36 del GDPR).

230 Cfr. L. Greco, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 257.

231 Cfr. l'art. 4, n. 7 del GDPR il quale definisce il titolare del trattamento come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*". Tale definizione è sostanzialmente coerente con quanto già previsto dall'art. 4, comma 1, lett. f) – ora abrogato - del Codice Privacy, a mente del quale il titolare del trattamento era definito come "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*". In proposito, è stato osservato come la terminologia italiana possa apparire "fuorviante" rispetto alla terminologia inglese, in quanto "*il* Data Controller *non è infatti titolare, padrone, dei dati, ma solamente titolare "del trattamento dei dati*", i quali restano però di esclusiva "p*roprietà" del soggetto a cui si riferiscono, che in termini privacy si definisce l'interessato (in inglese, a sua volta, è il* Data Subject)" (cfr. R. Panetta, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato – Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019, p. 17).

232 Cfr. Gruppo di Lavoro Articolo 29 (il "WP29"), *Parere 1/2010 sui concetti di "responsabile del trattamento*" e "*incaricato del trattamento*", adottato il 16 febbraio 2010 (il "Parere 1/2010", consultabile al seguente *link* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_it.pdf).

233 Cfr. P. Voigt e A. von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, Cham, 2017, p. 18.

di trattamento e non già la persona fisica legittimata a manifestare la volontà della persona giuridica all'esterno [234].

A parere di chi scrive, giova precisare che società appartenenti a un medesimo gruppo non costituiscono articolazioni interne di un unico titolare del trattamento, bensì soggetti distinti [235]. Ciò in quanto, nel mondo della *data protection*, la teoria del gruppo ha una rilevanza limitata [236]. Pertanto, in assenza di esenzioni *ad hoc* relative al trasferimento di dati personali fra diverse società appartenenti al medesimo gruppo [237], la circolazione di dati personali infragruppo si configura come comunicazione di dati a terzi che, per essere effettuata lecitamente, necessita, *inter alia*, di un'idonea base giuridica. In proposito, è interessante notare come il GDPR preveda espressamente che titolari del trattamento facenti parte di un medesimo gruppo imprenditoriale o di enti collegati a un organismo centrale possano avere "*un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti*" [238]. Tuttavia, giova ricordare che la sussistenza di una base giuridica del trattamento non comporta necessariamente l'automatica sussistenza di una valida base giuridica per poter lecitamente trasferire tali dati personali al di fuori dello Spazio Economico Europeo [239].

234 Cfr. il provvedimento del Garante "*Titolare, responsabile e incaricato – individuazione del "titolare del trattamento"*" – 9 dicembre 1997 (doc. web n. 30915, consultabile al seguente *link* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/30915) ove il Garante precisa che "*il riferimento alla "persona fisica" che compare nella definizione del "titolare" […] non riguarda coloro che amministrano o rappresentano la persona giuridica, la pubblica amministrazione o l'ente, ma concerne gli individui che effettuano un trattamento di dati a titolo personale (ad esempio, il libero professionista, il piccolo imprenditore), e che assumono individualmente la piena responsabilità di un'attività che va distinta nettamente, anche sul piano giuridico, da quella che singole persone fisiche possono coordinare nell'ambito e nell'interesse di una persona giuridica, di un'impresa o di un ente nel quale ricoprono incarichi di rilievo. In altre parole, qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.) anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante ecc.)*.". Cfr. altresì il provvedimento "*Titolare, responsabile e incaricato – individuazione del "titolare del trattamento"*" – 9 dicembre 1997 (doc. web n. 39785, consultabile al seguente *link* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785) e le *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*" – 14 giugno 2007 (doc. web n. 1417809, consultabile al seguente *link* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1417809).

235 Cfr. il provvedimento *Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011* del Garante (doc. web n. 1813953, consultabile al seguente *link* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953): "*il flusso di dati personali riferiti ai clienti nell´ambito di gruppi si configura come comunicazione a terzi*" mentre "*il flusso di dati tra diverse agenzie o filiali di una stessa banca costituisce circolazione di informazioni all´interno di un unico titolare del trattamento e, non configurando un´operazione di comunicazione di dati a terzi, non richiede il consenso degli interessati*". Cfr. altresì il *Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018, pubblicato dall'Agenzia dell'Unione europea per i diritti fondamentali*, Bruxelles, p. 125.

236 Ad esempio, la nozione di gruppo di impresa rileva nel contesto delle norme vincolanti d'impresa (o *binding corporate rules*) di cui all'art. 47 del GDPR, le quali costituiscono una delle "garanzie adeguate" che consentono di trasferire lecitamente dati personali verso un paese terzo in mancanza di una decisione di adeguatezza della Commissione Europea (cfr. l'art. 46(2(b) del GDPR).

237 Cfr. P. Voigt e A. von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, Cham, 2017, p. 135.

238 Cfr. il considerando n. 48 del GDPR.

239 Ed invero, il considerando n. 48 precisa che "*sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in paese terzo*".

Da ultimo, si segnala che l'art. 4(2)(c) del GDPR prevede l'inapplicabilità del GDPR alle attività di trattamento effettuate "*da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico*" e che, dunque, non hanno "*una connessione con un'attività commerciale o professionale*" [240]. Fra le attività che potrebbero esservi ricomprese, il considerando n. 18 del GDPR indica, a titolo esemplificativo, "*la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività*".

Preliminarmente si osserva che tale esenzione c.d. "domestica" non è una novità assoluta, in quanto già prevista nella Direttiva [241] e, conseguentemente (seppur con qualche differenza) [242] anche nel Codice Privacy [243]. Ciò che è nuovo è il riferimento all'utilizzo di social network e ad attività online.

Da un punto di vista generale, la valutazione di quali attività abbiano carattere esclusivamente personale o domestico dipende dalle circostanze concrete [244]. In passato, il WP29 aveva proposto una formulazione alternativa del considerando che nell'allora bozza di regolamento [245] riguardava l'esenzione domestica. La formulazione alternativa suggerita dal WP29 indicava una serie di circostanze da prendere in considerazione per valutare se un'attività di trattamento ricadesse o meno nella predetta esenzione, quali, ad esempio: (i) se vi fosse stata comunicazione di dati personali a un numero indefinito di persone oppure a una ristretta cerchia di amici, familiari o conoscenti; (ii) se i dati personali oggetto di comunicazione riguardassero individui che non hanno alcuna relazione di tipo personale con il soggetto che li pubblica; e (iii) se la scala e la frequenza dell'attività di trattamento fossero tali da suggerire un'attività professionale o a tempo pieno [246].

240 Cfr. il considerando n. 18 del GDPR.

241 Cfr. l'art. 3(2) il quale prevedeva l'inapplicabilità delle disposizioni della Direttiva "*ai trattamenti di dati personali* […] *effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico*". Cfr. altresì il considerando n. 12 ("[…] *deve essere escluso il trattamento di dati effettuato da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico quali la corrispondenza e la compilazione di elenchi di indirizzi*").

242 Cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 37.

243 Cfr. l'art. 5, comma 3 (ora abrogato) del Codice Privacy il quale prevedeva che "*il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati personali sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31*".

244 Cfr. M*anuale sul diritto europeo in materia di protezione dei dati*, edizione 2018, pubblicato dall'Agenzia dell'Unione europea per i diritti fondamentali, Bruxelles, p. 116.

245 Ci si riferisce alla bozza di regolamento approvata il 25 gennaio 2012 (consultabile al seguente *link* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:IT:PDF) il cui considerando n. 15 prevedeva che "*Il presente regolamento non deve applicarsi al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività esclusivamente personali o domestiche, quali la corrispondenza e gli indirizzari, e senza scopo di lucro, vale a dire senza alcuna connessione con un'attività commerciale o professionale*".

246 Cfr. Annex 2 *Proposals for Amendments regarding exemption for personal or household activities* del WP29 del 27 febbraio 2013 (consultabile al seguente *link* https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf), p. 10 ("[…] *In determining whether the processing falls within the exemption, consideration should be given to whether the personal data is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances; whether the personal data is about individuals who have no personal or household relationship with the person posting it; whether the scale and frequency of the processing of personal data suggests professional or full-time activity* […]"). Tra l'altro, a parere di chi scrive tale approccio del WP29 è in linea con la posizione precedentemente assunta in relazione all'applicabilità o meno (e, se sì, in che termini)

In considerazione di quanto sopra e in attesa di pronunce della Corte di Giustizia Europea che interpretino le norme del GDPR sul punto, a parere di chi scrive sembra condivisibile la posizione interpretativa di coloro i quali ritengono che l'esenzione domestica così come formulata nel GDPR debba essere interpretata nel senso di applicarsi "*quando sia la raccolta dei dati personali sia la loro circolazione si mantengano all'interno di una sfera* puramente *personale o domestica, anche non necessariamente materiale*" [247].

b) La determinazione "[del]*le finalità e* [dei] *mezzi del trattamento*"

La cifra che contraddistingue la figura del titolare del trattamento dal responsabile del trattamento consiste nel potere decisionale su finalità e mezzi del trattamento.

Come chiarito dal WP29, qualificare un determinato soggetto come titolare del trattamento presuppone un'analisi di tipo fattuale e non formale [248]. Ciò in quanto la qualifica di titolare non richiede una designazione, una nomina o una formalizzazione, poiché tale qualifica discende dalla "*circostanza fattuale di procedere a un trattamento di dati personali e di avere le prerogative decisorie inerenti a quel trattamento*" [249] e, dunque, non è liberamente allocabile per contratto in capo a una delle parti [250]. Del resto, il WP29 ha altresì precisato che "*in caso di dubbio,*

dell'esenzione domestica nel contesto delle attività di trattamento effettuate da una persona fisica mediante *social network* (cfr. *Parere 5/2009* sui social network on-line, adottato dal WP 29 il 12 giugno 2009 (consultabile al seguente *link* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_it.pdf), in cui il WP29 aveva chiarito che "*quando l'accesso alle informazioni del profilo non si limita ai contatti scelti, come nel caso in cui tutti gli iscritti al [social network] hanno la possibilità di consultare un profilo o i relativi dati possono essere indicizzati da motori di ricerca, si oltrepassa la sfera personale o domestica. Analogamente se un utente decide con cognizione di causa di non limitare l'accesso ad "amici" scelti, assume gli obblighi di un [titolare] del trattamento*").

247 Cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 39. Cfr. altresì il punto n. 27 della Relazione esplicativa della Convenzione n. 108 modernizzata (consultabile al seguente *link* https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a), ove si precisa che la condivisione di informazioni all'interno della sfera personale ricomprende la condivisione all'interno della famiglia, di una cerchia ristretta di amici o di una cerchia numericamente ristretta di persone e fondata su una relazione di carattere personale oppure sulla base di una particolare relazione di fiducia ("*The sharing of data within the private sphere encompasses notably the sharing between a family, a restricted circle of friends or a circle which is limited in its size and based on a personal relationship or a particular relation of trust*").

248 Cfr. il Parere 1/2010, p. 10. Cfr. altresì la *Risposta a un quesito relativo al ruolo del consulente del lavoro dopo la piena applicazione del Regolamento (UE) 679/2016* resa dal Garante il 22 gennaio 2019 (consultabile al seguente *link* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970: "*L'Autorità, vigente la precedente disciplina, si è espressa sulla qualificazione in termini di titolare o responsabile di alcune figure che effettuano trattamenti di dati personali, anche nell'ambito del rapporto di lavoro, all'esito dell'esame – effettuato sul piano sostanziale e non formale – delle attività in concreto svolte*").

249 Cfr. G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, p. 81. Cfr. altresì L. Greco, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 252.

250 Cfr. il Parere 1/2010, p. 12 ("*Può accadere che un contratto non indichi chi è il [titolare] del trattamento, ma contenga elementi sufficienti per assegnare tale qualifica a una parte che risulta esercitare un ruolo dominante. Può anche accadere che il contratto sia più esplicito quanto alla designazione del [titolare] del trattamento: se non vi sono ragioni di dubitare che le clausole interessate non rispecchino accuratamente la realtà dei fatti, nulla impedisce di applicare le condizioni del contratto. Tuttavia, le clausole di un contratto non sono sempre decisive, poiché ciò consentirebbe alle parti di assegnare le responsabilità nel modo più conveniente. […] il fatto stesso che qualcuno determini le modalità del trattamento dei dati personali può far scattare la qualifica di [titolare] del trattamento, anche se al di fuori dell'ambito di una relazione contrattuale o anche se esplicitamente esclusa dal contratto.*"). Cfr. altresì A. D'Ottavio, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole*

per individuare il [titolare] del trattamento si possono esaminare anche altri elementi extracontrattuali, come il grado di controllo reale esercitato da una parte, l'immagine data agli interessati e il legittimo affidamento di questi ultimi sulla base di questa visibilità […]" [251].

Ciò premesso, si tratta però di comprendere che cosa significhi, in concreto, determinare finalità e mezzi del trattamento: in proposito, il WP29 ha precisato che "*determinare le finalità e gli strumenti equivale a determinare il 'perché' e il 'come' di certe attività di trattamento*" [252], a prescindere dalla circostanza che il titolare del trattamento tratti effettivamente i dati personali o vi abbia accesso [253].

Tuttavia, se è vero che il potere decisionale sul "perché" del trattamento farebbe scattare comunque la qualifica di titolare del trattamento [254], è altrettanto vero che non un qualsiasi potere decisionale sul "come" è sufficiente: ciò in quanto il "come" del trattamento rilevante ai fini della qualificazione come titolare del trattamento non riguarda solo gli aspetti meramente tecnici ed esecutivi delle attività di trattamento, ma concerne anche gli "*elementi essenziali tradizionalmente e intrinsecamente riservati al* [titolare] del *trattamento, come 'quali dati trattare?', 'per quanto tempo trattarli?', 'chi vi ha accesso?'*" [255].

c) La determinazione di finalità e mezzi del trattamento effettuata "*singolarmente o insieme ad altri*": i contitolari del trattamento

Ad avviso di chi scrive, l'aspetto più interessante della terza componente della definizione di titolare del trattamento risiede nell'ipotesi in cui più titolari del trattamento determinino congiuntamente mezzi e finalità dell'attività di trattamento: ciò non tanto per quanto riguarda la nozione di contitolarità – già contemplata dalla Direttiva – quanto per le ricadute pratiche che, alla luce del GDPR, la contitolarità comporta.

Preliminarmente appare opportuno chiarire che la contitolarità non presuppone una ripartizione simmetrica fra contitolari, delle determinazioni circa finalità e mezzi del trattamento, in quanto "*la*

del mercato – Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy), Milano, 2019, p. 150. In proposito, cfr. anche G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, p. 82, la quale ha precisato come "*la titolarità del trattamento dei dati personali non è cedibile né attraverso un atto di natura convenzionale, né altrimenti*.".

251 Cfr. il *Parere* 1/2010, p. 12.

252 Cfr. il *Parere* 1/2010, p. 13

253 Cfr. il Parere 1/2010, p. 23 ("[…] *il fatto d'avere accesso ai dati non è un prerequisito per essere* [titolare] *del trattamento*."). Cfr. altresì la sentenza resa dalla Corte di Giustizia Europea ("CGUE") resa il 5 giugno 2018 nel caso C-210/16 in cui la CGUE, ravvisando la contitolarità nel trattamento fra l'amministratore di una *fanpage* su Facebook e Facebook Ireland e Facebook Inc., ha precisato che "[…] *la direttiva 95/46 non impone che, qualora vi sia una* [titolarità] congiunta di uno o più operatori per un medesimo trattamento, ciascuno abbia accesso ai dati personali *interessati*".

254 Cfr. il *Parere* 1/2010, p. 14.

255 Cfr. il *Parere* 1/2010, p. 14

partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale" [256].

In caso di contitolarità, l'art. 26 del GDPR prevede l'obbligo [257], in capo ai contitolari, di determinare mediante un accordo interno "*le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal* [GDPR]*, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14*" del GDPR, con la facoltà di designare un punto di contatto al quale gli interessati potranno rivolgersi per esercitare i diritti loro riconosciuti dal GDPR. Tale accordo dovrà "*riflette*[re] *adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati*" [258]. Tuttavia, la norma non precisa quali, fra gli obblighi derivanti dal GDPR ulteriori rispetto alla gestione delle richieste di esercizio dei diritti da parte degli interessati e agli obblighi informativi *ex* artt. 13 e 14 del GDPR, possano (o debbano) essere ricompresi in tale accordo interno.

In proposito, si osserva che per quanto attiene all'effettuazione della valutazione di impatto *ex* art. 35 del GDPR ("DPIA") e agli obblighi di notifica del data breach *ex* artt. 33 e 34 del GDPR, il WP29 ha fornito alcune indicazioni. Più precisamente, circa la DPIA, ha precisato che "[q]*ualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità*" [259]. Mentre per quanto attiene agli obblighi di notifica del *data breach ex* artt. 33 e 34 del GDPR, il WP29 ha precisato che l'accordo fra contitolari dovrà includere la

256 Cfr. il *Parere* 1/2010, p. 20 ("[…] *si è in presenza di una situazione di [contitolarità] quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti che caratterizzano il* [titolare] *del trattamento* […]. *Nel contesto della [contitolarità], comunque, la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale. In effetti, quando vi è una pluralità di attori, questi possono avere una relazione molto stretta (condividendo, ad esempio, tutte le finalità e tutti gli strumenti di un trattamento) o più distante (condividendo, ad esempio, solo le finalità o i mezzi, o una parte di essi).*"). Cfr. altresì la sentenza della CGUE resa il 5 giugno 2018 nel caso C-210/16 in cui la CGUE, al paragrafo n. 36, osserva che "[…] *la creazione di una fanpage su Facebook implica da parte del suo amministratore un'azione d'impostazione dei parametri in base, segnatamente, al suo pubblico destinatario nonché agli obiettivi di gestione o di promozione delle sue attività , che influisce sul trattamento di dati personali ai fini della creazione di statistiche stabilite a partire dalle visite della fanpage. Tale amministratore può, tramite filtri messi a disposizione da Facebook, definire i criteri a partire dai quali si devono stabilire tali statistiche e designare perfino le categorie di persone i cui dati personali saranno oggetto di utilizzo da parte di Facebook. Di conseguenza, l'amministratore di una fanpage presente su Facebook contribuisce al trattamento dei dati personali dei visitatori della sua pagina*".

257 In proposito, si osserva che, ai sensi dell'art. 83(4)(a) del GDPR, l'inosservanza di tale obbligo è punibile con una sanzione amministrativa fino a € 10.000.000 o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

258 Cfr. l'art. 26(2) del GDPR.

259 Cfr. le *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* del WP29 adottate il 4 ottobre 2017 (consultabili al seguente *link* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236), p. 8.

determinazione di chi, fra i contitolari, dovrà procedere a tale notifica, raccomandando che "*gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento*" [260].

L'art. 26(2) del GDPR prevede che il contenuto essenziale di tale accordo interno dovrà essere "*messo a disposizione dell'interessato*", senza, tuttavia, precisare in quale modo tale messa a disposizione debba avvenire né quali informazioni ulteriori rispetto a quelle di cui agli artt. 13 e 14 del GDPR debbano essere fornite agli interessati. Sul punto, parte della dottrina ha sostenuto che i punti essenziali dell'accordo potrebbero essere resi disponibili sui siti internet di ciascun contitolare del trattamento .Tuttavia, ad avviso di chi scrive sembra maggiormente condivisibile la posizione interpretativa di coloro i quali ritengono che il contenuto essenziale dell'accordo andrebbe incorporato nell'informativa ex artt. 13 e 14 del GDPR, "*evita*[ndo] *di reiterare le informazioni di cui gli interessati siano già a conoscenza* [ed] *evidenziando, invece, alcune utili precisazioni sui termini della contitolarità, come ad esempio le specifiche operazioni di trattamento rispetto alle quali si sostanzia la contitolarità e le rispettive responsabilità dei (con)titolari con riferimento agli obblighi previsti dal* [GDPR]" [261].

Infine, per quanto riguarda l'opponibilità di tale accordo interno a terzi, si osserva che l'art. 26(3) del GDPR prevede che l'interessato possa esercitare i diritti garantiti dal GDPR nei confronti di ciascun contitolare a prescindere da quanto previsto dall'accordo. Inoltre, l'art. 82(4) del GDPR,"*al fine di garantire il risarcimento effettivo dell'interessato*", prevede la responsabilità solidale nei confronti dell'interessato di ciascun contitolare del trattamento per l'intero ammontare del danno [262].

260 Cfr. le *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679* del WP29 adottate il 6 febbraio 2018 (consultabili al seguente *link* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052), p. 14.

261 Cfr. A. D'Ottavio, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato – Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019, p. 160. Cfr. altresì E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 139 il quale precisa che "*deve ritenersi che la dichiarazione del rapporto di contitolarità e le informazioni essenziali debbano essere fornite all'interessato già con l'informativa e vadano poi ulteriormente rese in occasione dell'accesso ai dati personali*".

262 Cfr. art. 82(4) del GDPR il quale prevede che "q*ualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato*". Per la rilevanza di tale accordo interno, nei rapporti fra contitolari, in caso di esercizio dell'azione di regresso, cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 136.

3. Il Responsabile (esterno) del trattamento dei dati

Un'altra figura chiave per lo svolgimento delle attività sui dati personali è quella del Responsabile del trattamento dei dati (o *Data Processor*), ovvero il soggetto designato dal Titolare che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. Ai sensi dell'art. 4(8) del GDPR, il Responsabile è la persona fisica o giuridica, pubblica o privata, riconosciuta o no, che svolge attività di trattamento *per conto* del Titolare [263]. Il citato art. 4 non ha innovato in alcun modo la nozione di Responsabile del trattamento rispetto al passato, ripropone in maniera pressoché identica la definizione contenuta all'art. 2, lett. e) della Direttiva 95/56/CE [264]. Ciò che ha fatto il GDPR è intervenire significativamente sulla disciplina di tale figura, attribuendogli maggiore rilevanza esterna e maggiore responsabilità nella gestione del trattamento dei dati.

In particolare, l'art. 28 del GDPR individua in modo più puntuale di quanto non facesse la disciplina previgente sia gli imprescindibili elementi soggettivi per la corretta individuazione del Responsabile sia le caratteristiche e il contenuto dell'atto di designazione.

a) Le caratteristiche soggettive del responsabile

L'art. 28 del GDPR prevede al primo comma quali debbano essere i requisiti soggettivi del responsabile del trattamento che vengono individuati nelle "*garanzie sufficienti*" per mettere in atto le misure tecniche e organizzative adeguate nonché garantire la tutela dei diritti dell'interessato. In termini generali è il Titolare che designa il Responsabile del trattamento (e, come si dirà nel prosieguo, quest'ultimo potrà invece designare altri (sub)Responsabili del trattamento) e, poiché il Titolare del trattamento risponde della gestione effettuata dal responsabile, è fondamentale, come descritto nel considerando 81 del GDPR [265], che il Responsabile dimostri di avere una competenza qualificata (ad esempio, frequentazione di corsi di aggiornamento), e garantisca una particolare affidabilità, un requisito fondato su aspetti etici

263 Come specificato dal WP29, con il *Parere* 1/2010, p. 25: "*Per poter agire come incaricato del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal responsabile del trattamento ed elaborare i dati personali per conto di quest'ultimo. Questa attività di trattamento può essere limitata a un compito o a un contesto molto specifici o può essere più generale ed ampia*".

264 L'art. 2, lett. e) della Direttiva 95/56/CE definisce il responsabile del trattamento come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento*".

265 In base al considerando 81 del GDPR, "*Per garantire che siano rispettate le prescrizioni del presente regolamento (…), quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento.* (…)". Inoltre, l'art. 28(5) del GDPR prevede che l'adesione da parte del responsabile a un codice di condotta o a un meccanismo di certificazione può essere utilizzato come elemento per dimostrare le garanzie sufficienti.

e deontologici (ad esempio, l'assenza di condanne penali). Ovviamente dovrà anche disporre delle risorse necessarie per l'attuazione e la piena osservanza degli obblighi derivanti dall'atto di designazione e dalle norme in materia al fine di mitigare il rischio connesso al trattamento dei dati da lui effettuato. Di conseguenza, il responsabile deve avere a disposizione risorse sufficienti in termini di personale, economici e quant'altro necessario a svolgere i compiti affidati dal titolare.

Invero, l'art. 28(1) del GDPR sembrerebbe prevedere una forma di responsabilità *per culpa in eligendo* del Titolare: la previsione del Regolamento in base alla quale il titolare deve avvalersi di "*responsabili del trattamento che presentino garanzie sufficienti*" per la piena tutela dei diritti degli interessati richiama proprio il concetto di una responsabilità del titolare per eventuali danni causati dall'attività di trattamento svolta dal Responsabile che dovesse disattendere i requisiti di idoneità e adeguatezza, rilevandosi così incompetente, inesperto o comunque non sufficientemente capace [266].

Parimenti, si potrebbe ritenere che il titolare risponda anche di una *culpa in vigilando*, sebbene non espressamente enunciata: fra le istruzioni che il Titolare impartisce al Responsabile, infatti, è obbligatoria anche quella che prevede di poter svolgere, direttamente e/o indirettamente, attività di revisione e ispezione, derivando, nell'ipotesi di mancato controllo, una responsabilità per *culpa in vigilando*.

Alla luce del quadro appena esposto, sembrerebbe che l'obiettivo del Regolamento fosse quello di garantire all'interessato una piena tutela nel caso di danni subiti a causa della condotta del Responsabile: infatti, "*il diritto dell'interessato al risarcimento del danno risulta in tutti i casi poter essere potenzialmente soddisfatto, sia che quest'ultimo si rivolga al titolare sia che si confronti con il responsabile*" [267]

b) L'atto di designazione

Con riferimento alla designazione, la stessa deve avvenire per contratto o altro atto giuridico, scritto, stipulato anche in forma elettronica, con cui si vadano a disciplinare tassativamente le tematiche riportate al paragrafo 3 dell'articolo 28 del GDPR, ovvero, in estrema sintesi:

- la materia disciplinata
- la durata, natura e finalità del trattamento;
- le categorie dei dati oggetto del trattamento;
- e categorie di interessati;

266 Cfr. L. Greco, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 264 e ss.

267 Cfr. L. Greco, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 265.

- gli obblighi e diritti del titolare;
- le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e del Regolamento.

In altri termini, nell'atto di designazione si possono distinguere previsioni che attengono agli obblighi di assistenza in favore del titolare nello svolgimento delle attività di trattamento (lett. e), f) e h) dell'art. 28 del GDPR) [268] e previsioni che attengono all'obbligo di garantire la sicurezza e la riservatezza (lett. b), c), d) e g) dell'art. 28 del GDPR) [269].

Un cenno a parte merita l'ulteriore previsione in base alla quale il Responsabile deve agire nel trattamento dei dati solo "*su istruzione documentata*" del Titolare (lett. a) dell'art. 28 del GDPR). Come noto, l'elemento cardine del ruolo del responsabile "*consiste nella strumentalità rispetto alla finalità decisa dal titolare. Per questa ragione, il Responsabile deve attenersi nel trattamento dei dati alle istruzioni del titolare* [cfr anche art. 29 del GDPR]*, benché, a seconda del tipo di incarico ricevuto o di contratto, possa disporre di un margine discrezionale nella determinazione dei mezzi del trattamento*" [270] . D'altronde, l'elemento più importante che consente la qualificazione del soggetto quale Responsabile sta nel fatto che il suo intervento deve avvenire "…per conto del Titolare del trattamento…". Intervenire "per conto di…" significa, come rilevato anche dal WP29, "*servire gli interessi di un altro soggetto, e ciò richiama il concetto giuridico di "delega". Nel caso della normativa sulla protezione dei dati,* [il responsabile del trattamento] *deve attuare le istruzioni ricevute dal* [titolare] *del trattamento almeno per quanto attiene alla finalità del trattamento stesso e agli aspetti fondamentali dei mezzi*" [271]. Tanto è vero che, laddove il Responsabile dovesse andare oltre il proprio mandato e fuoriuscire dall'alveo della

268 Segnatamente, quanto agli obblighi di assistenza, le lettere e), f) e h) dell'art. 28 del GDPR prevedono che il responsabile del trattamento:
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

269 Quanto agli obblighi di sicurezza e riservatezza, le lett. b), c), d) e g) dell'art. 28 del GDPR prevedono che il responsabile del trattamento:
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati

270 Cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 146

271 Cfr. il *Parere* 1/2010, p. 26

strumentalità, usando i dati per finalità e mezzi propri, il Responsabile andrebbe a collocarsi in una posizione assimilata a quella del titolare (o del titolare autonomo o del contitolare), così come prevede l'art. 28(10) del GDPR, determinando l'applicazione delle disposizioni relative.

Non è un caso che il Regolamento abbia previsto in maniera così dettagliata il contenuto dell'atto di designazione, indicando una serie di previsioni inderogabili: invero, sono diverse le situazioni in cui sussiste un certo sbilanciamento tra la posizione del titolare e quella responsabile del trattamento che inevitabilmente potrebbe riflettersi nel contenuto dell'atto di designazione. Si pensi, ad esempio al grande fornitore di servizi, che tratta dati in qualità di responsabile del trattamento, da un lato, e agli utenti di tali servizi, quali titolari del trattamento: in tali situazioni, la forza negoziale di ciascun titolare del trattamento è assai ridotta con la conseguenza che l'utente/titolare si vedrebbe costretto ad aderire allo schema di designazione predisposto unilateralmente dal fornitore/responsabile del trattamento. In tale contesto si inseriscono gli artt. 28(7) e 28(8) che introducono la possibilità per la Commissione europea o le Autorità garanti di predisporre "clausole contrattuali tipo" per la designazione a responsabile che riproducano i contenuti minimi indicati dall'art. 28(3) del GDPR. L'adozione di tali modelli appare senza dubbio una soluzione idonea in quelle particolari situazioni in cui, ad esempio, titolare e responsabile faticano a trovare un accordo sul contenuto dell'atto di designazione. Va da sé che le parti potranno integrare, ove ritenuto opportuno, le clausole dei modelli, purché tali interventi non alterino i contenuti fissati dalla legge [272].

Come accennato, nel caso di trattamento in violazione delle norme del Regolamento europeo, il responsabile, da un lato, è passibile di sanzione amministrativa pecuniaria nella misura prevista dall'art. 83 del GDPR [273]; dall'altro, risponde per il danno cagionato all'interessato. Con riferimento a tale ultimo profilo, per esemplificare, il responsabile potrebbe rispondere nei casi in cui:

- travalica le istruzioni del titolare;
- agisce in contrasto con le istruzioni del titolare;
- non assiste il titolare (ad esempio per le violazioni dei dati o la valutazione di impatto);
- non pone a disposizione del titolare le informazioni necessarie per un audit;

272 Cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 147 e ss.

273 Quanto all'ammontare della sanzione pecuniarie, cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 146 laddove si afferma che "*L'inadempimento del responsabile ai suoi obblighi è sanzionato secondo l'art. 83.4.a), ossia fino a € 10.000.000 (dieci milioni) o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*". Mentre, l'inosservanza di un ordine dell'autorità di controllo è sanzionata fino a € 20.000.000 (venti milioni) o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore ai sensi dell'art. 83(5)(e) e 83(6) del GDPR.

- non informa il titolare che una sua istruzione è in violazione della normativa;
- pur essendovi obbligato non designa il DPO;
- designa un sub-responsabile non essendo stato previamente autorizzato;
- designa un sub-responsabile che non presta garanzie sufficienti;
- non tiene il registro dei trattamenti.

Quindi, mentre il titolare è tenuto a risarcire qualsivoglia danno abbia cagionato in virtù della violazione del GDPR nel trattamento dei dati, il responsabile risponde solo se non ha adempiuto agli obblighi a lui specificatamente diretti o ha agito in modo difforme o contrario alle istruzioni del titolare.

L'art. 82 del GDPR [274] prevede, inoltre, un regime di responsabilità solidale tra il titolare e il responsabile, se entrambi i soggetti sono responsabili. In tali casi, tutti i soggetti responsabili sono chiamati a rispondere nei confronti dell'interessato danneggiato in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo. Laddove un titolare del trattamento o un responsabile abbiano risarcito per intero il danno, tale soggetto avrà diritto di agire in regresso verso i titolari o i responsabili del trattamento del pari responsabili del danno, per ottenere il rimborso della quota di risarcimento corrispondente alla loro parte di responsabilità.

Il titolare e il responsabile sono esonerati da responsabilità se dimostrano che l'evento dannoso non è imputabile alla loro condotta, o se dimostrano di aver adottato tutte le misure idonee per evitare il danno stesso.

274 L'art. 82 del GDPR, rubricato '*Diritto al risarcimento e responsabilità*', prevede:
"*1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.*
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.
6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2".

4. Il Sub-Responsabile del trattamento dei dati

Il secondo comma dell'art. 28 del GDPR prevede un'importante novità rispetto al Codice Privacy disponendo che il responsabile possa ricorrere a sua volta ad un nuovo responsabile (c.d. sub-responsabile). Tale novità rende più agevole la ripartizione dei ruoli rispetto alla disciplina anteriore - che prevedeva solo in capo al titolare la possibilità di designare il responsabile -, tenendo in considerazione in modo più attinente alla realtà la pluralità di soggetti che possono intervenire nello svolgimento di un determinato servizio. L'esigenza di tale cambiamento nasce dalla necessità di superare le rigidità e difficoltà manifestatesi ante GDPR a fronte dell'obbligo per il titolare, per un verso, di nominare quale responsabile tutti i soggetti terzi di cui un proprio fornitore si avvaleva nello svolgimento dei propri servizi; per altro verso, di vigilare sull'operato di tutti i soggetti coinvolti nell'attività di trattamento.

Al fine di poter ovviare alla pluralità di passaggi in capo al titolare e per responsabilizzare maggiormente il prestatore di servizi nell'avvalersi di soggetti terzi, il GDPR ha introdotto la figura del sub-responsabile del trattamento. Per potersi avvalere di tali soggetti, il responsabile deve ottenere una previa autorizzazione per iscritto da parte del titolare, che può essere specifica per il singolo responsabile o generale.

Nel primo caso il titolare, al momento del conferimento della suddetta autorizzazione, ha già effettuato le proprie valutazioni in merito all'opportunità e adeguatezza del terzo ad essere nominato sub-responsabile.

In caso di autorizzazione generale, al contrario, il responsabile è tenuto ad indicare al titolare i potenziali sub-responsabili, al fine di dare modo al titolare, entro il tempo concordato nel contratto, di potersi opporre in merito alla nomina. In mancanza di opposizione il responsabile può procedere a nominare il terzo sub-responsabile, mediante apposito contratto o altro atto giuridico vincolante, in cui dovranno essere inseriti i medesimi obblighi in materia di protezione dei dati contenuti nell'accordo stipulato tra titolare e responsabile iniziale.

Il modello adottato dal GDPR ricalca la soluzione adottata dalla Commissione europea in materia di trasferimento dei dati all'estero (cfr. decisione 2010/87/UE) e ricorrente alle clausole contrattuali standard nell'ambito dei rapporti tra esportatore dei dati stabilito in Italia ed importatore dei dati stabilito fuori dell'Unione Europea (i 28 Stati membri dell'UE e quelli dello Spazio Economico Europeo/SEE) [275].

275 Si tratta della Decisione della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio (consultabile al seguente *link* https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32010D0087): ai sensi della citata decisione, in quel caso, con il consenso del titolare del trattamento, il responsabile importatore dei dati, in caso di subcontratto, impone direttamente al proprio subcontraente il rispetto di obblighi in materia di trattamenti dei dati conformi agli obblighi da lui assunti nei confronti del titolare. Inoltre, un'ulteriore applicazione del sopracitato modello si trova nell'opinione 5/2012 in materia di *cloud computing* adottata dal WP29 il 1° luglio 2012 (consultabile al seguente *link* https://www.garanteprivacy.it/documents/10160/2045741/WP+196+-+Parere+052012+sul++cloud+computing.pdf – cfr. p. 22).

Infine, sul responsabile gravano oneri informativi e di aggiornamento circa eventuali modifiche o aggiunte di altri responsabili del trattamento rispetto alle quali il titolare potrà esprimere la propria opposizione.

Il responsabile deve pattuire inoltre con il sub-responsabile garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il relativo trattamento soddisfi i requisiti del GDPR. A norma del Regolamento, a rispondere davanti al titolare di eventuali inadempienze del sub-responsabile è il primo responsabile con cui il titolare ha un rapporto diretto. Dunque, il GDPR pone indirettamente a carico del responsabile iniziale una responsabilità *per culpa in eligendo* e *per culpa in vigilando* che legittimano implicitamente la possibilità per quest'ultimo di impartire istruzioni al sub-responsabile, purché conformi a quelle del titolare e strumentali alle finalità di trattamento.

5. I 'soggetti designati'

5a il Responsabile (interno) del trattamento

Nella vigenza del Codice per la protezione dei dati personali, la nostra prassi applicativa ha conosciuto la figura del responsabile 'interno' del trattamento ovvero il soggetto interno alla struttura del titolare (dipendente o collaboratore) al quale vengono affidate determinate attività in materia di protezione dei dati personal, dotato di una certa autonomina nel determinare i mezzi e le modalità del trattamento, nel rispetto delle finalità individuate dal titolare del trattamento. Tale figura non ha mai trovato definizione a livello normativo, ma risultava compatibile con le definizioni contenute nella Direttiva 95/46/CE e nel previgente Codice Privacy [276].

È inevitabile chiedersi se la figura del responsabile interno sia da considerarsi compatibile con il Regolamento. L'art. 28 e l'impianto generale del regolamento in tema di responsabile del trattamento non consentono di ritenere ammissibile la figura di responsabile del trattamento all'interno dell'organizzazione in quanto il GDPR disciplina in modo molto dettagliato la figura del responsabile del trattamento, introducendo altresì un serie di specifici adempimenti in capo a questa figura: in particolare, l'adozione del il registro delle attività di trattamento, la nomina del DPO sono obblighi necessariamente pensati per un soggetto esterno alla struttura del titolare. In altri termini, molti degli obblighi introdotti dal GDPR e la previsione di un impianto sanzionatorio particolarmente gravoso fanno propendere per la non applicabilità della disciplina nei confronti di un dipendente o collaboratore del titolare [277].

276 Ai sensi dell'art. 4, comma 1, lett. g) del Codice Privacy, si intende "*la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare del trattamento dei dati personali*".

277 Cfr. E. Pelino, in L. Bolognini, E. Pelino e C. Bistolfi, *Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 148

In assenza di una previsione specifica della figura del responsabile interno da parte del GDPR, è con l'introduzione dell'art. 2-*quaterdecies* del nuovo Codice in materia di protezione dei dati personali [278] rubricato "*Attribuzione di funzioni e compiti a soggetti designati*" che il legislatore ha colmato un vuoto aperto dal Regolamento Ue e lo ha fatto sostanzialmente recuperando i contenuti del previgente codice della privacy. Infatti, il comma 1 prevede che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*".

A dirci che si tratta di una conferma sostanziale del regime pregresso è la relazione illustrativa al decreto legislativo n. 101 del 10 agosto 2018, ovvero il decreto che ha adeguato l'ordinamento italiano sulla protezione e circolazione dei dati al GDPR, intervenendo sul testo del Codice Privacy previgente.

Nella relazione si legge, infatti, che la disposizione in questione prevede il potere di titolare e responsabile, di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, dovranno essere espressamente designati. Tale disposizione, prosegue la relazione illustrativa, permette di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione che, ai sensi del previgente codice in materia di protezione dei dati personali ma in contrasto con il regolamento, potevano essere definiti, a seconda dei casi, responsabili o incaricati (per tale ultima figura vedi *infra*) [279].

Per l'effetto, l'impresa può assegnare funzioni privacy a un soggetto apicale; oppure l'impresa può decidere che specifici compiti siano assegnati a una persona fisica espressamente designata. La norma precisa, inoltre, che le persone individuate dal titolare devono essere espressamente designate con l'indicazione analitica dei compiti (così come prevedeva tra l'altro il previgente Codice Privacy). Il soggetto deve essere designato, infatti, per specifici compiti e funzioni: l'atto di designazione non può essere generico, ma deve indicare con esattezza di quali adempimenti si deve occupare il designato.

5b Gli incaricati del trattamento

Un'altra figura particolarmente importante nell'organigramma *privacy* è quella che nell'ancora vigente Codice Privacy è denominata "*incaricato al trattamento dati*", ovvero, ai sensi della lett. h) dell'art. 4 del previgente Codice

278 Il Decreto legislativo 10 agosto 2018, n. 101 - emanato in attuazione dell'articolo 13 della Legge di delegazione europea 2016-2017 (Legge 25 ottobre 2017, 163) - è volto ad armonizzare la disciplina nazionale (il Codice Privacy) alla normativa europea, che è divenuta pienamente operativa a partire dal 25 maggio scorso. Il citato Decreto, pubblicato in G.U. il 4 settembre 2018 ed entrato in vigore il 19 settembre 2018, (i) ha abrogato espressamente le disposizioni del Codice Privacy incompatibili con le disposizioni contenute nel GDPR, tra cui ad esempio gli artt. 4, 28, 29 e 30, e (ii) ha introdotto una serie di penetranti modifiche tra cui il l'art. 2-*quaterdecies* rubricato "*Attribuzione di funzioni e compiti a soggetti designati*".

279 Cfr. Relazione illustrativa dello schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, p. 13 (consultabile al *link*: http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0022_F001.pdf&leg=XVIII#pagemode=none).

Privacy, "*le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile*". Tale soggetto nel GDPR viene qualificato quale "*persona autorizzata al trattamento dei dati personali*" permanendo nella sostanza una identità di ruoli e modalità di nomina. Sul punto la stessa Autorità Garante, nella sua Guida all'applicazione del GDPR, ha stabilito sin da subito che l'organizzazione degli incaricati può permanere immutata. Ha evidenziato sul punto il Garante: "*Pur non prevedendo espressamente la figura dell'"Incaricato" del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento)*". Continua il Garante confermando che "*Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di Titolari e Responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene che Titolari e Responsabili del trattamento possano mantenere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante*" [280]

Dunque, il nuovo Regolamento prevede ai sensi dell'art. 29 "*Trattamento sotto l'autorità del Titolare o del Responsabile*" che, chiunque agisca sotto l'autorità del titolare o del responsabile e che abbia accesso a dati personali non possa trattarli se non è istruito da questi ultimi, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Sempre con riferimento a detti soggetti, l'art. 4 del GDPR [281] contiene una specifica definizione laddove si riferisce a "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*", espressione che inevitabilmente si riferisce a dipendenti o collaboratori: pertanto, non vi è dubbio che essi appaiano le figure sostanzialmente analoghe di "*Incaricato del trattamento*" ai sensi del vecchio Codice Privacy anche se il regolamento in realtà non conferisce ad esse un inquadramento formale. definizione

In questo contesto si inserisce il secondo comma dell'articolo 2-*quaterdecies* del Codice Privacy che richiama la figura degli autorizzati al trattamento: "*il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*". Si tratta di una previsione che ricalca quella riguardante gli incaricati: peraltro, poiché è la stessa la relazione illustrativa, come abbiamo già visto, a

280 Cfr. *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali* con cui il Garante per la protezione dei dati personali ha inteso offrire un panorama delle principali problematiche che imprese e soggetti pubblici devono tenere presenti nell'applicazione del Regolamento (la Guida è consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali).

281 L'art. 4, n. 10, GDPR rubricato "*Definizioni" inquadra nella definizione di "terzo", "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*".

informare del recupero della figura degli incaricati, è ragionevole accostare gli *autorizzati* agli *incaricati*.

Quanto alla nomina dell'incaricato o degli incaricati, le norme lasciano al titolare e al responsabile l'individuazione delle modalità più opportune per autorizzare il trattamento: quindi, si ritiene che, in virtù del principio di *accountability*, è opportuno optare per una modalità che consenta di dimostrare l'avvenuta autorizzazione, dal momento che bisogna lasciare traccia di avere dato istruzioni. Quindi, la designazione, che può avvenire anche con unico atto per più incaricati, deve avvenire con forma scritta, tramite atto nel quale sono indicati i nominativi e i compiti, compreso gli obblighi inerenti le misure di sicurezza. L'incaricato deve, ovviamente, attenersi strettamente alle istruzioni ricevute. La nomina non necessita di firma degli incaricati per accettazione, anche se è utile una presa visione quale prova della conoscenza dell'incarico.

Né il GDPR né il Codice Privacy individuano il contenuto sostanziale delle istruzioni che dovranno necessariamente essere formulate tenendo conto di alcuni parametri di riferimento inerenti le finalità perseguite, la tipologia di dati trattati, le operazioni di trattamento da eseguire, il rischio del trattamento, le funzioni e il ruolo ricoperto dal destinatario dei dati. Una volta individuato l'ambito del trattamento a seconda del ruolo svolto, secondo la dottrina, "*le istruzioni devono garantire una adeguata gestione del rischio che, naturalmente, è diverso a seconda delle mansioni svolte; in ogni caso, dovrebbero essere oggetto di un riesame e un aggiornamento periodico, proprio per fronteggiare adeguatamente il rischio medesimo che può variare in relazione all'evoluzione tecnologica ovvero a mutamenti aziendali che implichino un rimodellamento del trattamento su nuove tipologie di dati di operazioni o di rischi*" [282].

Va, infine, osservato che la mancata osservanza dell'obbligo di fornire istruzioni assume rilevanza sotto il profilo sanzionatorio: l'art. 29 del GDPR [283] è ricompreso tra quelle disposizioni per la cui violazione è comminata la sanzione amministrativa pecuniaria fino a € 10.000.000, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83,(4, lett. a) del GDPR). Del pari, "*il titolare del trattamento è parimenti esposto al risarcimento del danno cagionato all'interessato del trattamento che violi il [Regolamento], così come il responsabile del trattamento, qualora quest'ultimo, però, abbia agito proprio "in modo difforme o contrario rispetto alle legittime istruzioni del titolare" medesimo (art. 82(2))*" [284].

282 Cfr. L. Ferola, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e Normativa privacy - Commentario*, Milano, 2018, p. 277, che aggiunge "*L'applicazione in concreto dell'art. 29, secondo i criteri sopra invocati, si armonizza con il modello dinamico di sicurezza che impone al titolare e al responsabile del trattamento di adottare "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" (art. 32): adeguatezza che va declinata in termini di continua verifica e ammodernamento delle misure organizzative che, se aggiornate, devono necessariamente riflettersi sulle istruzioni da fornire a chi tratta materialmente i dati sotto l'autorità del titolare o del responsabile*".

283 Parimenti, anche l'art. 32 del GDPR, che al suo paragrafo 4 riproduce letteralmente l'art. 29 del GDPR, rientra tra le disposizioni enunciate all'art. 83(4), lett. a), del GDPR la cui violazione viene punita con una sanzione amministrativa pecuniaria fino a € 10.000.000, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

284 Cfr. L. Ferola, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e Normativa privacy - Commentario*, Milano, 2018, p. 279.

CAPITOLO 3 di Pietro Boccaccini, Giacomo Gori e Andrea Mantovani

Note pratiche sul trattamento dei dati personali

Note pratiche sul trattamento dei dati personali effettuato per finalità di marketing e di profilazione

SOMMARIO: 1. Ambito di applicazione del GDPR e note pratiche relative al trattamento di dati personali effettuato per finalità di profilazione – 2. La base giuridica per il trattamento dei dati personali nel contesto delle attività di marketing e profilazione (fra consenso e legittimo interesse) – 3. Il ruolo delle terze parti

1. Ambito di applicazione del GDPR e note pratiche relative al trattamento di dati personali effettuato per finalità di profilazione

1.1. Ambito di applicazione del GDPR

Il Regolamento (UE) 2016/679 (il cosiddetto *General Data Protection Regulation*, "**GDPR**"), applicabile dal 25 maggio 2018, ha introdotto significative novità in tutti gli Stati membri dell'UE in materia di trattamento e di protezione dei dati personali, anche in relazione al trattamento di dati per finalità di *marketing* e di profilazione.

Con l'entrata in vigore del GDPR, nonostante questo sia direttamente applicabile in tutti gli Stati membri dell'UE, è sorta l'esigenza di adeguare tutti gli ordinamenti nazionali. In Italia, è stato a tal fine approvato il D. Lgs. 101 del 2018 che prevede numerose modifiche al D. Lgs. 196 del 2003 (il cosiddetto "Codice Privacy") affinché questo risulti in linea con il nuovo quadro normativo europeo. Il nuovo articolo 1 del Codice Privacy (che prima prevedeva il diritto di tutti alla protezione dei dati personali) prevede ora che il trattamento dei dati personali debba avvenire secondo le norme del GDPR e del Codice Privacy stesso, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

L'ambito di applicazione territoriale del GDPR è assai vasto. Il regolamento si applica, innanzitutto, al trattamento dei dati personali effettuato nel contesto delle attività di uno stabilimento da parte di un titolare del trattamento (o di un responsabile) nell'UE, indipendentemente dal fatto che il trattamento sia effettuato materialmente nell'UE. Per stabilimento si intende non necessariamente

la sede legale, ma una qualsiasi stabile organizzazione che svolga attività effettiva e reale (sono stati considerati stabilimento una controllata o un rappresentante, ad esempio). Non è invece considerato stabilimento, fra l'altro, un computer o un server *tout court*, senza la presenza di un'organizzazione umana.

Inoltre, il GDPR si applica anche al trattamento dei dati personali di interessati che sono nell'UE (non necessariamente essendo residenti in uno Stato membro), effettuato da un titolare del trattamento (o da un responsabile) che non è stabilito nell'UE, quando le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi a tali interessati nell'UE; o
- il monitoraggio del loro comportamento, ove questo abbia luogo nell'UE.

Sotto il profilo pratico, per determinare se vi sia la direzione di un'offerta o di servizi verso un soggetto che si trova nell'UE, occorre stabilire quale sia concretamente l'intenzione del titolare (o del responsabile). In tal senso, costituiscono indici rilevanti, tra altri, l'uso di una lingua dell'UE per consentire all'utente di ordinare beni o servizi o di usare una valuta avente corso legale nell'UE.

Per valutare se il monitoraggio del comportamento degli interessati abbia luogo nell'UE, rappresenta un indice significativo il tracciamento degli interessati su Internet, incluso anche il ricorso a tecniche di profilazione.

Alla luce di quanto sopra, il GDPR troverà applicazione in caso un operatore commerciale effettui attività di trattamento di dati personali:

- per finalità di *marketing*: (i) ove tale operatore sia stabilito in uno (o più) Stati membri dell'UE, ovvero (ii) nel caso in cui tale soggetto non sia stabilito nell'UE ma effettui attività di *marketing* connesse alla fornitura di beni o servizi a interessati che si trovano nell'UE;
- per finalità di profilazione: (i) ove l'operatore che tratti i dati per tali finalità sia stabilito in uno (o più) Stati membri dell'UE, ovvero (ii) nel caso in cui tale soggetto non sia stabilito nell'UE ma profili interessati che si trovano nell'UE.

1.2. Note pratiche relative al trattamento effettuato per finalità di profilazione

Per "profilazione" si intende quella forma di trattamento automatizzato dei dati personali che valuta aspetti personali di una persona fisica al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici sull'interessato stesso.

La profilazione è quindi costituita da tre elementi:

- deve essere una forma di trattamento automatizzato;
- deve essere effettuata su dati personali; e
- il suo obiettivo deve essere quello di valutare aspetti personali relativi a una persona fisica.

In questo paragrafo, si intende fare una rapida riflessione su alcuni diritti e principi da rispettare e su alcuni accorgimenti da seguire ove vengano adottati processi decisionali automatizzati volti alla profilazione degli interessati, sempre più utilizzati in molti settori, tra cui anche quello bancario, finanziario, sanitario, assicurativo, pubblicitario.

Il GDPR prevede, innanzitutto, che il titolare del trattamento (*i.e.* colui che determina le finalità e i mezzi del trattamento) debba informare l'interessato dell'esistenza di un processo decisionale automatizzato. Nel caso in cui la decisione assunta dal titolare sia basata unicamente su un trattamento automatizzato (*i.e.* senza alcun coinvolgimento umano nella decisione) che produca effetti giuridici sull'interessato (*e.g.* il rifiuto automatico di una richiesta di credito *online*), occorre anche fornire informazioni significative:

- sulla logica utilizzata per tale trattamento (che non deve essere necessariamente una spiegazione complessa degli algoritmi utilizzati né tantomeno la divulgazione dell'algoritmo completo); e
- sulle conseguenze previste per l'interessato (fornendo eventualmente anche esempi reali e concreti del tipo di possibili effetti).

Per quanto riguarda la strutturazione dell'informativa, considerato che il processo di profilazione è quasi sempre invisibile all'interessato, ad un trattamento che implica il ricorso a tecnologie sofisticate deve corrispondere l'utilizzo di strumenti informativi per l'interessato che siano altrettanto elaborati (ad esempio, informative stratificate su più livelli, informative dinamiche, ecc.). Le prassi operative applicate dal titolare dovrebbero risultare in maniera chiara ed esaustiva.

In generale, l'informativa – da rendere al momento della raccolta dei dati oppure entro un mese, se i dati non vengono ottenuti dall'interessato – deve essere incentrata sull'utente e deve essere fornita in forma concisa, trasparente, intellegibile, facilmente accessibile, adottando un linguaggio semplice e chiaro.

Talvolta il trattamento dei dati viene effettuato dagli operatori per finalità ulteriori rispetto a quelle inizialmente previste e in relazione alle quali sia stata fornita l'informativa. Si pensi, ad esempio, ad una applicazione per *smartphone* che individua ristoranti sulla base della localizzazione dell'utente: l'interessato si aspetterebbe che i suoi dati personali vengano trattati per aiutarlo a trovare un ristorante nella zona di suo interesse, non per ricevere pubblicità su servizi di *food delivery* perché la applicazione ha rilevato che l'utente, sovente, rincasa tardi. Di tale ulteriore finalità di trattamento, occorrerebbe certamente informare l'interessato. Inoltre, sarebbe necessario ottenere il consenso dell'interes-

sato rispetto a tale ulteriore finalità di trattamento, a meno che questo non sia necessario in considerazione, tra l'altro, del particolare rapporto tra il titolare e l'interessato, della natura dei dati, delle garanzie adottate dal titolare, ecc.

In relazione a tutti i trattamenti di dati personali:

- effettuati per finalità di profilazione (ove il presupposto di legittimità sia l'esecuzione di un compito di interesse pubblico o il perseguimento di un legittimo interesse del titolare); o
- effettuati per finalità di *marketing* diretto (compresa la profilazione, nella misura in cui sia connessa a tale *marketing* diretto);

l'interessato ha il diritto di opporsi in qualsiasi momento e senza che da ciò derivi alcun onere. Il titolare deve informare espressamente l'interessato di tale diritto, separatamente da ogni altra informazione.

Se il trattamento è basato sul legittimo interesse del titolare e l'interessato si oppone al trattamento per finalità di profilazione, il titolare deve interrompere l'attività che implica la profilazione in attesa della verifica sull'eventuale prevalenza di motivi legittimi del titolare rispetto a quelli dell'interessato (che potrebbero ricorrere, ad esempio, ove la profilazione abbia un'utilità sociale e non solo privata).

Nel caso, invece, in cui l'interessato si opponga al trattamento dei suoi dati per finalità di *marketing* diretto, non occorrerebbe fare alcun bilanciamento di interessi.

Inoltre, il titolare del trattamento che intenda fare ricorso a tecniche di profilazione, in osservanza del principio della minimizzazione dei dati, dovrà prestare attenzione a non raccogliere più dati di quelli che sono necessari per la specifica finalità e dovrà anche verificare che l'analisi dei dati (che devono comunque sempre essere esatti e aggiornati) non contenga distorsioni e che l'insieme dei dati ottenuti dalla profilazione dell'interessato sia rappresentativo della reale situazione soggettiva.

L'interessato ha anche il diritto di ottenere informazioni dettagliate sui dati personali utilizzati per la profilazione e il titolare deve rendere disponibili i dati utilizzati come *input* per la creazione del profilo e consentire l'accesso anche ai dettagli relativi ai segmenti nei quali l'interessato è stato inserito (*e.g.* libero professionista con reddito compreso tra X e Y e propensione di spesa mensile per l'acquisto di prodotti *online* pari a Z). Tale diritto dell'interessato non deve comunque ledere il diritto opposto del titolare alla tutela dei propri segreti industriali e dei propri diritti di proprietà intellettuale e industriale, come i diritti d'autore a tutela dei propri software utilizzati anche per trattamenti automatizzati di dati per profilare gli utenti.

I diritti di rettifica e di cancellazione dei dati personali che spettano agli interessati devono applicarsi sia ai dati personali di *input* (che vengono usati per la creazione del profilo) sia ai dati di *output* (il profilo vero e proprio o il segmento di riferimento, ad esempio).

Se la base per il trattamento è il consenso dell'interessato o se il trattamento basato sulla profilazione è necessario per concludere o dare esecuzione a un contratto, il titolare del trattamento deve attuare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati. Tali misure dovrebbero includere quanto meno la possibilità per l'interessato di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione. Qualsiasi riesame dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza necessaria per modificare la decisione. Le garanzie adeguate dovrebbero includere anche la specifica informazione all'interessato e il diritto di ottenere una spiegazione della decisione conseguita dopo la valutazione basata sulla profilazione e di contestare la decisione.

Il GDPR (considerando 71) prevede che le decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, non dovrebbero riguardare minori. Il Gruppo di Lavoro Articolo 29 (l'organo consultivo indipendente dell'UE per la protezione dei dati personali, ora sostituito dal Comitato europeo per la protezione dei dati) non ritiene tuttavia che ciò rappresenti un divieto assoluto di questo tipo di trattamento in relazione ai minori. Potrebbero esservi infatti alcune circostanze nelle quali è necessario che il titolare del trattamento prenda decisioni basate unicamente sul trattamento automatizzato aventi effetti giuridici in relazione ai minori, ad esempio per tutelarne il benessere. In questi casi devono comunque essere messe in atto garanzie adeguate, in considerazione del fatto che gli interessati sono minori.

È infine opportuno precisare che laddove un titolare intenda effettuare trattamenti di dati personali:

- che prevedano l'uso di nuove tecnologie; e
- che possano presentare rischi elevati per i diritti e le libertà degli interessati (considerati la natura, l'oggetto, il contesto e le finalità del trattamento); e
- che implichino una valutazione sistematica e globale di aspetti personali basata sulla profilazione e sulla quale si fondano decisioni che hanno effetti giuridici sull'interessato;

dovrà necessariamente effettuare una valutazione d'impatto dei trattamenti (la cosiddetta DPIA, *Data Protection Impact Assessment*), predisposta ai sensi dell'articolo 35 del GDPR, prima di procedere al trattamento. Nel caso in cui dalla valutazione d'impatto effettuata risulti che il trattamento presenterebbe un rischio elevato in assenza di misure per attenuare il rischio, sarà necessario consultare l'autorità di controllo prima di procedere al trattamento.

2 La base giuridica per il trattamento dei dati personali nel contesto delle attività di marketing e profilazione (fra consenso e legittimo interesse)

2.1. Il consenso

Il consenso degli interessati è la base giuridica che i titolari del trattamento tradizionalmente impiegano per le attività di *marketing* diretto e di profilazione.

Al punto 11 dell'art. 4 del GDPR, il legislatore europeo precisa che tale consenso deve integrare una manifestazione di volontà dell'interessato (i) libera, (ii) specifica, (iii) informata e (iv) inequivocabile.

Come osservato dal Gruppo di Lavoro Articolo 29 nelle *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679* (adottate il 28 novembre 2017 e successivamente emendate il 10 aprile 2018), si tratta di una nozione "*sostanzialmente simile a quella della direttiva 95/46/CE*". Conseguentemente, i titolari del trattamento che abbiano raccolto il consenso degli interessati prima dell'entrata in vigore del GDPR nel rispetto della disciplina allora in vigore, di norma non sono tenuti a richiederlo nuovamente in conseguenza dell'applicazione del GDPR. In ogni caso, qualunque consenso deve poter essere revocato senza che l'interessato ne subisca un pregiudizio, sebbene ciò non escluda "*la liceità del trattamento"* basato *"sul consenso prima della revoca*" (art. 7, comma 3, del GDPR).

(i) Il consenso non è considerato libero, fra l'altro, se raccolto tramite caselle precompilate (cfr. il considerando 32 del GDPR) o se all'interessato che non lo fornisca venga negata la prestazione di un servizio (cfr. l'art. 7, comma 4, del GDPR). Non sembra agevole armonizzare con tale regola la posizione espressa dalla Suprema Corte nella sentenza n. 17278 del 2 luglio 2018, con la quale è stato ritenuto valido il consenso alla ricezione di comunicazioni promozionali imposto agli utenti come condizione di iscrizione a un servizio di *newsletter*.

(ii) Poiché il consenso dev'essere anche specifico, il titolare del trattamento deve acquisirne uno *ad hoc* per ciascuna distinta finalità perseguita. Quanto all'attività di *marketing*, il Garante per la protezione dei dati personali ha comunque permesso, nell'ottica di semplificazione degli adempimenti a carico dei titolari, la raccolta di un unico consenso che comprenda sia le modalità "tradizionali" di contatto (quali posta cartacea e telefonate con operatore) sia quelle di cui all'art. 130, commi 1 e 2 del Codice Privacy (quali posta elettronica e telefonate senza operatore). Anche la cessione di dati personali a terzi (comprese altre società del gruppo a cui appartenga il titolare), affinché questi svolgano proprie attività di *marketing* e/o di profilazione, richiede un consenso specifico.

(iii) Dato che il consenso dev'essere informato, il Garante per la protezione dei dati personali ha ritenuto che, "*ai fini della legittimità della comunicazione promozionale effettuata, non è lecito, con la medesima, avvisare della possibilità di opporsi a ulteriori invii, né è lecito chiedere, con tale primo messaggio*

promozionale, il consenso al trattamento dati per finalità promozionali" (cfr. le *Linee guida in materia di attività promozionale e contrasto allo spam* - 4 luglio 2013). Ne discende che il titolare del trattamento che abbia necessità di contattare l'interessato per richiederne il consenso dovrà fare ciò utilizzando modalità che non lo presuppongono (ad esempio, mediante telefonata con operatore ad un numero che sia incluso negli elenchi dei contraenti e non iscritto nel registro delle opposizioni).

(iv) Per aversi manifestazione inequivocabile di volontà dell'interessato, può essere sufficiente, in relazione allo specifico contesto, una sua dichiarazione verbale, che può essere registrata per assicurarne la prova. Possono invece risultare insufficienti meccanismi di raccolta del consenso che si basino sul silenzio o sull'inattività dell'interessato e non sono generalmente considerate ammissibili procedure di rinuncia (*opt-out*) che richiedono un intervento dell'interessato per rifiutare il consenso.

2.2. Il legittimo interesse

In alternativa al consenso, il titolare del trattamento può valutare se ricorrere alla base giuridica del legittimo interesse, previo esito positivo del *balancing test* di cui all'art. 6, comma 1, lett. f) del GDPR e salvo il diritto di opposizione dell'interessato ex art. 21, comma 2, del GDPR.

D'altronde, con il GDPR la base giuridica in discorso è divenuta accessibile a discrezione del titolare del trattamento e non più soltanto "*nei casi individuati dal Garante*", come invece prevedeva il vecchio art. 24, comma 1, lett. g) del Codice Privacy. Peraltro, ad avviso di chi scrive, la previgente norma era di dubbia legittimità, giacché essa introduceva un requisito supplementare rispetto a quanto stabilito nella Direttiva 95/46/CE, in contrasto con quanto sancito dalla Corte di Giustizia dell'Unione europea nel caso Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado (cause riunite C-468/10 e C-469/10).

Quanto al *marketing*, il considerando 47 del GDPR precisa che "*può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto*". Peraltro, già prima dell'avvento del GDPR il Gruppo di Lavoro Articolo 29, nel *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/EC* (adottato il 9 aprile 2014), aveva segnalato che "*in alcuni casi*" il legittimo interesse potesse costituire "*un fondamento giuridico adeguato*" per l'attività in questione.

L'area di operatività del legittimo interesse nel contesto del *marketing* diretto è comunque considerevolmente delimitata dai vincoli che, a tutela dei destinatari di comunicazioni commerciali indesiderate, pone la normativa *ePrivacy* (attualmente soggetta a possibili modifiche, pendente l'approvazione di un regolamento europeo in materia). Tali vincoli si trovano negli artt. 129 e 130 del Codice Privacy, a mente dei quali comunicazioni di marketing mediante telefonate senza l'intervento di un operatore o "*mediante posta elettronica, telefax,*

messaggi del tipo Mms […] *o Sms* […] *o di altro tipo*" necessitano del consenso del destinatario, a meno che non si tratti di c.d. *soft spam*.

Soft spam (art. 130, comma 4, del Codice Privacy) si ha quando il titolare del trattamento utilizzi il recapito di posta elettronica fornito dall'interessato al momento della vendita di un prodotto o di un servizio, per comunicazioni volte a promuovere "*servizi analoghi a quelli oggetto della vendita*", sempre che l'interessato sia stato adeguatamente informato in proposito e abbia la possibilità di opporsi al trattamento sia al momento della raccolta del recapito sia in occasione di successive comunicazioni. Inoltre, come ha chiarito il Gruppo di Lavoro Articolo 29 nel *Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'articolo 13 della direttiva 2002/58/CE* (adottato il 27 febbraio 2004), la disciplina del *soft spam* si applica solo se è "*la stessa persona fisica o giuridica che ha raccolto i dati*" a inviare i "*messaggi di posta elettronica a fini di commercializzazione*".

Vi sono comunque casi per i quali la normativa in commento espressamente prevede che il tritolare del trattamento possa prescindere dalla raccolta del consenso preventivo del destinatario di un'attività di *marketing*. In particolare, quando il titolare utilizzi i recapiti contenuti negli "*elenchi cartacei o elettronici a disposizione del pubblico*" di cui all'art. 129 del Codice Privacy per effettuare telefonate con operatore o inviare posta cartacea, purché il destinatario della comunicazione non abbia esercitato il diritto di opposizione (*opt-out*) mediante iscrizione dei propri recapiti nel registro pubblico delle opposizioni (art. 130, comma 3-*bis*, del Codice Privacy).

Le chiamate con operatore e il *marketing* per mezzo della posta cartacea a recapiti che non siano contenuti negli elenchi dei contraenti non rientrano fra le fattispecie per le quali l'art. 130, commi 1 e 2, del Codice Privacy impone esplicitamente il ricorso alla base giuridica del consenso. Pertanto, ad avviso di chi scrive (e sebbene la posizione del Garante per la protezione dei dati personali sul tema sia stata sempre restrittiva), per tali tipologie di contatto può valutarsi la possibilità di ricorrere alla base giuridica del legittimo interesse, ove il titolare accerti, come indicato nel considerando 47 del GDPR, che l'interessato possa "*ragionevolmente attendersi*" il trattamento dei dati personali in questione.

La selezione della base giuridica per l'attività di profilazione non è soggetta ai limiti di cui alle disposizioni *ePrivacy* sopra commentate.

In alcuni casi, come quando la profilazione abbia ad oggetto 'categorie particolari di dati personali' di cui all'art. 9 del GDPR, il trattamento dovrà comunque basarsi sul preventivo consenso dell'interessato. In altri casi, il titolare del trattamento potrà ricorrere alla base giuridica del legittimo interesse, previo *balancing test*. Come chiarito dal Gruppo di Lavoro Articolo 29 nelle *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (adottate il 3 ottobre 2017 e successivamente emendate il 6 febbraio 2018), questo test deve tener conto in particolare del "*livello di dettaglio del profilo", della "completezza del profilo", dell'"impatto della profilazione (gli effetti sull'interessato)*" e delle "*garanzie destinate ad assicurare la correttezza, la non discriminazione e l'esattezza nel processo di profilazione*". In ogni caso,

come ha precisato il Gruppo di Lavoro Articolo 29 nelle *Linee guida* testé citate, "*sarebbe difficile per il titolare del trattamento giustificare il ricorso al legittimo interesse come base legittima per pratiche intrusive di profilazione e tracciamento per finalità di marketing o pubblicità, ad esempio quelle che comportano il tracciamento di persone fisiche su più siti web, ubicazioni, dispositivi, servizi o l'intermediazione di dati*".

Pare utile segnalare anche che, nel *Provvedimento del 22 febbraio 2018*, il Garante per la protezione dei dati personali, fra l'altro, ha ritenuto che, nei casi di trattamento fondato sul legittimo interesse condotto tramite l'uso di nuove tecnologie o strumenti automatizzati, debba essere "*effettuata, prima di procedere al trattamento, la valutazione di impatto di cui all'art. 35 del Regolamento*", considerato che tale trattamento "*può di per sé presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati*", ferma restando la necessità di consultare preventivamente il Garante ai sensi dell'art. 36 del GDPR, qualora, all'esito della valutazione d'impatto, il rischio residuo rimanga elevato.

3 Il ruolo delle terze parti

Oltre al titolare, diversi sono i soggetti che possono essere legittimati, a diverso titolo, a trattare i dati degli interessati. Tra questi rientrano i responsabili esterni, i contitolari e i terzi diversi dai responsabili esterni.

3.1. Il responsabile esterno

Il GDPR all'art. 4 definisce il responsabile del trattamento come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Nella vigenza della precedente disciplina – pur in essenza di esplicito riconoscimento né nella direttiva 95/46/CE né nel Codice della Privacy, la dottrina e la prassi operativa del Garante avevano riconosciuto la possibilità di nominare un responsabile interno ed uno esterno.

La definizione di responsabile del trattamento contenuta nel GDPR, viceversa, non sembra compatibile con la figura del responsabile interno: ciò si desume, ad esempio dal fatto che in base all'art. 28, paragrafo 3, il contenuto minimo del contratto (o di altro atto giuridico vincolante) che deve intercorrere tra titolare e responsabile del trattamento lascia presupporre che il responsabile del trattamento sia un soggetto esterno alla struttura organizzativa del titolare.

Altro elemento che depone a favore della predetta interpretazione si rinviene ad esempio nell'obbligo di tenuta del registro delle attività di trattamento, incompatibile con soggetti responsabili interni all'organizzazione del titolare.

In base all'art. 28 del GDPR, la scelta sul responsabile deve cadere su soggetti "*che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate*" tali da soddisfare i requisiti del regolamento e garantiscano la tutela dei diritti dell'interessato.

Come accennato, il rapporto tra titolare e responsabile deve essere disciplinato in modo dettagliato e vincolante e prevedere quanto meno che il responsabile:

- tratti i dati sulla base di documentate istruzioni impartite dal titolare;
- garantisca che le persone autorizzate al trattamento dei dati personali si impegnino alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti le misure di sicurezza previste dall'articolo 32 del GDPR;
- nel caso in cui ricorra ad un sub-responsabile, provveda con un'autorizzazione scritta (specifica o generale) del titolare del trattamento, fermo restando che, in caso di autorizzazione generale, il titolare deve essere informato di eventuali modifiche affinché possa, se del caso, opporsi; inoltre gli stessi obblighi gravanti sul responsabile – in particolare per quanto concerne l'adeguatezza delle misure tecniche ed organizzative – dovranno essere previsti per il sub-responsabile e, nel caso in cui questi ometta di adempiere ai propri obblighi, il responsabile conserva, nei confronti del titolare, l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile;
- assista il titolare del trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su indicazione del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi assunti e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Oltre a quanto sopra, il responsabile ha l'obbligo di conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità.

3.2. Gli altri terzi

Nel caso in cui, una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile trattino dati degli interes-

sati, si parla genericamente di terzi. Detti terzi, inoltre, possono anche rivestire la qualifica di destinatari nel caso in cui i dati personali gli siano stati comunicati.

I terzi, a differenza del responsabile, non trattano i dati per conto del titolare ma per conto proprio. La differenza non è di poco conto poiché il terzo che tratta i dati, ancorché quale soggetto destinatario, è un titolare autonomo ed ha l'obbligo di adempiere a quanto previsto dall'art. 14 del GDPR per quanto concerne l'informativa da rendere ai soggetti interessati.

Tale informativa, in particolare, dovrà essere fornita entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati.

Inoltre, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, l'informativa dovrà essere resa al più tardi al momento della prima comunicazione all'interessato oppure nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

3.3. I contitolari

Mentre il responsabile tratta i dati sulla base delle finalità e con le modalità decise dal titolare, nel caso in cui due o più titolari del trattamento determinino congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

L'art. 26 del GDPR prevede che i contitolari determinino in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

Va da sé che il suddetto accordo dovrà essere redatto con estrema attenzione in modo da disciplinare adeguatamente i rapporti tra i contitolari e con gli interessati ai quali, su richiesta degli stessi, il contenuto dell'accordo andrà comunicato.

Peraltro, indipendentemente dal contenuto dell'accordo, gli interessati potranno esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento. A tal fine, il suddetto accordo dovrà prevedere un punto di contatto per gli interessati in modo che gli stessi possano individuare il titolare a cui far riferimento tra i vari contitolari.

Quanto sopra, tuttavia, è spesso soggetto ad ulteriore regolamentazione tra le parti. Ad esempio, è possibile prevedere che i contitolari siano responsabili in solido per l'intero ammontare del danno nei confronti dell'interessato, ma sia consentita l'azione di regresso di ciascun contitolare nei confronti dell'altro effettivamente responsabile del danno.

CAPITOLO 4 di Angela Berinati, Simona Custer e Marta Margiocco

La protezione dei dati personali nel rapporto di lavoro

SOMMARIO: 1. La protezione dei dati personali nel rapporto di lavoro – 1.1 Il trattamento dei dati personali del dipendente svolto dal datore di lavoro – 1.2 Il trattamento dei dati di soggetti terzi svolto dal lavoratore nell'adempimento delle proprie mansioni lavorative – 2. Privacy e profili giuslavoristici: i controlli datoriali – 2.1. Videosorveglianza e geolocalizzazione: dagli adempimenti privacy agli obblighi giuslavoristici – 2.1.1 La normativa privacy ed i relativi adempimenti – 2.1.1.1 Videosorveglianza – 2.1.1.2 Geolocalizzazione – 2.1.2 Gli obblighi giuslavoristici – 3. Gli strumenti informatici aziendali: l'importanza delle policy – 3.1 Il contenuto del disciplinare

1. La protezione dei dati personali nel rapporto di lavoro

Il Regolamento (UE) 2016/679 [285] non contiene una disciplina di dettaglio relativa al trattamento dei dati personali nell'ambito del rapporto di lavoro ma rimanda agli Stati Membri l'adozione di norme specifiche per assicurare la protezione dei diritti e delle libertà dei lavoratori, evidenziando la necessità di individuare misure appropriate a tutela dei lavoratori con riferimento alla trasparenza del trattamento, al trasferimento di dati personali nell'ambito di un gruppo imprenditoriale e ai sistemi di monitoraggio sul posto di lavoro [286].

In Italia tali norme specifiche non sono state per il momento adottate. Le previsioni in materia di trattamento di dati personali nell'ambito del rapporto di lavoro contenute nel D. Lgs. n. 196/2003 [287], come modificato dal D. Lgs. n. 101/2018 [288], cui pure è dedicato il titolo VIII della Parte II, sono scarne e poco aggiungono alla disciplina esistente.

285 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito GDPR.

286 Cfr. considerando (155) e articolo 88 GDPR.

287 Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, di seguito Codice della Privacy.

288 Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

È tuttavia prevista all'articolo 111 del Codice della Privacy l'adozione da parte del Garante per la protezione di dati personali di regole deontologiche per i soggetti pubblici e privati con riferimento ai trattamenti svolti nell'ambito dei contratti di lavoro, proprio in attuazione di quanto previsto dal GDPR.

In assenza di una disciplina specifica in materia è quindi necessario fare riferimento alla disciplina generale, oltre che alle interpretazioni date dal Gruppo di lavoro articolo 29 [289] e dal Garante per la protezione dai dati personali.

1.1. Il trattamento dei dati personali del dipendente svolto dal datore di lavoro

I dati personali dei dipendenti trattati dal datore di lavoro in qualità di titolare del trattamento sono normalmente raccolti presso l'interessato e pertanto l'informativa, avente il contenuto di cui all'articolo 13 GDPR, deve essere data al momento della raccolta dei dati.

L'attenzione sarà qui di seguito rivolta solo ad alcuni degli elementi dell'informativa, ovvero la finalità, la base giuridica, le categorie di destinatari e l'esistenza di un processo decisionale automatizzato.

La finalità del trattamento dei dati personali dei dipendenti svolto dal datore di lavoro è in primo luogo la gestione del rapporto di lavoro, che comprende aspetti diversi quali assunzione, esecuzione del contratto di lavoro (adempimenti di gestione, pianificazione e organizzazione del lavoro), parità e diversità e salute e sicurezza sul posto di lavoro, esercizio dei diritti e dei vantaggi connessi al lavoro, cessazione del rapporto di lavoro [290]. Il datore di lavoro può tuttavia trattare i dati personali dei dipendenti per altre finalità, quali la protezione della proprietà propria o del cliente e la profilazione del rendimento professionale dei dipendenti.

La base giuridica del trattamento è nella maggior parte dei casi l'esecuzione del contratto di lavoro di cui è parte l'interessato (articolo 6, paragrafo 1, lettera b), GDPR) o l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (articolo 6, paragrafo 1, lettera c), GDPR). In alcuni casi la base giuridica del trattamento può essere il legittimo interesse del datore di lavoro, qualora il trattamento sia strettamente necessario per conseguire finalità legittime e sia conforme ai principi di proporzionalità e sussidiarietà.

È invece improbabile che il trattamento dei dati personali dei dipendenti svolto dal datore di lavoro possa basarsi sul consenso. Il rapporto tra datore di lavoro e dipendente è caratterizzato da uno squilibrio di potere tra le due parti, che nella maggior parte dei casi non consentirebbe al lavoratore di negare il proprio consenso [291]; il lavoratore potrebbe cioè essere portato a esprime il

nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

289 Gruppo di lavoro europeo indipendente che ha trattato questioni relative alla protezione dei dati personali fino al 25 maggio 2018, oggi sostituito dal Comitato europeo per la protezione dei dati.

290 Cfr. articolo 88, paragrafo 1, GDPR.

291 Cfr. Garante per la protezione dei dati personali, provvedimento del 13 dicembre 2018, n. 500, doc.

proprio consenso non in modo libero, ma in ragione del timore di subire ripercussioni a fronte del proprio rifiuto e pertanto tale consenso non sarebbe valido perché non prestato liberamente [292].

Il trattamento di categorie particolari di dati personali [293] è consentito qualora sia necessario ad assolvere ad obblighi e a esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (articolo 6, paragrafo 2, lettera b), GDPR) [294] . Quanto invece al trattamento dei dati personali relativi a condanne penali o reati, lo stesso è consentito nello stesso caso ma solo se autorizzato da una norma di legge e nei limiti stabiliti da leggi, regolamenti e contratti collettivi (articolo 10 GDPR; articolo 2-octies, comma 3, lettera a), Codice della Privacy).

In attuazione di quanto previsto dall'articolo 21 del D. Lgs. n. 101/2018, il Garante per la protezione dei dati personali, con provvedimento del 13 dicembre 2018 [295], ha individuato le prescrizioni contenute nelle autorizzazioni generali già adottate, e tra queste l'autorizzazione generale 1/2016 al trattamento dei dati sensibili nel rapporto di lavoro, che risultano compatibili con il GDPR e con il Codice della Privacy come modificato dal D. Lgs. n. 101/2018. Tale provvedimento è stato posto in consultazione pubblica e ad oggi non è ancora stato adottato il provvedimento finale. Si segnala tuttavia che il contenuto delle "Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016)", allegate a tale provvedimento, riprende sostanzialmente quello dell'autorizzazione adottata nel 2016; tra le nuove previsioni, quella che precisa che qualora per l'organizzazione del lavoro il datore di lavoro metta a disposizione di soggetti diversi dall'interessato (ad esempio i colleghi dello stesso) dati relativi a presenze o assenze dal servizio, non devono essere esplicitate le ragioni dell'assenza dalle quali sia possibile evincere categorie particolari di dati personali.

L'informativa deve poi indicare gli eventuali destinatari o categorie di destinatari dei dati personali. Nell'ambito del rapporto di lavoro tipico esempio di responsabile del trattamento (e quindi di destinatario dei dati personali) è il consulente del lavoro [296], cui il datore di lavoro, in qualità di titolare del trat-

web n. 9068983; Garante per la protezione dai dati personali, provvedimento del 19 luglio 2018, n. 427, doc. web n. 9039945. Cfr. anche Gruppo di lavoro articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679* adottate il 28 novembre 2017, come modificate e adottate da ultimo il 10 aprile 2018 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051); Gruppo di lavoro articolo 29, *Parere 2/2017 sul trattamento dei dati personali nel luogo di lavoro*, adottate l'8 giugno 2017 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169).

292 Secondo quanto previsto dall'articolo 4, paragrafo 1, numero 11) GDPR, il consenso deve essere una "*manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato*". Cfr. considerando (42) e (43) GDPR.

293 Secondo la definizione data dall'articolo 9, paragrafo 1, GDPR, si tratta dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

294 Con specifico riferimento al trattamento di dati personali relativi alla salute, in attuazione di quanto previsto dall'articolo 2-septies del Codice della Privacy, il Garante adotterà ogni due anni un provvedimento avente ad oggetto le misure di garanzia necessarie al trattamento.

295 Cfr. Garante per la protezione dei dati personali, provvedimento del 13 dicembre 2018, n. 497, doc. web n. 9068972.

296 Cfr. Risposta a un quesito relativo al ruolo del consulente del lavoro dopo la piena applicazione del

tamento, affida lo svolgimento di attività relative alla gestione del rapporto di lavoro e agli adempimenti in materia di lavoro, previdenza e assistenza sociale.

Il consulente del lavoro tratta infatti dati dei dipendenti raccolti dal datore di lavoro nel perseguimento di finalità legittime, per conto dello stesso, nell'ambito delle istruzioni e delle direttive ricevute.

Il datore di lavoro deve inoltre informare il dipendente dell'esistenza di un processo decisionale automatizzato, compresa la profilazione ovvero il trattamento automatizzato di dati personali per valutare aspetti riguardanti il rendimento professionale [297]. Qualora quindi il datore di lavoro intenda procedere alla profilazione dei dati del dipendente deve fornire informazioni sulla logica utilizzata e sull'importanza e le conseguenze di tale trattamento.

Nel caso in cui il datore di lavoro tratti anche dati personali dei familiari o conviventi dei propri dipendenti, occorrerà valutare se sia necessario dare una informativa specifica ai familiari o se invece tale trattamento, essendo relativo a dati personali non raccolti presso l'interessato, possa rientrare nella previsione di cui all'articolo 14, paragrafo 5, lettera c) GDPR, ai sensi della quale il titolare del trattamento non è tenuto a dare l'informativa se l'ottenimento o la comunicazione dei dati personali è espressamente previsto dal diritto dell'Unione o dello Stato Membro cui è soggetto il titolare del trattamento, che preveda misure appropriate di tutela. Si segnala che le "Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016)" citate sopra si applicano espressamente ai dati personali di familiari e conviventi dei dipendenti per il rilascio di agevolazioni e permessi.

Merita infine un breve approfondimento il trattamento dei dati dei candidati svolto dal potenziale datore di lavoro.

Qualora i dati personali dei candidati siano raccolti direttamente presso l'interessato (ad esempio attraverso la sezione "lavora con noi" del sito internet) l'informativa deve essere data al momento della raccolta dai dati mentre, come precisato dall'articolo 111-bis del D. Lgs. n. 196/2003, in caso di ricezione di *curricula* spontaneamente trasmessi dagli interessati l'informativa deve essere data al momento del primo contatto utile successivo all'invio del *curriculum* [298].

Secondo il Gruppo di lavoro articolo 29 [299], il trattamento dei dati personali di candidati presenti sui profili degli stessi sui social media, anche se

Regolamento (UE) 679/2016 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970). Il Garante per la protezione dei dati personali, riscontrando un quesito ricevuto dal Consiglio nazionale dei consulenti del lavoro, ha confermato che il consulente del lavoro, nel trattamento dei dati personali dei dipendenti dei propri clienti, assume il ruolo di responsabile del trattamento anche alla luce del GDPR, in linea con la precedente disciplina.

297 Cfr. articolo 4, paragrafo 1, numero 4).

298 Si ricorda che ai sensi dell'articolo 13, comma 5 bis, del D. Lgs. n. 196/2003, prima delle modifiche introdotte dal D. Lgs. n. 101/2018, in caso di curricula spontaneamente trasmessi dagli interessati il titolare del trattamento era tenuto a fornire all'interessato al momento del primo contatto successivo all'invio del curriculum, solo una informativa breve contenente almeno le finalità e modalità del trattamento, i destinatari dei dati e l'ambito di diffusione dei dati medesimi e gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e di almeno un responsabile del trattamento.

299 Cfr. Gruppo di lavoro articolo 29, *Parere 2/2017 sul trattamento dei dati personali nel luogo di lavoro, adottate*

pubblicamente accessibili, è consentito solo se tale trattamento sia necessario e pertinente per l'esecuzione dello specifico lavoro e solo qualora sia stata data adeguata informativa in merito. I dati personali raccolti nell'ambito del processo di selezione devono inoltre essere cancellati al termine dello stesso, mentre per poterli conservare per future opportunità lavorative, il potenziale datore di lavoro deve informarne l'interessato in modo specifico [300].

1.2. Il trattamento dei dati di soggetti terzi svolto dal lavoratore nell'adempimento delle proprie mansioni lavorative

Ci si sofferma ora brevemente sul trattamento svolto dai dipendenti, nell'adempimento delle proprie mansioni lavorative, dei dati personali di soggetti terzi. È quindi necessario un cambio di prospettiva perché in questo caso l'interessato non è il dipendente ma un soggetto terzo, i cui dati personali sono trattati dal dipendente nell'adempimento delle mansioni lavorative a lui assegnate dal datore di lavoro, che è il titolare o il responsabile di tale trattamento.

Come previsto dall'articolo 4, paragrafo 1, numero 10) GDPR, i dati personali possono infatti essere legittimamente trattati, oltre che dal titolare e dal responsabile, da "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" [301], che devono essere specificamente istruite in tal senso dal titolare del trattamento [302].

La norma non prevede quale forma debbano avere tali autorizzazioni. Il Codice della Privacy precisa al riguardo che spetta al titolare o al responsabile del trattamento, alla luce del principio di responsabilizzazione che ispira il GDPR, individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta [303].

Si ritiene opportuno che le autorizzazioni al trattamento siano documentate in forma scritta, oltre che oggetto di periodici momenti di formazione, e indichino, nel modo più preciso possibile, l'ambito del trattamento consentito (categorie di dati personali e di soggetti interessati), le operazioni di trattamento consentite e le misure di sicurezza da applicare al trattamento.

l'8 giugno 2017 cit.

300 Cfr. Gruppo di lavoro articolo 29, *Parere 2/2017 sul trattamento dei dati personali nel luogo di lavoro, adottate l'8 giugno 2017* cit; Consiglio d'Europa, raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, adottata dal Comitato dei Ministri il 01 aprile 2015 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4224268).

301 Quella del soggetto autorizzato al trattamento è una figura molto vicina a quella dell'incaricato al trattamento di cui all'articolo 30 del Codice della Privacy prima delle modifiche introdotte dal D. Lgs. n. 101/2018 come indicato dallo stesso Garante per la protezione dei dati personali qui https://www.garanteprivacy.it/Regolamentoue/titolare-responsabile-incaricato-del-trattamento.

302 Cfr. articolo 29 e 32, paragrafo 4, GDPR.

303 Cfr. articolo 2-*quaterdecies* Codice della Privacy.

2. Privacy e profili giuslavoristici: i controlli datoriali

2.1. Videosorveglianza e geolocalizzazione: dagli adempimenti privacy agli obblighi giuslavoristici

L'installazione di impianti di videosorveglianza e di sistemi di geolocalizzazione costituisce da sempre una tematica molto delicata, cui occorre guardare con particolare attenzione.

Detti strumenti, infatti, se da un lato comportano il trattamento di dati personali, con la conseguente necessità di tutelare gli interessati sotto il profilo privacy, dall'altro possono costituire una forma di controllo dei dipendenti, con tutte le conseguenze che ne derivano sotto il profilo giuslavoristico.

Il datore di lavoro si trova, quindi, a dover ottemperare non soltanto a tutti gli adempimenti previsti dalla normativa in materia di protezione dei dati personali (*in primis*, il Regolamento UE n. 2016/679 [304], di seguito indicato come "Regolamento" o "GDPR") ma anche agli obblighi sanciti dallo Statuto dei Lavoratori (Legge n. 300/1970 [305]).

Si tratta, per questo, di temi complessi, che impongono adeguamenti normativi sotto svariati profili.

Di seguito, vengono riassunte le principali norme di riferimento, con lo scopo di fornire una panoramica sui relativi adempimenti da attuare.

2.1.1 La normativa privacy ed i relativi adempimenti

L'utilizzo di sistemi di videosorveglianza e di geolocalizzazione comporta il trattamento di tutta una serie di dati (di lavoratori e non) che, in quanto persone fisiche, sono tutelati dalla normativa privacy.

La società che si avvale di dette strumentazioni, in quanto titolare del trattamento, deve quindi adeguarsi alle prescrizioni in materia.

La normativa, tuttavia, è piuttosto articolata.

Infatti, oltre al Regolamento - che disciplina i principi generali e gli adempimenti che il titolare è tenuto a rispettare e porre in essere ai fini di un lecito trattamento dei dati - ci sono i provvedimenti resi nel tempo dal Garante [306]

304 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

305 Legge 20 maggio 1970, n. 300 (in Gazz. Uff., 27 maggio, n. 131), *Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento* (Statuto dei Lavoratori).

306 Garante per la protezione dei dati personali, provvedimento in materia di videosorveglianza del 08.04.2010, doc. web n. 1712680; Garante per la protezione dei dati personali, provvedimento in materia di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro del 04.10.2011, n. 370, doc. web. n. 1850581.

che contengono, invece, prescrizioni più specifiche e mirate in materia; provvedimenti, questi, che devono essere letti ed interpretati alla luce dei principi esposti nel Regolamento.

Al fine di rendere un quadro di insieme quanto più concreto possibile, di seguito vengono indicati i principali adeguamenti richiesti dalla normativa.

2.1.1.1 Videosorveglianza

a. L'informativa

Gli interessati (lavoratori della società o comunque soggetti che accedono alle aree interessate) devono, anzitutto, essere informati di stare per accedere ad un'area videosorvegliata e delle finalità per cui è attivo il sistema di videosorveglianza.

A tale scopo, occorre predisporre la cartellonistica adeguata, che deve riportare il nominativo del titolare del trattamento e le finalità perseguite.

Il cartello deve [307]:

- essere apposto prima del raggio di azione delle telecamere, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche nel caso in cui il sistema di videosorveglianza sia attivo in orario notturno;
- contenere un simbolo o un'icona di immediata comprensione, che identifichi se le immagini sono solo visionate o anche registrate.

Detta informativa, c.d. "minima o semplificata", deve poi rinviare ad un'informativa completa, redatta nel rispetto dell'articolo 13 del GDPR e che deve, quindi, contenere tutti gli elementi previsti dalla norma [308] ed essere disponibile

307 Si veda l'articolo 3.1, Garante per la protezione dei dati personali provvedimento in materia di videosorveglianza del 08.04.2010, doc. web n. 1712680.

308 Nello specifico, l'articolo 13 del GDPR prevede che "*In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenute, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari di dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare il periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento 'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo*

agevolmente e senza oneri a tutti gli interessati, con modalità facilmente accessibili anche di natura telematica (ad esempio, tramite la pubblicazione in reti intranet o siti internet, l'affissione in bacheche e/o locali, ecc.).

b. Le misure di sicurezza

È fondamentale che il titolare del trattamento - al fine di limitare i rischi di violazioni di dati (dispersione, accesso non autorizzato, ecc.) - individui e metta in atto, anche con riferimento al sistema di videosorveglianza, tutte le misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, conformemente al principio di "*accountability*" [309] previsto dal Regolamento.

Particolare attenzione deve essere adottata nel caso in cui il sistema di videosorveglianza preveda la conservazione delle immagini. Si deve, infatti, ricordare che il GDPR sancisce il principio della limitazione della conservazione [310], secondo cui i dati possono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

In linea con quanto previsto dal Garante Privacy nel provvedimento in materia di videosorveglianza del 08.04.2010, la conservazione delle immagini deve, quindi, essere limitata a poche ore o, al massimo, alle 24 ore successive alla rilevazione, fatta salva l'esigenza di ulteriore conservazione in caso di festività o per assolvere a specifiche richieste avanzate dall'autorità giudiziaria. Solo in ipotesi eccezionali e per alcuni tipi di attività particolarmente a rischio [311] è possibile, invece, prevedere un allungamento dei tempi di conservazione, che, comunque, non possono superare la settimana.

Devono, poi, essere previsti particolari accorgimenti tecnici che garantiscano, ad esempio, di non superare il periodo di conservazione e misure che assicurino l'accesso alle immagini ai soli soggetti autorizzati, di cui si parlerà nel punto seguente.

9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo all'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato […]"

309 Il principio di *accountability* trova definizione nel considerando 74 e nell'articolo 5.2 del GDPR.

310 Il principio di limitazione della conservazione trova, invece, definizione nell'articolo 5.2 lettera e) del GDPR, ove è previsto che i dati personali devono essere "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato*".

311 Si veda Garante per la protezione dei dati personali, provvedimento in materia di videosorveglianza del 08.04.2010, doc. web n. 1712680, ove all'articolo 3.4 si legge espressamente che "[…] *per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina)* […]".

c. La nomina dei designati e dei responsabili del trattamento

Come noto, il Regolamento prevede che ***nessuno*** può trattare i dati se non è istruito in tal senso dal titolare .

È, quindi, indispensabile individuare i soggetti che, internamente alla società, hanno accesso alle immagini e ai locali ove sono situate le postazioni di controllo. Detti soggetti, denominati "**designati**" **al trattamento**, devono essere (i) formalmente nominati per iscritto e (ii) formati sulle modalità di trattamento dei dati.

Detti soggetti, oltre ad essere limitati nel numero, devono avere dei diversi livelli di accesso. È, quindi, opportuno individuare coloro che possono visionare unicamente le immagini e coloro che possono effettuare altre operazioni sui sistemi [312].

Occorrerà, poi, stipulare con coloro che, esternamente alla realtà aziendale, hanno accesso alle immagini (**responsabili del trattamento**), il contratto previsto dall'articolo 28 del Regolamento. Prima tra tutti, la società che si occupa della manutenzione del sistema di videosorveglianza.

d. Registro delle attività di trattamento

Il titolare deve avere, altresì, compilare il registro delle attività di trattamento (previsto dall'articolo 30 del Regolamento) inserendo, tra i trattamenti, la videosorveglianza e avendo cura di indicare, tra gli altri elementi richiesti dalla norma, le misure di sicurezza tecniche ed organizzative adottate.

e. La valutazione di impatto (DPIA)

L'articolo 35 del GDPR prevede l'obbligo di effettuare la valutazione di impatto nel caso di "*sorveglianza sistematica su larga scala di una zona accessibile al pubblico*".

Stando ai criteri individuati nelle Linee Guida [313] del Gruppo di lavoro articolo 29 [314] la valutazione di impatto è, invece, obbligatoria in caso di "*monitoraggio sistematico di una zona accessibile al pubblico*" e qualora il trattamento riguardi "*dati di soggetti vulnerabili*", tra cui vengono annoverati anche i lavoratori.

Alla luce di tali indicazioni, nel caso di installazione di un sistema di videosorveglianza che riprenda i lavoratori, la DPIA deve essere effettuata.

312 Si veda l'articolo 3.3.2, Garante per la protezione dei dati personali, provvedimento in materia di videosorveglianza del 08.04.2010, doc. web n. 1712680.

313 Linee-guida concernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679, WP248 rev. 01, adottate il 04.04.2017, come modificate e adottate da ultimo il 04.10.2017.

314 Gruppo di lavoro europeo indipendente che ha trattato questioni relative alla protezione dei dati personali fino al 25 maggio 2018, oggi sostituito dal Comitato europeo per la protezione dei dati.

Ad ulteriore conferma di questo orientamento, lo scorso ottobre l'Autorità Garante ha pubblicato l'elenco dei trattamenti soggetti a DPIA, includendo tra questi i "*trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dei dipendenti*".

Sembra, quindi, non esserci più alcun dubbio sulla necessità di effettuare la DPIA qualora la videosorveglianza comporti la possibilità di effettuare controlli a distanza dei lavoratori.

2.1.1.2 Geolocalizzazione

Quando si parla di geolocalizzazione nell'ambito dei rapporti di lavoro, si fa principalmente riferimento ai veicoli aziendali su cui sono installati dispositivi telematici (quali ad esempio il sistema di tracciamento di base GPS, i registratori di dati relativi ad eventi, ecc.), che consentono al datore di lavoro di raccogliere tutta una serie di dati non solo relativi al veicolo stesso, bensì anche a coloro che lo utilizzano, ovvero i lavoratori.

È, quindi, evidente che, anche in questo caso, il titolare/datore di lavoro, oltre a rispettare quanto sancito dallo Statuto dei Lavoratori, di cui si parlerà oltre, dovrà adottare tutte le tutele previste dalla normativa privacy [315].

a. L'informativa

Anche nel caso della geolocalizzazione, il titolare/datore di lavoro deve, anzitutto, informare gli interessati circa il trattamento dei dati.

Occorre, quindi:

- collocare nei veicoli in questione, utilizzati per l'esecuzione delle prestazioni lavorativa, vetrofanie recanti la dizione "*veicolo sottoposto a localizzazione*" o, comunque, avvisi ben visibili che segnalino la presenza di un sistema di geolocalizzazione del veicolo;
- informare i lavoratori con un'apposita informativa recante tutti gli elementi previsti dall'articolo 13 del GDPR.

Ai lavoratori deve, infatti, essere ben chiaro che a bordo dei veicoli che andranno a guidare sono stati installati dispositivi di tracciamento e che i loro movimenti verranno registrati durante l'uso dei veicoli stessi.

Qualora, poi, il datore di lavoro consenta al lavoratore l'uso privato del veicolo aziendale, questi dovrà avere la possibilità di disattivare temporaneamente il sistema di tracciamento della posizione qualora circostanze particolari di riservatezza lo giustifichino (come nel caso del prestatore di lavoro che si rechi ad

315 In particolare, Garante per la protezione dei dati personali, provvedimento in materia di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro del 04.10.2011, n. 370, doc. web. n. 1850581.

una visita medica). Il lavoratore deve, quindi, poter proteggere determinati dati relativi all'ubicazione, considerati di natura privata.

A detti adempimenti devono, poi, aggiungersi quelli già esaminati nel precedente paragrafo relativamente alla videosorveglianza, ovvero:

b. la nomina dei designati e dei responsabili del trattamento

c. il registro delle attività di trattamento

d. la valutazione di impatto - DPIA

Inoltre, nel rispetto dei principi di **necessità**, **pertinenza** e **non eccedenza**, il datore di lavoro deve trattare solo quei dati **necessari** rispetto alle finalità perseguite e non dovrebbe, di regola, monitorare continuativamente la posizione del veicolo, salvo che ciò sia necessario per il conseguimento di finalità legittimamente perseguite, né tantomeno utilizzare i dati personali per finalità di tracciamento e/o di valutazione dei lavoratori.

Il datore di lavoro, inoltre, deve assicurarsi che i sistemi informativi e i relativi programmi siano configurati in modo da: i) ridurre al minimo l'utilizzo di dati personali e ii) stabilire tempi di conservazione adeguati e commisurati al perseguimento delle finalità.

2.1.2 Gli obblighi giuslavoristici

I sistemi di videosorveglianza e geolocalizzazione sono strumenti dai quali può derivare la possibilità di un controllo a distanza dei lavoratori.

Entrano, quindi, in "gioco" l'articolo 4 dello Statuto dei Lavoratori [316] e le relative prescrizioni.

Il comma 1 della norma citata stabilisce che l'utilizzo di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività lavorativa è consentito a condizione che questi siano impiegati:

- per **esigenze organizzative e produttive**;
- per la **sicurezza sul lavoro**;
- per la **tutela del patrimonio aziendale**.

Dette finalità si ritengono soddisfatte, ad esempio, quando:

- i macchinari e gli impianti richiedono di un monitoraggio continuo, posto che necessitano di frequenti interventi di manutenzione urgente (esigenze organizzative e produttive);

316 Così come modificato alla luce dell'articolo 23 del Decreto Legislativo del 14 settembre 2015, n.151 (in Suppl. Ordinario n. 53 alla Gazz. Uff., 23 settembre 2015, n. 221) - Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183 (c.d. Jobs Act).

- è necessario garantire l'intervento tempestivo delle squadre di soccorso, in tutti quei casi in cui si svolgano attività intrinsecamente pericolose o siano impiegati materiali nocivi alla salute ovvero i lavoratori operino in luoghi isolati o in impianti di grandi dimensioni (sicurezza del lavoro);
- in presenza di beni materiali e immateriali di elevato valore economico, ovvero quando siano avvenuti intromissioni o furti denunciati (tutela del patrimonio aziendale).

Ricorrendo queste ipotesi, detti strumenti possono essere installati previo accordo collettivo stipulato con le rappresentanze sindacali [317] o, in mancanza di accordo, previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro [318].

Prima di procedere con l'istallazione dell'impianto audiovisivo e/o di altri strumenti da cui derivi un possibile controllo dell'attività lavorativa, il datore di lavoro deve, quindi, alternativamente:

- sottoscrivere un accordo collettivo con la rappresentanza sindacale unitaria (RSU) o aziendale (RSA) che regolamenti il funzionamento e l'utilizzo dell'impianto, se in azienda sono presenti la RSU o RSA;
- chiedere all'Ispettorato del Lavoro territorialmente competente l'autorizzazione all'installazione dell'impianto, mediante il deposito di un'apposita istanza ampiamente motivata, qualora il predetto accordo non sia stato raggiunto, oppure nel caso in cui in azienda non siano presenti la RSU o RSA.

Solo a dette condizioni l'utilizzo dell'impianto audiovisivo e di altri strumenti da cui derivi o possano derivare controlli a distanza dell'attività lavorativa del lavoratore potrà considerarsi legittimo.

3. Gli strumenti informatici aziendali: l'importanza delle policy

Per strumenti informatici aziendali si intendono tutti quegli strumenti - tra cui personal computer, laptop, tablet, smartphone, rete aziendale, navigazione internet, posta elettronica, ecc. - di proprietà del datore di lavoro, che questi mette a disposizione dei propri lavoratori per lo svolgimento dell'attività lavorativa.

L'impiego di detti strumenti non necessita dell'accordo sindacale e/o dell'autorizzazione amministrativa, né tantomeno gli stessi devono essere finalizzati al raggiungimento di esigenze organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale [319].

317 Rappresentanza sindacale unitaria o rappresentanze sindacali aziendali, così come indicato dall'articolo 4.1 della Legge 20 maggio 1970, n. 300.

318 Si veda l'articolo 4.1 della Legge 20 maggio 1970, n. 300 ove è indicato che "[…] *in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro*".

319 L'articolo 4.2 della Legge 20 maggio 1970, n. 300 prevede, infatti, espressamente che "*La disposizione*

Tuttavia è, comunque, necessario che il datore di lavoro, al fine di prevenire uno scorretto utilizzo di tali strumenti da parte dei lavoratori - che potrebbe esporre a rischi il datore di lavoro stesso - ed in ottemperanza a quanto previsto dallo Statuto dei Lavoratori [320], fornisca ai propri lavoratori delle precise indicazioni in merito:

- alle modalità di utilizzo di detti strumenti, con una breve descrizione degli stessi e delle attività consentite al lavoratore;
- alle modalità di realizzazione di eventuali controlli da parte del datore di lavoro;
- all'applicazione di eventuali sanzioni da parte del datore di lavoro in caso di violazione delle indicazioni fornite.

Tutto ciò, mediante la predisposizione di un apposito **disciplinare** (o **policy**) che deve garantire, da un lato, il diritto del datore di lavoro di proteggere la propria organizzazione aziendale e, dall'altro, il diritto del lavoratore a non vedere invasa la propria sfera personale, ovvero il diritto alla riservatezza e alla dignità, così come stabiliti dallo Statuto dei Lavoratori e dalla normativa privacy [321].

Una volta predisposto, il disciplinare deve essere reso noto a tutti i lavoratori, anche mediante affissione nella bacheca aziendale o pubblicazione nella intranet aziendale.

3.1 Il contenuto del disciplinare

Per la redazione di un corretto disciplinare sull'utilizzo degli strumenti aziendali non possono certamente essere trascurati gli aspetti privacy. È, quindi, opportuno che il datore di lavoro si attenga ai principi sanciti nel GDPR e, in particolar modo, nelle Linee Guida del Garante per posta elettronica e internet del 01.03.2007 [322] .

Infatti, è proprio in quest'ultimo documento che il Garante affronta le tematiche legate alla redazione del disciplinare, soffermandosi - dopo l'indicazione dei principi generali - sull'utilizzo della navigazione internet e della posta elettronica, nonché sull'esecuzione dei controlli da parte del datore di lavoro.

di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze".

320 L'articolo 4.3 della Legge 20 maggio 1970, n. 300 stabilisce che "*Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196*".

321 In particolare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati); le Linee Guida del Garante per posta elettronica e internet del 01.03.2007, doc. web n. 1387522 e i numerosi provvedimento emessi dal Garante in materia.

322 Linee Guida del Garante per la protezione dei dati personali posta elettronica e internet del 01.03.2007, doc. web n. 1387522.

a. Navigazione internet

Con specifico riferimento alla navigazione web, il Garante, sempre al fine di tutelare la riservatezza dei lavoratori, consiglia al datore di lavoro di adottare i seguenti accorgimenti:

- elencare i comportamenti non tollerati rispetto all'attività di navigazione;
- indicare in che misura è consentito l'utilizzo della navigazione internet per ragioni personali (anche e/o solo da determinate postazioni di lavoro), con quali modalità e per quanto tempo (ad esempio fuor dall'orario di lavoro, durante le paure o, con moderazione, durante l'attività lavorativa);
- individuare le categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurare i sistemi o utilizzare filtri che impediscano determinate operazioni, reputate inconferenti con l'attività lavorativa (quali ad esempio l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche);
- trattare dati in forma anonima o in modo tale da precludere l'immediata identificazione degli utenti mediante loro opportune aggregazioni (ad esempio con riferimento ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- prevedere la configurazione di sistemi software in grado di cancellare periodicamente i dati personali relativi alla navigazione e al traffico telematico, la cui conservazione non sia necessaria. Tale accorgimento, però, non può essere applicato quando la conservazione dei dati: i) è necessaria al perseguimento di finalità organizzative, produttive e di sicurezza; ii) è indispensabili per dare rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria e iii) è richiesta dall'autorità giudiziaria o dalla polizia giudiziaria;
- specificare le conseguenze - anche di natura disciplinare - che graveranno sul lavoratore, in caso di utilizzo indebito della navigazione.

b. Posta elettronica

Il contenuto dei messaggi di posta elettronica riguarda forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente. Tuttavia, con specifico riferimento all'utilizzo della posta elettronica nell'ambito lavorativo e considerato che spesso può risultare dubbio se il lavoratore - quale destinatario o mittente - utilizzi la posta elettronica operando per l'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa, è opportuno che il datore di lavoro disciplini nella policy i seguenti aspetti:

- rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (come ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, ecc.), affiancandoli eventualmente a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- valutare la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;
- indicare in che misura è consentito l'utilizzo dei servizi di posta elettronica per ragioni personali (anche e/o solo da determinate caselle di posta, oppure mediante l'uso di sistemi di webmail), con quali modalità e per quanto tempo (ad esempio fuor dall'orario di lavoro, durante le paure o, con moderazione, durante l'attività lavorativa);
- mettere a disposizione di ciascun lavoratore apposite funzionalità di sistema, che consentano di inviare automaticamente ed in caso di assenze (come nel caso di ferie o di attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" elettroniche o telefoniche di un altro soggetto o altre utili modalità di contatto della struttura.
- in caso di eventuali assenze non programmate (come ad esempio in caso di malattia), qualora il lavoratore non possa attivare la procedura descritta al precedente punto e perdurando l'assenza oltre un determinato limite temporale, disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad esempio l'amministratore di sistema o il referente privacy), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa si debba conoscere il contenuto dei messaggi di posta elettronica, consentire al lavoratore di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al datore di lavoro quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa;
- redigere un apposito verbale in caso di attivazione della predetta procedura e informare il lavoratore interessato alla prima occasione utile;
- prevedere che i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy;
- specificare le conseguenze - anche di natura disciplinare - che graveranno sul lavoratore, in caso di utilizzo indebito dell'account di posta elettronica.

In caso di cessazione del rapporto di lavoro, peraltro, il datore di lavoro è tenuto a disattivare immediatamente l'account di posta elettronica assegnato al lavoratore, con modalità tali da inibire in via definitiva la ricezione in entrata di

tutti i messaggi diretti al predetto account, nonché la conservazione sui server aziendali.

Contemporaneamente alla disattivazione, il datore di lavoro è altresì tenuto ad attivare un sistema di risposta automatica, che informi gli eventuali mittenti della disattivazione stessa e fornisca eventuali nuove coordinate di contatto del datore di lavoro stesso [323].

c. Controlli

Anche con riferimento ai controlli - che devono sempre essere rispettosi dei principi di pertinenza e non eccedenza [324] - il Garante ha fornito al datore di lavoro delle indicazioni ben precise, che devono essere adottate e rispettate per evitare di realizzare un'interferenza ingiustificata nei diritti e nelle libertà dei lavoratori.

Nel caso in cui un evento dannoso e/o una situazione di pericolo non siano stati impediti da accorgimenti tecnici, il datore di lavoro può adottare quelle misure atte a verificare i comportamenti anomali.

Nel verificare il comportamento anomalo, però, il datore di lavoro dovrà dapprima effettuare un controllo preliminare sui dati aggregati, ovvero sui dati riferiti all'intera struttura lavorativa o alle sue aree. Tale controllo (anonimo) potrà concludersi con un avviso generalizzato relativo a un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente alle istruzioni impartite.

Solo nel caso in cui venissero riscontrate altre anomalie, il datore è giustificato a realizzare dei controlli su base individuale.

È, però, importante ricordare che non possono essere effettuati da parte del datore di lavoro controlli prolungati, costanti e indiscriminati.

323 Si vedano tra i tanti Garante per la protezione dei dati personali, provvedimento del 01.02.2018, doc. web. n. 8366193 e Garante per la protezione dei dati personali, provvedimento del 22.12.2016 doc. web. n. 5958296, in materia di accesso alla posta elettronica dei dipendenti.

324 Si veda l'articolo 6.1 delle Linee Guida del Garante per la protezione dei dati personali per posta elettronica e internet del 01.03.2007, doc. web n. 1387522.

CAPITOLO 5 di Micaela Barbotti e Roberto Tirone

Privacy e Odv: l'impatto della disciplina privacy nell'attività dell'ODV

Compliance 231/2001. Privacy e Odv: l'impatto della disciplina privacy nell'attività dell'ODV, sui flussi informativi e sulle segnalazioni. Il ruolo del DPO

SOMMARIO: 1. La conservazione dei verbali dell'ODV – 2. Whistleblowing e privacy – 3. La qualificazione dell'OdV in ambito privacy – 4. Rapporti tra Organismo di Vigilanza e Data Protection Officer (DPO)

1. La conservazione dei verbali dell'ODV

La società, qualora abbia correttamente applicato il GDPR, dovrebbe aver inviato a tutti gli interessati una informativa sull'attività dell'ODV, sulla facoltà dell'ODV di esaminare documenti e di effettuare interviste ai dipendenti, e di acquisire, così, tutta una serie di informazioni e dati personali, incluse categorie particolari di dati personali, che vengono poi trasfusi sinteticamente in un verbale.

Gli interessati, poi, dovrebbero aver espresso il loro consenso scritto al trattamento dei dati da parte dell'ODV.

Ora, come è noto, l'ODV normalmente redige un verbale sull'attività svolta, riassumendo i dati acquisiti ed allegando la documentazione raccolta.

Inoltre, l'ODV effettua, in caso d'urgenza, una comunicazione al Consiglio di Amministrazione indicando i fatti di rilievo emersi durante una specifica sessione ovvero, in assenza di urgenza, aggiorna periodicamente il Consiglio di Amministrazione con un rendiconto scritto.

Anche tali comunicazioni potrebbero contenere dati personali, incluse categorie particolari di dati personali.

Diviene, quindi, importante individuare le regole sia del trattamento dei dati, sia della conservazione dei dati (verbali, documenti ecc.), sia delle modalità di trasmissione delle informazioni al Consiglio di Amministrazione.

È chiaro che il trattamento dei dati da parte dell'ODV dovrà essere limitato a quanto necessario per il corretto svolgimento della propria attività. L'ODV non dovrà, dunque, raccogliere e conservare dati irrilevanti od eccessivi rispetto ai fini istituzionali dello stesso ODV.

I dati raccolti dall'ODV, poi, dovranno essere conservati in modalità elettronica con un sistema criptato, il cui accesso sia limitato ai membri dell'ODV ed in modalità cartacea attraverso l'individuazione di un luogo chiuso a chiave, le cui chiavi siano in possesso dei soli membri dell'ODV (ad esempio un mobile presso la segreteria del Consiglio di Amministrazione).

Quanto al tempo di conservazione dei dati, il GDPR richiede che venga individuata una data massima di conservazione dei documenti contenenti dati personali tenendo conto che il trattamento di dati personali può essere effettuato per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono stati trattati.

La domanda che ci si deve porre è, dunque: quando cessa la necessità di conservazione dei documenti e dei verbali dell'ODV?

Rispondere a tale domanda non è semplice: i documenti acquisiti dall'ODV ed i verbali dell'ODV non solo solamente utili ai fini del controllo periodico, ma sono anche la prova dell'effettuazione dei controlli periodici; prova che potrebbe essere richiesta dall'autorità giudiziaria in un secondo momento.

Si potrebbe, dunque, affermare che i documenti ed i verbali dell'ODV debbano essere conservati sino alla prescrizione del reato più grave previsto dal DLGS 231/2001, ma ciò vorrebbe probabilmente dire che non verranno mai distrutti.

Maggiormente orientata ai principi del GDPR sembrerebbe essere la regola che molti ODV adottano per la quale i documenti ed i verbali dell'ODV devono essere distrutti dopo 5 o 10 anni a seconda della tipologia di documento.

2 Whistleblowing e privacy

Come noto la legge n. 179/2017, modificando l'articolo 6 del D. Lgs 231/2001, ha introdotto nel settore privato la disciplina del c.d."whistleblowing", sistema aziendale che consente al dipendente di segnalare, a tutela dell'integrità dell'ente, condotte illecite e irregolarità compiute da altri dipendenti.

Il whistleblowing ha diverse implicazioni in materia di protezione dei dati personali, e questo sia con riferimento all'interessato – soggetto segnalante, sia con riferimento all'interessato - soggetto segnalato che tuttavia non hanno ad oggi una specifica disciplina.

Tali implicazioni erano peraltro emerse già prima che tale sistema di segnalazione avesse in Italia una specifica disciplina, posto che anche prima dell'entrata in vigore della legge n. 179/2017 diverse realtà aziendali italiane avevano adottato meccanismi di segnalazione riconducibili al whistleblowing.

Nel 2006 il Gruppo di Lavoro ex articolo 29 (organismo consultivo indipendente composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione, oggi sostituito dal Comitato Europeo per la protezione dei dati) ha pubblicato un parere circa l'applicazione della disciplina in materia di prote-

zione dei dati personali alle procedure interne per la denuncia di irregolarità in determinati settori [325] e nel 2009 il Garante per la protezione dei dati personali ha emesso una Segnalazione al Parlamento e al Governo [326] in materia, auspicando un intervento legislativo.

Al fine di individuare i principi generali cui ispirare il trattamento dei dati personali nell'ambito dei sistemi di whistleblowing nel settore privato, può inoltre essere utile fare riferimento alle linee guida del Garante europeo della protezione dei dati pubblicate nel luglio 2016 [327], anche se le stesse si riferiscono ai sistemi di whistleblowing adottati all'interno delle istituzioni e degli organismi europei.

Sia il parere del Gruppo di Lavoro ex articolo 29 sia la Segnalazione del Garante evidenziano, tra gli aspetti critici della compatibilità della disciplina in materia di protezione dei dati con i sistemi di segnalazione di illeciti adottati dalle aziende, tra gli altri, quello del presupposto di liceità del trattamento e quello dell'esercizio del diritto di accesso da parte dell'interessato – segnalato.

Con riferimento al presupposto di liceità del trattamento e quindi alla sua base giuridica, si ritiene che il trattamento dei dati personali svolto dalla società possa ritenersi necessario per il perseguimento del legittimo interesse del titolare del trattamento ad attuare un sistema di segnalazione interno di condotte illecite rilevanti ai sensi di quanto previsto dal D. Lgs. 231/2001, rientrando quindi tale trattamento nella previsione di cui all'articolo 6, comma 1, lettera f), del GDPR.

Secondo quanto precisato dall'articolo 6 del D. Lgs 231/2001, come modificato dall'art. 2 della legge 179/2017, nelle attività di gestione delle segnalazioni deve essere garantita la riservatezza del segnalante. È cioè essenziale che venga protetto adeguatamente l'autore della segnalazione, in modo da evitare che il denunciato o terzi ne scoprano l'identità, e ciò ovviamente non solo per evitare ritorsioni sul soggetto denunciante ma anche, in linea generale, per incoraggiare l'uso del sistema.

La necessità di mantenere riservata l'identità del segnalante determina una necessaria limitazione del diritto di accesso del denunciato, ovvero di uno dei diritti che la disciplina in materia di protezione dei dati personali riconosce all'interessato.

Il legislatore italiano ha disciplinato in modo specifico questa fattispecie, inserendo una previsione in materia di whistleblowing nel D. Lgs. 101/2018, emanato a seguito dell'entrata in vigore del GDPR per coordinare la vecchia

325 Gruppo di lavoro articolo 29, Parere 1/2006 relativo all'applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denunzia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione la criminalità bancaria e finanziaria.

326 Garante per la protezione dei dati personali, Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale – 10 dicembre 2009.

327 Garante Europeo della protezione dei dati personali, *Guidelines on processing personal information within a whistleblowing procedure*, adottate nel luglio 2016

disciplina alla nuova e per disciplinare gli ambiti lasciati dal GDPR all'autonomia degli Stati Membri.

L'articolo 2 *undecies* del D. Lgs 101/2018 prevede infatti, alla lettera f), che l'interessato non possa esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto "alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio".

Tale previsione trova il suo fondamento nell'articolo 23 GDPR che, disciplinando quanto anticipato dal considerando 53, prevede che gli Stati membri possano limitare i diritti riconosciuti all'interessato qualora tale limitazione sia una misura necessaria ed adeguata a salvaguardare, tra l'altro, la prevenzione e l'accertamento di reati (lettera f).

Alla luce dell'art. 2 *undecies* del D. Lgs 101/2018, il principio generale ai sensi del quale l'interessato, esercitando il diritto di accesso previsto dall'articolo 15 del GDPR, avrebbe diritto, tra l'altro, a conoscere l'origine dei dati personali trattati, è oggetto di deroga con riferimento all'identità del soggetto che segnale un illecito nell'ambito del sistema di whistleblowing. Pertanto, in caso di esercizio del diritto di accesso da parte del soggetto denunciato, in nessun caso la società in qualità di titolare del trattamento potrà rivelare il nome del soggetto denunciante.

Vige ovviamente sulla società, in qualità di titolare del trattamento, l'obbligo di fornire agli interessati l'informativa relativa al trattamento dei dati personali ai sensi di quanto previsto dagli articoli 13 e 14 del GDPR. La società dovrà cioè, tra l'altro, indicare ai soggetti interessati le finalità e il funzionamento del sistema di segnalazione interno, i destinatari delle denunce, i diritti riconosciuti alla persona denunciata e il periodo di conservazione dei dati personali.

Con riferimento al periodo di conservazione dei dati personali vige il principio generale, enunciato oggi all'articolo 5 del GDPR, ai sensi del quale i dati personali possono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Ovviamente i dati personali trattati e conservati nell'ambito della procedura di segnalazione dovranno quelli strettamente e obbiettivamente necessari per verificare la fondatezza della denuncia. Sul tema del periodo di conservazione, il Parere del gruppo di Lavoro ex articolo 29 precisa che i dati personali trattati nell'ambito di una procedura interna di denuncia dovrebbero essere cancellati entro due mesi dal completamento della verifica dei fatti esposti nella denuncia, fatta eccezione per il caso di azione giudiziaria o disciplinare nei confronti del denunciato ed eventualmente del denunciante in caso ad esempio di dichiarazioni false o diffamatorie.

La società dovrà infine garantire la sicurezza dei dati raccolti attraverso il sistema di segnalazione e quindi, alla luce del principio di accountability e dell'articolo 32 GDPR, individuare e adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio, e questo con riferimento alle diverse modalità di segnalazione adottati dall'azienda, sia che

si tratti di modalità cartacee sia che si tratti di modalità telematiche. Tali dati personali dovranno ovviamente essere accessibili solo a determinati soggetti, specificamente autorizzati dal titolare del trattamento, che li tratteranno esclusivamente per il legittimo svolgimento dei compiti assegnati.

3. La qualificazione dell'OdV in ambito privacy

L'art. 4 del Regolamento UE 679/2016 (in seguito "Regolamento") definisce trattamento "Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Alla luce della predetta definizione, è pacifico che l'Organismo di Vigilanza, nello svolgimento dei propri compiti, tratti necessariamente dati personali: pensiamo, ad esempio, alla gestione dei flussi informativi, allo svolgimento delle attività di controllo e vigilanza, al c.d. whistleblowing ed anche alle attività di conservazione e archiviazione.

Si pone, dunque, l'esigenza di qualificare, dal punto di vista soggettivo, l'Organismo di Vigilanza, individuando poi di conseguenza tutti gli adempimenti da adottare, sia da parte dell'ente che dell'Organismo stesso.

Il tema è stato oggetto di dibattito e discussione anche in occasione delle *Corporate Round Tables* di ASLA del 14.11.2018, dove – considerata l'assenza di indicazioni univoche e concordanti – sono emerse sostanzialmente tra differenti soluzioni: Titolare del Trattamento, Responsabile del Trattamento ex art. 28 del Regolamento o Autorizzato al Trattamento. Le prime due ipotesi presuppongono una soggettività autonoma dell'OdV, la terza invece considera l'organismo come soggetto "interno" all'ente.

La tesi secondo la quale l'OdV debba qualificarsi come Titolare (autonomo) del Trattamento valorizza gli "*autonomi poteri di iniziativa e di controllo*" citati dall'art. 6, comma 1 lettera b) del D. Lgs. n. 231/2001 ed effettua un parallelismo con i poteri del Titolare di determinare le "finalità ed i mezzi del trattamento".

La qualifica dell'OdV come Titolare comporta che questi dovrà effettuare tutti gli adempimenti ed adottare tutte le misure imposte dal Regolamento al Titolare, dalle informative agli interessati, alle nomine dei Responsabili ex art. 28 e degli autorizzati, all'adozione del registro dei trattamenti e delle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e via di seguito.

La principale obiezione che viene mossa a questa tesi è che, in realtà, le finalità del trattamento non sono determinate dall'OdV, ma sono individuate nelle disposizioni contenute nel D. Lgs. n. 231/2001 e nel Modello Organizza-

tivo adottato dall'ente. Si è inoltre evidenziato che l'OdV è istituito dall'organo dirigente, che ne disciplina le principali regole di funzionamento.

Coloro che propendono verso l'inquadramento dell'OdV come Responsabile del Trattamento ex art. 28 partono proprio dal presupposto che la titolarità del trattamento rimane in capo all'ente, che poi "trasferisce" i dati all'OdV al fine di consentirgli l'espletamento dei suoi compiti. Proprio l'assenza di poteri decisionali in merito alle finalità ed ai mezzi del trattamento, ha come conseguenza che l'OdV debba essere nominato Responsabile ex art. 28 con un apposito atto, contenente tutte le prescrizioni cautelative. Anche questa tesi, non è esente da critiche. Si è, infatti, da più parti evidenziato che il requisito essenziale per assumere la qualifica di Responsabile è proprio quello di essere un soggetto giuridico diverso e distinto dal Titolare, requisito questo che difetta in caso di OdV qualificato come organo "interno" all'ente a cui si riferisce.

L'ultima ipotesi che si è andata di recente definendo, grazie anche a specifici approfondimenti da parte delle più importanti associazioni, prima tra tutte l'AODV, è quello di escludere che l'OdV possa qualificarsi Titolare o Responsabile ex art. 28, dovendo invece qualificarsi – ovviamente solo ai fini privacy - come "parte dell'impresa". In questo senso, al pari del Collegio Sindacale, sarà un soggetto organicamente inserito nell'ente, a cui l'ente stesso fornirà specifica autorizzazione al trattamento dei dati.

4 Rapporti tra Organismo di Vigilanza e Data Protection Officer (DPO)

L'art. 39 del Regolamento individua i compiti del DPO precisando che questi (almeno) deve:

- informare e fornire consulenza al Titolare o al Responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento e dalle disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del Titolare o del Responsabile;
- fornire parere in merito alla valutazione di impatto (DPIA) di cui all'art. 35 del Regolamento;
- cooperare con l'Autorità di controllo e fungere da punto di contatto con questa per questioni attinenti al trattamento.

Per il WP29 la nomina di un DPO è importante perché rappresenta un elemento fondante anche ai fini dell'accountability.

Per certi versi il DPO assume, con riferimento al Regolamento e alla normativa nazionale in materia di protezione dei dati, un ruolo simile a quello che svolge l'OdV rispetto al Modello Organizzativo. Entrambe le figure, con la

loro professionalità, competenza ed autonomia, valutano e vigilano, riportando all'organo dirigente.

Sebbene i delitti in materia di privacy non rientrino tra le fattispecie penali attualmente previste dalla normativa sulla responsabilità amministrativa degli enti ex D. Lgs. n. 231/2001, non mancano punti di contatto tra "privacy" e "231": si pensi ad esempio all'inclusione, tra i reati-presupposto, dei reati informatici e di trattamento illecito di dati indicati nell'art. 24 bis e di alcuni reati che richiedono l'utilizzo di sistemi informatici (come la frode informatica ed anche taluni delitti in materia di violazione del diritto d'autore). Secondo taluni autori, inoltre, i reati privacy potrebbero costituire i reati-scopo di un'associazione per delinquere.

Si comprende, dunque, il motivo per cui il DPO debba essere un interlocutore dell'OdV, esattamente come lo sono il Responsabile del Servizio di Prevenzione e Protezione ed i Responsabili dei Sistemi di Gestione aziendale (Qualità, Ambiente, Sicurezza ecc.); la cooperazione ed il confronto reciprocamente costruttivi evitano di creare sistemi di controlli interni sovrabbondanti e incoerenti, a vantaggio invece di meccanismi di controllo veramente efficaci ed efficienti. In questo modo, inoltre, si garantisce maggiormente il collegamento e la coordinazione tra i due modelli di compliance "privacy" e "231", collegamento e coordinazione peraltro che dovrebbero sussistere dalla fase di mappatura e valutazione del rischio a quella, appunto, dei controlli.

Auspicabile quindi che ODV calendarizzi almeno un incontro annuale con il DPO e disciplini l'invio di flussi informativi, da parte di quest'ultimo, in caso non solo di data breach, ma anche di criticità e violazioni che non abbiano comportato obblighi di notifica al Garante.

Basilare inoltre che OdV e DPO collaborino e cooperino nel processo di aggiornamento del Modello Organizzativo ed anche nell'implementazione della procedura per la gestione delle segnalazioni, dove è fondamentale garantire il principio della riservatezza.

Quanto, infine, alla possibilità per il DPO di essere componente dell'OdV, secondo esperti autorevoli, sarebbe preferibile optare per la risposta negativa e ciò proprio in considerazione dei compiti e del ruolo che gli sono attribuiti, primi tra tutti quelli di fungere da punto di contatto con l'Autorità Garante e di punto di riferimento per gli interessati.

CAPITOLO 6 di Tiziana Boneschi, Pietro Orzalesi e Cecilia Pontiggia

Whistleblowing: la complessità di un sistema semplice

SOMMARIO: 1. Introduzione – 2. Il Whistleblowing in Europa – 3. Il Whistleblowing in Italia: evoluzione del contesto normativo di riferimento – 4. La Legge n. 179/2017: nuove tutele nel settore privato – 5. La gestione delle segnalazioni – 6. Applicazioni pratiche a confronto

1. Introduzione

Obiettivo del tavolo di lavoro è stato quello di approfondire i temi "caldi" connessi all'istituto del whistleblowing, tra cui la regolamentazione e la documentazione del processo di segnalazione, la sicurezza informatica, l'implementazione del sistema nell'ambito di gruppi multinazionali nel coacervo delle discipline locali, l'identificazione del destinatario delle segnalazioni e il ruolo dell'Organismo di Vigilanza nominato ai sensi del D.Lgs. 231/2001, nonché gli strumenti di tutela della riservatezza dell'identità del segnalante e l'eventuale anonimato.

Ciò alla luce del quadro normativo come di seguito rappresentato.

2. Il Whistleblowing in Europa

Il *Whistleblowing* è un istituto di derivazione anglosassone attraverso il quale i dipendenti di un'organizzazione, pubblica o privata, segnalano a organismi preposti o autorità la commissione di un reato, di un illecito o semplicemente di una condotta immorale o di comportamenti scorretti tenuti da soggetti appartenenti alla medesima organizzazione.

Il *Whistleblower* è pertanto chi effettua tali segnalazioni e che, in ragione di ciò, deve essere tutelato da possibili ritorsioni provenienti dall'organizzazione per cui lavora.

L'introduzione della disciplina in esame, comporta senz'altro un effetto benefico rilevante: essa permette infatti la tempestiva conoscenza di situazioni di rischio e/o di danno, contribuendo a creare un clima trasparente e un senso di partecipazione all'interno dell'organizzazione stessa, migliorandone conseguentemente l'immagine e la reputazione.

Data l'importanza del tema e la frammentarietà delle soluzioni adottate dai diversi Paesi europei, il 16 aprile 2019 il Parlamento Europeo ha approvato la Direttiva 2018/0106 sul *Whistleblowing*, volta a rafforzare la tutela nei confronti dei lavoratori che segnalano le violazioni del diritto comunitario in settori quali appalti pubblici, servizi finanziari, riciclaggio di denaro, sicurezza dei prodotti e dei trasporti, sicurezza nucleare, salute pubblica, protezione dei consumatori e dei dati.

La Direttiva, oltre ad armonizzare la disciplina nei vari Paesi dell'Unione, introduce maggiori garanzie a sostegno dei segnalanti, in particolar modo ricercando la piena equiparazione tra il settore pubblico e quello privato, a differenza di quanto previsto sino ad ora dalla legislazione nazionale italiana.

Al fine di garantire la sicurezza dei potenziali segnalanti e la riservatezza delle informazioni divulgate, i meccanismi di protezione contemplati dalla Direttiva consentono di trasmettere le segnalazioni attraverso tre differenti canali: *i*) il primo interno alla medesima organizzazione presso cui si lavora; *ii*) il secondo diretto alle Autorità nazionali competenti, qualora i canali interni non siano efficaci o siano tali da compromettere l'efficacia dell'azione investigativa e infine *iii*) il terzo, destinato ai mezzi di informazione, quali organi e agenzie competenti della Ue, da utilizzare ad esempio in caso di inerzia o di pericolo imminente per il pubblico interesse.

Tra le maggiori novità si evidenzia inoltre l'obbligo di esaminare le segnalazioni anche se anonime, condizione tra l'altro non espressamente contemplata dalla Legge italiana n. 179/2017.

Rimaniamo pertanto in attesa di sviluppi in quanto, a seguito all'approvazione definitiva del testo di legge da parte dei Ministri Ue, gli Stati membri sono chiamati ad adeguare le normative nazionali entro due anni.

3. Il Whistleblowing in Italia: evoluzione del contesto normativo di riferimento

Nel sistema normativo italiano, la prima forma di espressa tutela nei confronti del *Whistleblower* risale all'entrata in vigore della L. 190/2012, c.d. Legge Severino, recante "*Disposizioni per la prevenzione e la repressione della corruzione dell'illegalità nella pubblica amministrazione*", che ha introdotto nel D.Lgs. 165/2001 (c.d. "TU Pubblico Impiego") l'art. 54-bis, "*Tutela del dipendente pubblico che segnala illeciti*".

Nella sua originaria formulazione, detto articolo vietava di sottoporre a sanzione, licenziamento o a misura discriminatoria, il dipendente pubblico che denuncia all'Autorità Giudiziaria, alla Corte dei conti o all'ANAC, ovvero riferisce al proprio superiore gerarchico, condotte illecite di cui sia venuto a conoscenza in ragione del proprio rapporto di lavoro.

L'istituto è stato poi riformato dalla Legge del 30 novembre 2017, n. 179 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*", che è in particolare intervenuta su due fronti: da un lato, ha implementato la tutela già prevista per i dipendenti pubblici, ampliando il campo applicativo

dell'art. 54-*bis* del TU Pubblico Impiego; dall'altro ha introdotto nel D.Lgs. 231/2001 un esclusivo sistema di misure dedicate al *Whistleblower* "privato", da adottarsi da parte degli enti che abbiano scelto di adottare un Modello di organizzazione, gestione e controllo ai sensi dello stesso D.Lgs. 231/2001.

La *ratio* sottesa alla normativa in esame è proprio quella di individuare strumenti di tutela nei confronti di tutti i lavoratori che denuncino reati o irregolarità di cui siano venuti a conoscenza nell'ambito delle proprie attività lavorative [328] .

4. La Legge n. 179/2017: nuove tutele nel settore privato

Come sopra accennato, il Legislatore, sul fronte privato, ha incardinato la tutela del *Whistleblower* nella sistematica del D.Lgs. 231/2001 in materia di responsabilità da reato degli enti.

La nuova disciplina non si rivolge pertanto a tutti gli enti, ma solo a quelli che abbiano scelto di adottare un Modello Organizzativo ai sensi del D.Lgs. 231/2001, con la conseguenza che, rappresentando l'adozione del Modello stesso una facoltà e non un obbligo, la tutela del *Whistleblowers* parrebbe ritenersi, a sua volta, meramente facoltativa.

Passando all'analisi del dettato normativo del D.Lgs. 179/2017, un primo problema da affrontare è quello dell'individuazione del soggetto destinatario della denuncia, dal momento che l'art. 6 del D.Lgs. 231/2001 sconta sul punto una certa genericità.

Una lettura attenta della disciplina in commento parrebbe tuttavia avvalorare l'idea secondo cui sarebbe proprio l'Organismo di Vigilanza a dover rivestire il ruolo di responsabile della procedura di segnalazione, nonché soggetto ultimo destinatario della stessa segnalazione; come noto, infatti, l'Organismo è già il naturale destinatario di flussi informativi aventi ad oggetto anomalie o atipicità riscontrate dai responsabili delle diverse funzioni aziendali nell'espletamento dei propri compiti.

Pertanto, indirizzare all'Organismo il flusso informativo costituito dalle segnalazioni dei *whistleblower* sembra essere del tutto in linea con l'impianto del D.Lgs. 231/2001 e, del resto, è ormai prassi consolidata che nei Modelli siano previsti meccanismi di segnalazione di violazioni del Modello o di comportamenti illeciti all'Organismo di Vigilanza.

Tuttavia, come anticipato, il nuovo comma 2-*bis* dell'art. 6 D.Lgs. 231/2001 non menziona espressamente l'Organismo di Vigilanza quale destinatario delle segnalazioni, lasciando pertanto le organizzazioni libere di adottare soluzioni diverse. In tali casi, l'ente dovrà in ogni caso avere cura di far pervenire all'Organismo la notizia della segnalazione, per mettere quest'ultimo nelle condizioni di poter espletare i propri compiti di vigilanza sull'efficacia ed efficienza del Modello Organizzativo adottato dallo stesso ente.

328 Borsari R., Falavigna F., *Whistleblowing, obbligo di segreto e "giusta causa" di rivelazione*, in La Responsabilità amministrativa delle società e degli enti, 2/2018.

Il citato comma 2-*bis* prevede altresì che i canali di segnalazione debbano garantire la "*riservatezza dell'identità del segnalante nell'attività di gestione della segnalazione*". Tale requisito potrà ritenersi soddisfatto sia con l'introduzione di specifici obblighi di riservatezza in capo ai soggetti incaricati della gestione delle segnalazioni, sia con l'implementazione di specifici strumenti informatici all'uopo predisposti e di misure volte a garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione [329].

Sul punto, la Legge opportunamente richiede che i canali con cui veicolare le segnalazioni dei lavoratori garantiscano la riservatezza dell'identità del denunciante nelle diverse fasi di gestione della denuncia e che, almeno uno di essi, provveda a tali garanzie con modalità informatiche.

Al riguardo, si evidenza che il profilo della riservatezza dell'identità del segnalante diverge da quello dell'anonimato: il primo infatti presuppone la rivelazione della propria identità da parte del denunciante che può godere di una tutela adeguata soltanto se si rende riconoscibile; ciò non esclude però che i Modelli Organizzativi possano contemplare anche canali per effettuare segnalazioni in forma anonima.

Tale ipotesi, tuttavia, sembra rendere più complessa la verifica della fondatezza della segnalazione, con il rischio di alimentare denunce infondate e mere doglianze che potrebbero riguardare ben poco la tutela dell'integrità dell'ente. Per contenere questo rischio, sarebbe quanto meno opportuno rafforzare il fondamento della medesima denuncia, richiedendo che la stessa venga adeguatamente documentata e che vengano forniti dettagli e particolari atti a circoscrivere l'evento e collocarlo in contesti ben determinati [330].

Nonostante ciò, il silenzio della Legge pare lasciare ancora una volta l'organizzazione libera di optare per un sistema che consenta la segnalazione anonima oppure no, salvo poi tutelare coloro che decidano di rivelare la loro identità. Emerge in tutta evidenza, quindi, la necessità di ben regolamentare tale aspetto con gli strumenti propri dell'organizzazione aziendale (es. *policy* e procedure aziendali) [331].

5. La gestione delle segnalazioni

Il sistema del *Whistleblowing* implica importanti e complessi aspetti che, come visto, non sono del tutto normati e che devono pertanto essere oggetto di una puntuale gestione e regolamentazione interna da parte dell'organizzazione.

È infatti necessaria una chiara e precisa definizione dei soggetti incaricati di ricevere le segnalazioni, dei relativi obblighi di riservatezza, delle sanzioni applicabili in caso di violazione Il rilascio della certificazione ISO 37001 porterebbe

329 Pansarella M., *Problematiche giuridiche ed organizzative del Whistleblowing nei Modelli 231*, in La responsabilità amministrativa delle società e degli enti, 1/2018.

330 Confindustria, *La disciplina in materia di whistleblowing*, Nota illustrativa, Gennaio 2018.

331 Pansarella M., *Problematiche giuridiche ed organizzative del Whistleblowing nei Modelli 231*, in La responsabilità amministrativa delle società e degli enti, 1/2018.

ad ottenere degli indubbi vantaggi di tali obblighi, nonché delle diverse fasi in cui si articola il processo di gestione delle segnalazioni, tra cui:

i) la ricezione e la registrazione della segnalazione, che può avvenire mediante l'istituzione di un registro delle segnalazioni, nel quale annotare le denunce pervenute e le conseguenti azioni poste in essere;

ii) l'analisi della segnalazione, consistente nella verifica della fondatezza della segnalazione e della credibilità del segnalante;

iii) la programmazione e l'attuazione, una volta appurata la fondatezza della denuncia, delle più opportune azioni in risposta alla segnalazione;

iv) infine, l'eventuale irrogazione della sanzione, che inevitabilmente implica il coinvolgimento delle funzioni aziendali a ciò preposte.

Da quanto sopra detto, si desume come il processo di gestione della segnalazione risulti essere un sistema complesso che richiede un'adeguata regolamentazione [332], ancor più necessaria nell'ambito di grandi gruppi societari, anche multinazionali, generalmente caratterizzati da una stratificata struttura societaria e da un'articolata rete di canali di comunicazione/segnalazione, che potrebbero nascere anche dall'esigenza di adeguarsi a ulteriori specifiche normative di settore, nazionali e internazionali.

In tali contesti è pertanto fondamentale che il meccanismo di *Whistleblowing*, come sopra delineato, sia armonicamente inserito tra i preesistenti flussi e canali di comunicazione, evitando inutili duplicazioni e sviluppando soluzioni pratiche che non potranno che essere costruite "*su misura*", in base alla realtà della singola azienda e del singolo gruppo, in un'ottica di maggiore efficacia, efficienza e trasparenza delle comunicazioni che alimentano e supportano la vita lavorativa.

6. Applicazioni pratiche a confronto

I temi di cui ai precedenti paragrafi sono stati vivacemente discussi dai partecipanti al tavolo di lavoro, rappresentanti sia del mondo aziendale sia della realtà dei *provider* di servizi informatici *ad hoc*, i quali hanno condiviso le proprie esperienze in ambito nazionale e internazionale, nonché le soluzioni pratiche adottate in termini di articolazione del sistema e gestione della segnalazione e del segnalante.

332 Pansarella M., *Problematiche giuridiche ed organizzative del Whistleblowing nei Modelli 231*, in La responsabilità amministrativa delle società e degli enti, 1/2018.

CAPITOLO 7 di Antonio Bana, Francesca Chiara Bevilacqua e Piero Magri

I rischi e benefici derivanti dall'attività investigativa interna nel procedimento penale delle società

SOMMARIO: 1. Introduzione – 2. Questioni processuali e privilegio legale (attorney-client privilege) – 3. La reazione della società: attività di controllo e report – 4. Bibliografia

1. Introduzione

Il tema di questo tavolo dell'edizione 2018 delle *Corporate Compliance Round Tables* di ASLA nasce da una constatazione pratica comune ai suoi moderatori: è diventata sempre più frequente la richiesta del mondo societario, agli studi legali che si occupano di *compliance* e *white-collar crime*, di supportare l'impresa quando si trovi al cospetto di segnalazioni di potenziali illeciti al suo interno, o comunque di *report* circa presunte forme di devianza dalle *policy* anti-reato aziendali, e desideri verificarle e gestirle in prima persona.

E invero le imprese (e così i componenti dei loro organi di gestione e controllo) non paiono più valutate oggi, da Autorità Giudiziarie e *stakeholders,* unicamente nell'attività di prevenzione degli illeciti, ma anche nella loro risposta ai medesimi.

Dall'apparato organizzativo aziendale e dai suoi attori, difatti, non ci si aspetta solamente uno sforzo preventivo in termini di codici etici e procedure di condotta, di formazione e via dicendo. Ci si attende ora anche, anzitutto, l'approntamento di un adeguato sistema di veicolazione di segnalazioni di possibili illeciti, secondo canoni di riservatezza e di garanzia per il segnalante in buona fede (così come esige il nuovo requisito di idoneità dei modelli organizzativi, introdotto nel D. Lgs. 231/2001 dalla l. 179/2017 in materia di *whistleblowing*). Ci si attende poi un approccio reattivo rispetto all'emersione di simili tematiche, volto cioè ad analizzare senza indugio e con le cautele del caso quanto emerso, a comprenderne i risvolti sia in termini di possibili falle (o elusioni) del proprio sistema anti-reato, sia in termini di potenziali approdi giudiziari, e ad intervenire di conseguenza.

Specialmente in società articolate e di dimensioni consistenti, la buona *compliance* non è dunque la mera (e già assai complessa) declinazione in concreto

dei dettami normativi e prasseologici del settore, ma è anche la capacità del sistema aziendale di reggere agli urti delle potenziali emergenze, arginandone l'effetto, con interventi sia a livello disciplinare, dove necessario, sia sulla stessa organizzazione interna, in particolare nelle aree critiche che si siano scoperte, ad esempio mediante la creazione di nuove procedure, o il rafforzamento di quelle preesistenti, la programmazione di sessioni di formazione aggiuntive specifiche, e così via.

La segnalazione del potenziale illecito, dunque, richiede alle società, in linea con le *best practice* di *compliance* internazionali, una risposta celere ed efficace, il coinvolgimento, o almeno l'informativa, degli attori societari più opportuni (tra cui, a seconda dei casi e delle specifiche organizzative della singola società, l'organo gestorio, il *Compliance Officer*, il *General Counsel*, l'Organismo di Vigilanza ex D. Lgs. 231/2001, l'*Internal Audit* ecc.), l'approfondimento di quanto emerso e l'approntamento delle misure di intervento più adeguate, il tutto nell'attento rispetto delle disposizioni, oltre che corporate e penali, tra le altre di tipo *labour* e *privacy*.

In simili contesti le società, specie se inserite in gruppi multinazionali, svolgono spesso indagini interne particolarmente approfondite circa i fatti segnalati o comunque emersi nell'agire aziendale, molte volte attraverso la funzione *internal audit* interna e la collaborazione del *team* legale e *compliance in-house*, attraverso interviste, ricerche ed analisi di documenti ed email ecc.

Frequentemente, inoltre, sono le funzioni di gruppo, o meglio quelle incardinate presso la società capogruppo, magari straniera, ad attivarsi rispetto a episodi presuntivamente verificatisi esclusivamente nelle controllate italiane. Ciò comporta una delicata gestione a livello di gruppo, in termini anche solo di collaborazione tra *management* e funzioni estere e corrispondenti locali (oltre che dei rispettivi consulenti legali esterni), ma anche - a volte - una certa frizione tra mentalità differenti, specialmente se sui fatti segnalati esista già o paia prossimo un intervento dell'Autorità Penale, e se non sia chiaro se il ruolo della società sia quello di mera vittima del comportamento deviante di qualche scheggia impazzita della sua organizzazione, o sia invece potenzialmente inquadrabile da un'eventuale Procura della Repubblica quale "*co-protagonista*" dell'illecito in ipotesi verificatosi.

Se infatti, soprattutto in alcuni contesti di *common law*, un'approfondita indagine interna è consueta, ed è frequente anche addirittura il *self-reporting* alle Autorità Giudiziarie, nell'auspicio di accedere a programmi di *pre-trial diversion*, nel contesto italiano c'è di norma maggiore cautela. Da un lato c'è sempre il desiderio di non interferire, neppure involontariamente, con le indagini della Magistratura, e anzi di collaborare con le stesse; dall'altro c'è il timore di scoprire problematiche ben più grosse di quelle inizialmente segnalate, magari neppure note alle Autorità. Tutto ciò nella consapevolezza che il sistema processuale penale italiano è imperniato sull'obbligatorietà dell'azione penale, e ha un approccio in termini di *leniency* meno forte o se non altro meno regolamentato di certi corrispondenti stranieri (pur con qualche accento diverso in materia di corruzione, specialmente a seguito delle ultime riforme). Le indagini interne, in

certe circostanze, possono quindi comportare indubbiamente anche dei rischi, oltre che dei benefici, come recita il titolo di questo contributo.

Non per questo le indagini interne non costituiscono un ottimo e, in certi casi, quasi necessario strumento. Si tratta però di uno strumento da maneggiare con particolare cautela: occorre infatti ponderare attentamente, e caso per caso, sia l'effettiva opportunità di attivarlo, sia le modalità di sviluppo in concreto: è tra l'altro proprio in queste situazioni che il legale esterno può fornire un contributo importante. Invero, se in alcune circostanze un normale audit interno, non dissimile dai tanti che le società periodicamente e opportunamente svolgono, è del tutto adeguato, in altri, quelli più delicati e più rischiosi per le società stesse, è senz'altro preferibile quanto meno impiegare il meccanismo che il codice di procedura penale italiano da ormai numerosi anni offre, nel tentativo di avvicinarsi ad una parità delle armi accusa – difesa, vale a dire le cosiddette *investigazioni difensive* (titolo VI *bis* del libro V del c.p.p., v. *infra*), come noto attuabili anche in maniera *preventiva*.

In tutti questi frangenti, in ogni caso, l'esigenza difensiva delle società, che molto rapidamente potrebbero passare da apparenti persone offese dal reato a potenziali responsabili dell'illecito amministrativo dipendente dal reato stesso, o anche solo responsabili civili per tale reato in quanto realizzato da un collaboratore, deve rappresentare un filo rosso da non trascurare. Come si vedrà oltre, tra l'altro, le conseguenze di simili scelte in termini di *attorney-client privilege* sono significative, e la forza del materiale raccolto secondo il rigoroso approccio processual-penalistico in un eventuale sbocco giudiziario è incomparabilmente diversa.

In definitiva, le indagini interne, se opportunamente declinate, possono consentire alle società di identificare problematiche serie, magari prima che giungano a stadi di maggiore gravità, possono consentire di raccogliere preziose evidenze probatorie, utili in ogni sede, da quella disciplinare a quella penale, possono dimostrare l'adeguatezza anche nei momenti critici del sistema di *compliance aziendale*, nonché la diligenza e professionalità degli esponenti societari coinvolti nell'affrontare l'emergenza e superarla, cogliendo l'occasione altresì di migliorare l'organizzazione aziendale.

Non è naturalmente possibile in questa sede trattare diffusamente di tutti gli aspetti evocati né riportare tutti gli interessantissimi spunti ed esperienze emersi nel dialogo con i partecipanti alla tavola rotonda. Ci si concentrerà dunque su alcuni di essi, in particolare quello di natura più strettamente processuale penale, e quello relativo ad uno dei principali attori di queste dinamiche, vale a dire l'Organismo di Vigilanza ex D. Lgs. 231/2001.

2. Questioni processuali e privilegio legale (*attorney-client privilege*)

I rischi e benefici derivanti dall'attività investigativa interna

Tematica di assoluto interesse è quella che attiene alle investigazioni interne societarie, svolte spesso dalla funzione di internal audit nello specifico ambito della prevenzione del rischio reato di cui al D.Lgs.231/ 01.

Sempre più rilevante appare oggigiorno il ruolo dell'informazione e delle notizie di stampa anche nell'ambito dei contesti societari nel momento in cui anche solo a livello mediatico si viene coinvolti in ambito reputazionale, minando potenzialmente l'integrità societaria.

Ecco perché si ritiene indispensabile operare all'interno soprattutto delle grandi organizzazioni aziendali di quei meccanismi di flussi informativi idonei a rilevare le potenziali minacce, i cosiddetti "*campanelli d'allarme*", in modo da poter anticipare in modo concreto potenziali danni in un'ottica di azioni preventive e correttive nei confronti dell'organismo societario.

In questo contesto e a fronte dell'inasprimento sanzionatorio sul versante penalistico dei reati presupposto inseriti nel D.Lgs 231, l'impresa moderna ritiene sempre più necessario elevare il suo grado di tutela verso una *corporate compliance* sempre più qualificata, che possa rientrare a pieno titolo tra le priorità dell'agire nel sistema organizzato aziendale.

Giova sul punto analizzare e confrontarsi con sistemi di prevenzione investendo correttamente in sistemi di risorse dell'attività d'indagine interna.

In questo modo l'Ente potrà comprendere meglio le cause e le modalità operative attraverso le quali la norma è stata violata al fine di implementare le proprie risorse in misure correttive idonee ad evitare che si possano verificare illeciti.

Il presupposto dell'avvio di qualsiasi indagine interna è costituito dall'avvertimento anche di mero sospetto di notizie riguardanti violazioni che andrebbero ad incidere sul sistema di procedure e dei principi cardine del Modello organizzativo aziendale.

La notizia può avere ad oggetto anche condotte che dimostrino sin dall'inizio una loro criticità che deve avere un corretto approccio nel sistema di gestione tra le segnalazioni con il relativo avvio delle più corrette procedure.

Si ricorda che esistono soluzioni IT che offrono la possibilità di impostare indicatori automatici di anomalie anche note come "*red flags*" al verificarsi di determinati eventi.

Da qui nasce tutta una attività di monitoraggio svolta regolarmente dall'ODV e/o dall'*internal audit* unitamente alle segnalazioni interne provenienti dai sistemi di *whistleblowing* e dai differenti sistemi della funzione aziendale IT che possono indicare l'esistenza di fenomeni sospetti.

Da un punto di vista schematico e prima di addentrarci nel merito dell'argomento relativo alla tematica delle investigazioni interne societarie si ritiene opportuno evidenziare gli argomenti più salienti della questione attraverso i seguenti punti di riflessione:

- Ruolo assunto nel sistema dei controlli interni;
- Possibili interazioni tra i controlli interni e l'ODV;
- Attività operative che coinvolgono l'internal audit nel processo investigativo delle violazioni del MOG.

Altri punti di riflessione che si devono tenere conto in una attenta analisi preventiva sono le seguenti attività:

- Le investigazioni interne a seguito della notizia di reato presupposto;
- Le indagini difensive penali ex art.327 bis c.p.p.;
- L'attività investigativa preventiva nelle procedure previste dall'art. 327 bis c.p.p.all' art 391 *nonies* c.p.p. Da questo presupposto si analizzeranno i profili processuali in merito:
  - al ruolo dell'internal audit nel procedimento penale delle società;
  - ai benefici derivanti dall'attività investigativa interna nel procedimento penale delle società;
  - alle analisi dei profili processuali penali che possono riguardare l'operato dell'internal auditor nella particolare cornice del procedimento penale degli enti;
  - alle difficoltà operative connesse all'attività investigativa: i controlli a distanza, lo statuto dei lavoratori e i profili di controllo in materia di protezione dei dati personali.

Sotto il profilo del codice di procedura penale nell'ambito delle operazioni di Polizia Giudiziaria durante la fase delle indagini preliminari possiamo suddividere le seguenti attività:

- **AD INIZIATIVA**: Sommarie informazioni (art.250 c.p.p.), Perquisizioni urgenti (art. 352 c.p.p.), Acquisizione di plichi e corrispondenza (art. 353 c.p.p.), Rilievi urgenti (art. 354 c.p.p.)
- **DELEGATA**: Individuazione di persone e cose (art 361 c.p.p.)
- Interrogatorio indagato libero (art.370 c.p.p.)
- Confronti (art. 370 c.p.p.)
- Sommarie informazioni (art.362 c.p.p.)
- Perquisizioni fuori dei casi urgenti (art. 352 c.p.p.)
- **DI ASSISTENZA**: Notifica atti (art, 148 2 comma c.p.p. e art. 151 c.p.p.), Documentazione atti PM (art. 373 6 comma c.p.p.).

Passando ora ad analizzare brevemente le indagini difensive penali queste sono state introdotte dalla legge 7 dicembre 2000, numero 37 al fine di una corretta esigenza di parità tra accusa e difesa [167].

167 Sul punto si veda l'interessante scritto di A. Jannone "*231 e difesa post factum, tecniche, metodi e framework legale di case management*" dove l'autore ha cura di rilevare l'importanza del "*diritto di difendersi provando ma anche quello del diritto di difendersi cercando*" (in *La resp.ammi. soc. e enti 2010*, (3) pag.43 e ss.)

Interessante rilevare come la difesa seguendo la facoltà ex art. 327- *bis* c.p.p. al 3° comma viene prevista la possibilità di mettere a disposizione nell'indagine difensiva dei propri investigatori privati autorizzati e consulenti tecnici, tra i quali generalmente possono essere menzionati anche i componenti della Funzione di Internal Audit.

Riteniamo opportuno evidenziare alcune linee guida operative sulla regolamentazione delle attività da svolgere al fine di disciplinare correttamente:

- le modalità delle segnalazioni;
- le modalità di trattamento da parte degli organi preposti;
- la corretta gestione di "*crisi*" per la legge 231 (indagini interne e relative comunicazioni);
- le modalità del disciplinare al fine di facilitare e regolamentare i flussi informativi tra gli organi e le funzioni dell'ente potenzialmente coinvolto predisponendo una scaletta di controlli da effettuare.

Tali controlli a nostro modo di vedere dovranno svilupparsi su:

- coloro che ricevono o possono ricevere le segnalazioni;
- natura e ambito delle segnalazioni;
- coloro che hanno la responsabilità di "gestire" le segnalazioni e la loro fondatezza;
- coloro che sono interessati dalle informazioni segnalate;
- coloro che hanno la responsabilità di prendere gli opportuni provvedimenti.

Si giunge in questo modo a considerare il fatto che le indagini difensive sembrano essere un valido strumento per affrontare e gestire eventuali situazioni emergenziali che potrebbero coinvolgere l'Ente che pur avendo adeguatamente ottemperato agli obblighi di cui al D. Lgs.231/01 voglia ottemperare a tutte le ulteriori ed eventuali criticità.

Questo tipo di attività, a differenza di quelle tipiche svolte dall'ODV e dall'internal audit, porterebbe a tutelare maggiormente le acquisizioni di dichiarazioni scritte, verbali, interviste e richieste di documenti che una volta svolte dal difensore e da suoi collaboratori opportunamente delegati sarebbero sottoposti ad una particolare e specifica tutela giudiziaria caratterizzata dalle disposizioni in materia di segreto professionale ex art 200 c.p.p.

In questo modo, infatti, tutte quelle garanzie di libertà del difensore stabilite anche dalla norma di cui all'art.103 c.p.p. garantirebbero la possibilità di "*non produrre in giudizio i verbali contenenti dichiarazioni sfavorevoli al cliente*" (si veda Cass Pen S.U., 27 giugno 2016, Schera, in Dir. e Giustizia, 2016 p.44).

Infatti, in tema di c.d. segreto professionale (*attorney-client privilege*) ai sensi dell'art. 200 c.p.p. gli avvocati, gli investigatori e i consulenti tecnici non possono essere obbligati a deporre su quanto hanno potuto apprendere per ragione della propria professione, salvi i casi in cui hanno l'obbligo di riferirne all' autorità giudiziaria. Spetterà poi al giudice valutare l'eventuale fondatezza in merito alla richiesta di esimersi dal deporre o meno.

Da ultimo ricordiamo che vi sono ulteriori garanzie di libertà che possono e devono essere assicurate in materia di ispezioni, perquisizioni, sequestri e intercettazioni (sul punto si veda l'ampio lavoro svolto da C. Coratella, *Il D.Lgs 231/2001 e la nuova frontiera delle indagini difensive* in *La responsabilità amministrativa delle società e degli enti*, pag.145 e ss).

Ricordiamo inoltre che le indagini difensive assumono un ruolo fondamentale con riferimento all'applicazione di misure cautelari personali di soggetti apicali o subordinati dell'Ente, di conseguenza poiché l'art 292 c.p.p. stabilisce che l'ordinanza che dispone la misura cautelare deve rispettare, a pena di nullità riscontrabile anche d'ufficio, alcuni requisiti contenutistici, questa risulta essere nulla se non contiene la valutazione degli elementi a carico e a favore dell'imputato, di cui agli artt. 358 e 327 *bis* c.p.p.

Il legislatore ha riconosciuto, infatti, al difensore e a tutti i soggetti inclusi nell'art. 391 *bis* c.p.p., importanti garanzie al fine di tutelare l'attività d'indagine.

In questo caso i soggetti inclusi non hanno l'obbligo di denuncia relativamente ai reati dei quali abbiamo avuto notizia nel corso della loro attività investigativa e non possono essere assunti come testimoni nel caso in cui nel medesimo procedimento abbiano acquisito la documentazione in merito alle informazioni assunte ai sensi dell'art 391 ter c.p.p.

Consideriamo, infine, che in sede di investigazioni interne all'Ente, questo strumento consente al difensore di "*rivedere*" l'iter degli eventi potenzialmente pregiudizievoli, mantenendo le fondamentali garanzie legate all'esercizio del diritto di difesa.

3. La reazione della società: attività di controllo e report

Il sistema dei controlli interni può assumere connotazioni differenti a seconda delle caratteristiche della società. Gli organi principali deputati al controllo sono l'*Internal auditing* (che non sempre è presente e spesso, nelle multinazionali, è collocato nella capogruppo straniera), il *compliance officer* o la struttura di *Ethics & Compliance*, l'Organismo di Vigilanza e il Collegio Sindacale.

Quando vengono trasmesse segnalazioni di fatti che possono costituire ipotesi di reato è opportuno che vi sia una interazione tra tutti questi organi, se presenti, pur nel rispetto della riservatezza della identità del segnalante la cui tutela è prevista espressamente anche dalla normativa in materia di *whistleblowing*.

In questa prospettiva si ritiene sempre più opportuno che ogni società si doti di apposite procedure interne per la disciplina e la gestione delle segnalazioni di illeciti.

In particolare, l'Organismo di Vigilanza ha un ruolo fondamentale nell'attività di gestione e controllo delle segnalazioni. Tuttavia, nelle ipotesi in cui sia presente anche una struttura di *Internal auditing*, è evidente che l'ODV si rivolgerà per lo più a quest'ultima perché svolga le necessarie indagini interne, chiedendo però di essere informato tempestivamente dell'esito delle stesse.

Purtroppo può capitare che l'ODV non venga informato di tutti gli illeciti denunciati direttamente all'*Internal auditing* o ad altra struttura aziendale e

ciò potrebbe costituire un vulnus nel corretto sistema dei controlli interni che potrebbe ripercuotersi anche sulla tenuta del Modello Organizzativo.

Vero anche che non tutti gli illeciti devono essere segnalati all'ODV, ma solo quelli che riguardano le ipotesi di reato presupposto inseriti nel D.Lgs. 231/2001 o, più in generale, le violazioni del Modello di Organizzazione, Gestione e Controllo. Ad esempio ipotesi di molestie o di truffa a danno dell'ente potrebbero non essere comunicate all'ODV o, se comunicate, dovrebbero esere demandate alle strutture aziendali competenti.

A ogni modo, una volta recepita la relazione dell'*Internal auditing*, l'ODV deve discutere al proprio interno focalizzandosi su due aspetti fondamentali. In primo luogo l'ODV deve valutare se le procedure interne siano state violate e, di conseguenza, se le stesse siano realmente efficaci a prevenire la commissione di illeciti.

Tuttavia, qualora non sia stata adottata alcuna procedura finalizzata a evitare o prevenire la commissione dell'illecito, compito dell'ODV sarà naturalmente quello di segnalare la lacuna al CDA e di verificarne l'adozione.

Nella prima ipotesi, ovvero qualora la procedura sia stata implementata ma si sia rivelata insufficiente, l'ODV dovrebbe proporre modifiche o integrazioni volte a migliorare e rendere più efficiente il sistema di controllo interno e il Modello Organizzativo in punto di segregabilità e tracciabilità dei processi.

In secondo luogo, una attenta istruttoria gestita e verbalizzata dall'ODV potrebbe essere certamente utile non solo ai fini difensivi per la tutela dell'ente, anche eventualmente sotto il profilo dell'ottenimento di circostanze attenuanti nel processo penale a carico dell'ente, ma anche sotto il profilo della *reputation* dell'ente medesimo.

Va da sé che, qualora non sia presente all'interno dell'ente una struttura di *Internal auditing*, l'ODV avrà un ruolo più pregnante ma anche più complesso. Spesso dovrà quindi farsi assistere per l'attività investigativa da consulenti o avvocati esterni, attingendo dal proprio budget. L'ODV dovrebbe agire in piena autonomia, ma è evidente che il raccordo con la funzione legale o di *Compliance* della società potrebbe essere più che opportuno.

Occorre distinguere poi se la segnalazione si riferisca a (1) fatti illeciti ma di dubbia rilevanza penale o (2) atti illeciti che hanno già dato origine ad un procedimento penale. In quest'ultimo caso bisogna distinguere due ulteriori ipotesi, ovvero se (2a) il procedimento sia a carico solo di persone fisiche riconducibili all'ente (apicali o sottoposti) o se (2b) sia contestato qualche illecito ex D. Lgs. 231/2001 direttamente all'ente, magari con applicazione di misure cautelari interdittive.

Nel primo caso la presenza di un penalista nell'ODV o comunque il supporto dello stesso potrà essere decisivo. L'ODV deve comunque poter discutere di fatti che di per sé potrebbero non costituire una violazione 231, limitandosi ad evidenziare in questo caso l'inconsistenza o debolezza del Modello di Organizzazione e, di conseguenza, l'esigenza di un suo aggiornamento. Nella

medesima prospettiva anche una violazione di un principio del Codice Etico potrebbe, ad esempio, non costituire di per sé una violazione 231, ma potrebbe richiedere a ragione una attività di controllo da parte dell'ODV.

Qualora invece si tratti di un procedimento penale già instaurato, l'ODV dovrà coordinarsi il più possibile con i difensori nominati, richiedendo informazioni, report, aggiornamenti, nonché, eventualmente, un approfondimento sugli atti di indagine del procedimento penale.

È fondamentale però il rispetto dei ruoli: l'ODV non deve sostituirsi al difensore, ma limitarsi a comprendere se il reato sia stato valutato nel Modello e nella analisi dei rischi, se siano state adottate procedure idonee a prevenire la commissione dell'illecito contestato, se il Modello debba essere aggiornato al fine di rendere i principi di comportamento in esso descritti più stringenti e severi. Al tempo stesso, l'ODV non deve neppure essere organo di polizia: non ha obbligo di denuncia all'Autorità Giudiziaria, ma solo di segnalazione al CDA a cui poi spetterà prendere le decisioni più opportune in termini disciplinari o difensivi.

Certamente l'ODV può reagire a segnalazione di illeciti, intensificando le attività di verifica, anche intervistando le funzioni aziendali strategiche, ma dovrà sempre rispettare il proprio ruolo di organo posto a supporto e servizio dell'ente, quale organo delle procedure e non come facente funzioni dell'audit.

Nella prospettiva che l'ente debba affrontare un processo penale la gestione delle informazioni e dei documenti per l'Autorità Giudiziaria va governata con intelligenza e con un approccio strategico. Ad esempio l'ODV deve sapere che i verbali delle sue riunioni o le relazioni periodiche per l'organo amministrativo - di per sé riservati - potrebbero essere sequestrati o richiesti dall'Autorità Giudiziaria. Di conseguenza il contenuto dei verbali può essere più o meno dettagliato ma non può certamente costituire una autodenuncia per l'ente.

Ad esempio in casi di violazioni 231 in materia di sicurezza e ambiente non è raro imbattersi in report interni molto dettagliati, predisposti da funzioni interne (es. RSPP, EHS) su richiesta della casa madre, che hanno il legittimo scopo di approfondire le cause e valutare possibili azioni correttive. Tuttavia, occorre considerare che tali strumenti possono costituire la base per l'attività di indagine dell'Autorità Giudiziaria o - ed è capitato - anche per la pronuncia di una sentenza di condanna.

Qualora vi sia una indagine per fatti gravi è poi possibile che lo stesso Presidente ODV o gli altri componenti siano sentiti a sommarie informazioni per verificare la consapevolezza dei fatti e indagare come l'Organo abbia adempiuto ai propri compiti di vigilanza. Il tema è quello dell'efficacia del Modello che viene valutata anche attraverso l'analisi dell'adeguatezza dell'azione dell'ODV.

Altre volte invece l'attività dell'ODV rimane sullo sfondo dell'indagine penale, le Procure non acquisiscono e non valutano l'adeguatezza dei Modelli Organizzativi e si limitano a contestare il reato presupposto all'ente in una sorta di automatismo, come se ogni reato presupposto comporti in automatico la responsabilità dell'ente.

In questi casi spetterà al difensore dell'ente rapportarsi con l'ODV per gestire al meglio le informazioni da fornire all'Autorità Giudiziaria. Ad esempio, in materia di sicurezza e ambiente, si sta sviluppando sempre più la prassi che nei documenti che l'Organo di controllo richiede all'azienda a seguito di un infortunio vi sia anche il Modello Organizzativo.

In definitiva, si ritiene sia molto importante da una parte documentare tutte le verifiche che vengono effettuate internamente, ricostruendo quanto accaduto e conservando traccia delle motivazioni delle decisioni assunte, dall'altra regolamentare tempistiche, modalità e gestione delle segnalazioni ricevute (anche sotto il profilo informatico) e dei rapporti con gli organi esterni.

In questa prospettiva, le procedure dì *whistleblowing* e di ispezione sono decisive per il futuro dell'attività dell'ODV e dovranno individuare i destinatari delle segnalazioni e l'organo responsabile della loro gestione, descrivere l'oggetto delle segnalazioni, nonché identificare i soggetti titolati ad adottare gli opportuni provvedimenti disciplinari o a definire e attuare le necessarie azioni correttive.

4. Bibliografia

ASTROLOGO A. - SGUBBI F., Art. 5. *Responsabilità dell'ente*, in *La responsabilità amministrativa delle società e degli enti*. D.Lgs. 8 giugno 2001, n. 231, diretto da M. LEVlS - A. PERlNI, Bologna, 2014, p. 145 e ss.

BARTOLI R., *Le sezioni unite prendono coscienza del nuovo paradigma punitivo del «sistema 231».* In Soc., 2015, (2), p. 215 e ss.

CENTONZE F., *La normalità dei disastri tecnologici: il problema del congedo dal diritto penale*, Milano, 2004.

CENTONZE F., *Controlli societari e responsabilità penale*, Milano, 2009.

CENTONZE F., *Public Private Partnership and Agency ProbIems: The Use of Incentives in Strategies to Combat Corruption*, in AA.VV., *Preventing Corporate Corruption. The Anti-Bribery Compliance Model* a cura di F. CENTONZE - G. FORTl- S. MANACORDA, Heidelberg, 2014, p. 43 e ss.

CENTONZE F. - MANTOVANI M., *Dieci proposte per una riforma del dgs. n. 231/2001*, in AA.VV., *La responsabilità "penale" degIi enti. Dieci proposte di riforma*, a cura di F. CENTONZE - M. MANTOVANI, Bologna, 2016, p. 283 e ss.

CERESA-GASTAlDO M., *Il "processo alle società"*, nel d.lgs. 8 giugno 2001, n. 231, Torino, 2003.

CERESA-GASTALDO M., *Processo penale ed accertamento della responsabilità amministrativa degli enti: una innaturale ibridazione*, in Cass. pen, 2009, (5), p. 2232 e ss.

EPIDENDIO T. E., *Il Modello organizzativo 231 con efficacia esimente*, in *La responsabilità amministrativa delle società e degli enti*, 2010, (4), p. 157 e ss.

FIDELBO G., *L'accertamento dell'idoneità del Modello organizzativo in sede giudiziale*, in AA.VV., *La responsabilità da reato degIi enti collettivi: a dieci anni dal d.lgs. 231/2001*, a cura di V. MONGlLLO - A. M. STILE - G. STILE, Napoli, 2013, p. 174 e ss.

FORTUNATO S., *Il "Sistema dei Controlli" e la gestione dei rischi (a quindici anni dal t.u.f.)*, in Soc., 2015, (2-3), p. 249 e ss.

JANNONE A., *231 e difesa post delictum: tecniche, metodi e framework legale di case management*, in *La resp.amm. soc. e enti*, 2010, (3), p. 43 e ss.

JANNONE A., *Corruzione, frodi socieli e frodi aziendali*, Milano, 2016.

JANNONE A., *Il whistleblowing e la policy antifrode e anticorruzione: il quadro normativo e le soluzioni operative*, in *La resp. amm. soc. e enti*, 2010, (3), p. 219 e ss.

MANCUSO E. M., *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, in AA.VV., *La responsabilità "penale" degli enti. Dieci proposte di riforma*, a cura di F. CENTONZE - M. MANTOVANI, Bologna, 2016, p. 217 e ss.

MANCUSO E. M., *L'acquisizione di contenuti e-mail*, in AA.VV., *Le indagini atipiche*, a cura di A. SCALFATI, Torino, 2014, p. 53 e ss.

MARINUCCI G., *«Societas puniri potest»: uno sguardo sui fenomeni e sulle discipline contemporanee*, in Riv. It. dir. proc. pen., 2002, (4), p. 1193 e ss.

MARINUCCI G., *La responsabilità penale delle persone giuridiche. Uno schizzo dogmatico*, in Riv. It. dir. proc. pen., 2002, (4), p. 425 e ss.

MARlNUCCI G. - ROMANO M., *Tecniche normative nella repressione penale degli abusi di amministratori di società per azioni*, in AA.VV., *Il diritto penale delle società commerciali*, a cura di P. NUVOLONE, Milano, 1971, p. 98 e ss.

MUCCIARELLI F., *Una progettata modifica al d.lgs n.231/2001: la certificazione del modello come cause di esclusione della responsabilità*, in Soc; (10), p. 1247 e ss.

SUTHERLAND E. H., *White-Collar Crine*, New York, 1949.

TIEDEMANN K, *La responsabilità penale delle persone giuridiche nel diritto comparato*, in Riv. It. dir. proc. pen., 1995, (3), p. 610 e ss.

VARRASO G., *Il procedimento degli illeciti amministrativi dipendenti da reato*, in *Trattato di procedura penale*, diretto da G. UBERTIS - G.P. VOENA, vol. XLVII, Milano, 2012.

CAPITOLO 8 di Eva Cruellas, Eugenia Gambarara e Irene Picciano

Le nuove Linee Guida sulla compliance antitrust

SOMMARIO: 1. Introduzione – 2. Contenuto ed idoneità del programma di compliance antitrust – 3. La richiesta di valutazione del programma di compliance antitrust ai fini dell'eventuale riconoscimento dell'attenuante: adeguatezza ed effettiva applicazione del programma – 4. Il trattamento premiale dei programmi di compliance antitrust – 5. Recente case-law dell'AGCM sulla valutazione dei programmi di compliance antitrust

1. Introduzione

In data 25 settembre 2018 l'Autorità Garante della Concorrenza e del Mercato (AGCM) ha adottato le nuove Linee Guida sulla *compliance antitrust* [167], che forniscono un significativo orientamento alle imprese per: (i) la definizione del contenuto dei programmi di compliance; (ii) le modalità di presentazione della richiesta di valutazione del programma ai fini del riconoscimento dell'eventuale attenuante da parte dell'Autorità; e (iii) i criteri che l'Autorità intende adottare in tale valutazione ai fini del riconoscimento dell'attenuante.

Le nuove Linee Guida sono state adottate a seguito del parziale accoglimento delle osservazioni pervenute ad esito della consultazione pubblica avviata nell'aprile 2018 sulla bozza di dette Linee Guida, e si innestano nel sistema delle Linee Guida del 2014 sui criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della Legge n. 287/90 [168], in cui l'AGCM aveva incluso l'adozione e il rispetto di uno specifico programma di *compliance*, adeguato e in linea con le *best practice* europee e nazionali [169], tra le circostanze attenuanti che possono ridurre l'importo di una sanzione.

167 Disponibili al seguente link: https://www.agcm.it/dotcmsdoc/linee-guida-compliance/linee_guida_compliance_antitrust.pdf.

168 Delibera AGCM 22 ottobre 2014, n.25152 - Linee Guida sulla modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della Legge n. 287/90. Disponibili al seguente link: https://www.agcm.it/competenze/tutela-della-concorrenza/dettaglio?id=cbb9e335-a9ca-4efb-97ac-71dbd831c491&parent=Normativa&parentUrl=/competenze/tutela-della-concorrenza/normativa.

169 Paragrafo 23 delle Linee Guida sulla modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della Legge n. 287/90. L'AGCM ha inoltre specificato che "… *La mera esistenza di un programma di compliance non sarà considerata di per sé una circostanza attenuante, in assenza della dimostrazione di un effettivo e concreto impegno al rispetto di quanto previsto nello stesso programma (attraverso, ad esempio, un pieno coinvolgimento del management, l'identificazione del personale responsabile del programma, l'identificazione e valutazione dei rischi sulla base del settore di attività e del contesto operativo, l'organizzazione di attività di training*

I programmi di *compliance antitrust* sono sviluppati dalle imprese con lo scopo di assicurare il rispetto della normativa in materia di concorrenza e di prevenire eventuali illeciti, informando e rendendo consapevole il personale delle conseguenze derivanti dalle violazioni di tale normativa. Oltre all'Italia, anche le Autorità nazionali garanti della concorrenza di numerosi altri Stati Membri hanno fornito indicazioni in materia di compliance antitrust. Nel 2010 l'allora *Office of Fair Trading* (OFT) del Regno Unito, oggi divenuto *Competition and Markets Authority*, aveva redatto il documento "*Drivers of Compliance and Non-compliance with Competition Law*" [170], che già prevedeva che le imprese potessero godere di una riduzione della sanzione in presenza di un programma di compliance conforme alle linee guida. Nel 2012 l'*Autorité de la Concurrance* francese aveva pubblicato un documento-quadro [171] indicante le condizioni alle quali l'adozione di un programma di *compliance antitrust* poteva essere considerato ai fini della *leniency*/immunità parziale o come attenuante negli illeciti in cui la *leniency* non trovava applicazione [172]. A livello europeo, invece, la Commissione non prevede alcuna riduzione di sanzione in caso di adozione e finanche implementazione di un programma di *compliance* [173].

Di seguito verranno esaminati: il contenuto tipico di un programma di *compliance antitrus*t, necessario a renderlo idoneo a svolgere la sua funzione di prevenzione degli illeciti; la presentazione della richiesta di valutazione del programma ai fini dell'eventuale riconoscimento dell'attenuante; i trattamenti premiali eventualmente concessi, che variano in base al momento in cui viene adottato e implementato il programma di *compliance antitrust*.

2. Contenuto e idoneità del programma di compliance antitrust

Ai sensi delle Linee Guida, ai fini del riconoscimento di un programma di compliance per ottenere la riduzione della sanzione, è centrale la sua idoneità a svolgere una funzione di prevenzione degli illeciti. Pertanto, il programma dovrà tenere in considerazione le caratteristiche dell'impresa, ossia la sua natura,

adeguate alle dimensioni economiche dell'impresa, la previsione di incentivi per il rispetto del programma nonché di disincentivi per il mancato rispetto dello stesso, l'implementazione di sistemi di monitoraggio e auditing)…".

170 Disponibile al seguente link: https://www.gov.uk/government/publications/business-drivers-of-compliance-and-non-compliance-with-competition-law.

171 *Document-cadre du 10 février 2012 sur les programmes de conformité aux règles de concurrence*, disponibile al seguente link: *http://www.autoritedelaconcurrence.fr/doc/document_cadre_conformite_10_fevrier_2012.pdf.*

172 I programmi di *leniency* (clemenza) hanno la finalità di indurre le imprese partecipanti a un cartello a collaborare in maniera attiva e determinante all'individuazione delle condotte illecite, in cambio della non applicazione, o sostanziale riduzione, delle sanzioni. Tali programmi sono qualificabili come sistemi premiali che mirano a destabilizzare i cartelli minando la fiducia reciproca tra coloro che vi partecipano. Trattandosi di un sistema premiale, l'efficacia dei programmi di clemenza è legata alla deterrenza delle sanzioni e alla effettività della loro applicazione, che il *leniency applicant* sarà propenso a evitare o attenuare attraverso una concreta attività di collaborazione.

173 Si veda, *ex multis*, CGUE 18.07.2013, causa C-501/11P, *Schindler Holding Ltd e altri contro Commissione europea*, punti 113-114 e 140-144. Si veda altresì la sentenza del TAR Lazio, causa n. 9048, pubblicata il 28.07.2017: "*… il riconoscimento delle circostanze attenuanti, sia nell'an che nel quantum, è il risultato dell'esercizio di un'ampia discrezionalità da parte di AGCM (ex multis, Cons. Stato, Sez. VI, 3 giugno 2014, n. 2838; id., 9 febbraio 2011, n. 896) la quale, peraltro, segue un orientamento più indulgente di quello della Commissione europea, secondo cui l'esistenza di un programma di compliance non funge da esimente, posto che, laddove vi sia stata una violazione della normativa antitrust, questa è la prova stessa dell'inefficacia di un siffatto programma…*".

la sua dimensione e la sua posizione di mercato, ed il contesto di mercato in cui essa opera. Tra gli elementi tipici qualificanti di un programma di compliance vi sono:

- il riconoscimento del valore della concorrenza (ad esempio, in un codice etico o di condotta aziendale) come parte integrante della cultura e della politica dell'impresa;
- l'identificazione e la valutazione del rischio antitrust specifico dell'impresa, ossia la concreta analisi del rischio di porre in essere condotte anticompetitive che l'impresa si trova a fronteggiare. Una tale analisi permette infatti la corretta individuazione delle priorità di intervento, identificando le attività di prevenzione più adeguate e massimizzando in tal modo l'impiego delle risorse utilizzate per la realizzazione del programma;
- attività di formazione e *know-how* interno, al fine di diffondere la conoscenza delle tematiche antitrust tra i dipendenti e i funzionari, rendendoli consapevoli dei rischi antitrust legati alla loro attività;
- la definizione di processi gestionali idonei a ridurre il rischio che vengano poste in essere condotte in violazione della normativa a tutela della concorrenza come, ad esempio, modelli di *reporting* interno che consentano al personale di segnalare rapidamente problematiche antitrust ed ottenere chiarimenti su specifiche questioni, fino a consentire la denuncia, anche in forma anonima, di possibili violazioni;
- un sistema di misure disciplinari nel caso di violazione delle norme in materia di concorrenza da parte dei dipendenti e funzionari ed un sistema di incentivi al rispetto delle procedure e dei processi di gestione del rischio antitrust come individuati dal programma;
- un monitoraggio periodico del programma ed il suo eventuale aggiornamento, che tenga conto delle evoluzioni dell'attività dell'impresa e del contesto di mercato in cui essa opera, nonché dello stato dell'arte giurisprudenziale in materia.

3. La richiesta di valutazione del programma di compliance antitrust ai fini dell'eventuale riconoscimento dell'attenuante: adeguatezza ed effettiva applicazione del programma

L'adozione di un programma di *compliance* non è di per sé sufficiente per conseguire il riconoscimento di un'attenuante. Le Linee Guida specificano che l'applicazione di un trattamento premiale richiede che l'impresa dia prova dell'adeguatezza del programma e della sua effettiva applicazione. In particolare, un'impresa coinvolta in un procedimento istruttorio che intenda beneficiare di un'attenuante per il proprio programma di *compliance* dovrà presentare presso gli Uffici dell'AGCM un'apposita richiesta, accompagnata da una relazione illustrativa che spieghi i motivi per cui il programma possa considerarsi adeguato e le iniziative concrete realizzate dall'impresa per la sua efficace applicazione, allegando altresì la documentazione a riprova dell'effettiva attuazione. Inoltre, per i fini dell'attenuante, sono considerati solo i programmi adottati, attuati

e trasmessi dalle imprese interessate entro sei mesi dalla notifica dell'apertura dell'istruttoria. Nel caso in cui il programma di compliance sia stato modificato dopo l'avvio di un procedimento, l'impresa dovrà specificare, tra l'altro, i miglioramenti apportati e le ragioni della loro introduzione, nonché le iniziative adottate per l'esecuzione del nuovo programma [174].

Nell'ambito di procedimenti *antitrust* che coinvolgono sia un'impresa controllata che la controllante, il programma di *compliance* dovrà essere adottato e implementato a livello di gruppo per soddisfare il requisito di adeguatezza. Ai fini della valutazione dell'attenuante, verrà esaminato il programma adottato e attuato sia dall'impresa controllante, sia dalle controllate coinvolte. L'adozione di un programma di *compliance* da parte della capogruppo non sarà considerato di per sé un elemento sufficiente ad escluderne la responsabilità per la condotta anticoncorrenziale della controllata [175].

4. Il trattamento premiale dei programmi di compliance antitrust

L'attenuante riconosciuta alle imprese varia in base al momento in cui viene adottato il programma di *compliance*. Se questo viene adottato dopo l'avvio del procedimento istruttorio, è prevista la possibilità di una riduzione dell'importo base della sanzione fino al 5%. Per ottenere l'attenuante, è in ogni caso necessario che il programma venga attuato in tempo utile per essere valutato dall'AGCM nel corso del procedimento [176]. Per i programmi di *compliance* adottati prima dell'avvio del procedimento istruttorio, invece, l'ammontare della riduzione dipende dalla loro adeguatezza ed efficacia. In particolare:

- i programmi di *compliance* adeguati e che hanno funzionato in maniera efficace, consentendo la tempestiva scoperta e interruzione dell'illecito prima della notifica dell'avvio del procedimento istruttorio, permettono di beneficiare di una riduzione fino al 15% della sanzione. Nel caso in cui sia applicabile l'istituto della clemenza, l'attenuante del 15% può essere riconosciuta solo laddove l'impresa presenti la domanda di clemenza prima che l'AGCM abbia condotto ispezioni riguardanti la medesima ipotesi collusiva;
- i programmi di *compliance* che non hanno funzionato in maniera del tutto efficace, non consentendo la tempestiva scoperta e interruzione dell'illecito prima dell'avvio del procedimento dell'AGCM, ma che, tuttavia, non sono manifestamente inadeguati, possono permettere all'impresa di beneficiare di un trattamento premiale fino al 10% della sanzione, a condizione che essa integri adeguatamente il programma e inizi a darvi

174 Paragrafo 26 delle Linee Guida: "… *In questo caso, infatti, oggetto di apprezzamento da parte dell'Autorità potranno essere soprattutto i miglioramenti che l'impresa ha apportato a un programma che essa stessa ha ritenuto di modificare e l'impegno dimostrato nel dare esecuzione alle nuove misure di prevenzione di comportamenti anticompetitivi*…".

175 Paragrafi 43 e 44 delle Linee Guida.

176 Paragrafo 29 delle Linee Guida: "… *La quantificazione dell'attenuante è commisurata alla completezza e alla qualità del programma presentato (adeguatezza), ma anche alla maggiore o minore possibilità da parte dell'Autorità di verificare la fattiva, concreta e continuativa implementazione e attuazione del programma*…".

attuazione entro sei mesi dalla notifica dell'apertura dell'istruttoria [177]. L'ammontare dell'attenuante sarà valutato tenendo in considerazione la completezza del programma esistente al momento dell'avvio del procedimento istruttorio e delle modifiche attuate dall'impresa;

- i programmi di *compliance* manifestamente inadeguati [178], infine, non permettono di beneficiare di trattamenti premiali. Tuttavia, è previsto che, nel caso in cui l'impresa presenti modifiche sostanziali al programma entro sei mesi dalla notifica dell'apertura dell'istruttoria, essa possa beneficiare di una potenziale riduzione della sanzione fino al 5%.

È altresì prevista un'attenuante non superiore al 5% della sanzione per le imprese recidive [179], nel caso in cui esse siano già dotate di un programma di *compliance* prima della notifica dell'avvio dell'istruttoria e abbiano presentato delle modifiche allo stesso dopo l'avvio del procedimento. Nessuna attenuante sarà concessa a un'impresa recidiva che abbia già beneficiato di una riduzione della sanzione, a esito di una precedente istruttoria, per aver adottato un programma di *compliance* [180].

In generale, l'AGCM non considererà l'esistenza di un programma di *compliance* quale circostanza aggravante, salvo ipotesi eccezionali. Ad esempio, potrà sussistere un'aggravante qualora il programma sia stato strumentale all'occultamento dell'infrazione o abbia ostacolato l'attività istruttoria dell'AGCM [181].

L'AGCM applicherà le Linee Guida sulla compliance antitrust nei procedimenti istruttori avviati successivamente alla loro pubblicazione [182].

177 Paragrafo 37 delle Linee Guida: "… *È onere dell'impresa dimostrare che: i) il programma da essa adottato era ben calibrato nella prevenzione dei rischi di commissione di attività anti-competitive e che l'attuazione del programma è stata curata con serietà e costanza per tutta la sua durata, benché non abbia in concreto impedito il verificarsi di una condotta illecita e la sua cessazione/denuncia tempestiva; ii) le modifiche al programma proposte dall'impresa sono idonee a colmare le lacune che avevano impedito l'efficace funzionamento del programma di compliance originario*…".

178 La manifesta inadeguatezza di un programma di *compliance* può risultare da gravi carenze dei contenuti, dall'assenza di elementi probatori circa l'effettiva attuazione, o il coinvolgimento dei vertici del *management* aziendale nella condotta illecita. Inoltre, un programma è sempre considerato manifestatamente inadeguato se, nei casi in cui sia applicabile l'istituto della clemenza, l'impresa o l'associazione di imprese non abbia posto fine all'illecito e non abbia presentato domanda di clemenza ai sensi dell'articolo 15, comma 2- della Legge n. 287/1990.

179 Per impresa recidiva si intende un'impresa che "… *abbia precedentemente commesso una o più infrazioni simili o della stessa tipologia, in relazione all'oggetto o agli effetti, accertata/e dall'Autorità o dalla Commissione Europea, nei cinque anni precedenti l'inizio dell'infrazione oggetto di istruttoria*…". Si vedano il paragrafo 22 delle Linee Guida sulla modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della Legge n. 287/90.

180 Paragrafi 40 e 41 delle Linee Guida. Al contrario, ciò potrebbe costituire una circostanza aggravante; si veda il paragrafo 46 delle Linee Guida.

181 Tali ipotesi potrebbero costituire un'aggravante secondo quanto previsto dal paragrafo 21 delle Linee Guida sulla modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della Legge n. 287/90.

182 Le Linee Guida sulla *compliance antitrust* sono state pubblicate nel Bollettino settimanale dell'AGCM n. 37/2018 del 08.10.2018.

5. Recente *case-law* dell'AGCM sulla valutazione dei programmi di compliance antitrust

Recentemente, l'AGCM ha riconosciuto delle attenuanti sulla base dell'adozione di specifici programmi di *compliance antitrust*.

Con provvedimento del 20 dicembre 2018 [183], l'AGCM ha accertato la sussistenza di un'intesa, in violazione dell'articolo 101 del Trattato sul Funzionamento dell'Unione europea (TFUE), tra le principali captive banks e i relativi gruppi automobilistici operanti in Italia nel settore della vendita di autoveicoli mediante prodotti finanziari, nonché le relative associazioni di categoria. In particolare, l'AGCM ha accertato che le società *Banca PSA Italia S.p.A.*, *Banque PSA Finance S.A.*, *Santander Consumer Bank S.p.A.*, *BMW Bank GmbH, BMW AG*, *Daimler AG, Merceds Benz Financial Services Italia S.p.A.*, *FCA Bank S.p.A.*, *FCA Italy S.p.A.*, *CA Consumer Finance S.A.*, *FCE Bank Plc.*, *Ford Motor Company*, *General Motor Financial Italia S.p.A.*, *General Motors Company*, *RCI Banque S.A.*, *Renault S.A.*, *Toyota Financial Services Plc.*, *Toyota Motor Corporation*, *Volkswagen Bank GmbH*, *Volkswagen AG.* (c.d. *captive banks*), nonché le associazioni di categoria *Assofin* e *Assilea*, avevano posto in essere un'intesa volta al coordinamento delle strategie commerciali attraverso lo scambio di informazioni sensibili relative a quantità e prezzi, anche attuali e futuri.

L'istruttoria era stata avviata a seguito della presentazione di una domanda di clemenza da parte delle società *Daimler AG e Mercedes Benz Financial Services Italia S.p.A.*, a cui l'AGCM ha riconosciuto il beneficio dell'immunità totale dalla sanzione. Alle altre parti coinvolte, l'AGCM ha imposto una sanzione per un totale complessivo di circa 678 milioni di euro.

Nell'infliggere la sanzione, l'AGCM ha tenuto conto dell'adozione, da parte di alcune società, (segnatamente: *BMW Bank*, anche per *BMW AG*, *FCE Bank*, *TFS*, *TMC*, *Volkswagen Bank*, *FCA Bank*, *Banca PSA Italia*), nonché dall'associazione *Assilea* di specifici programmi di *compliance antitrust*. In particolare, risultava che tali parti avessero posto in essere programmi di *compliance* già in periodi antecedenti all'avvio dell'istruttoria i quali, erano stati ulteriormente integrati a seguito dell'avvio del procedimento, prima dell'invio della CRI. Tutti i programmi esaminati appaiono strutturati con un ampio programma di formazione e informazione dei dipendenti, oltre che dei vertici aziendali. Inoltre, in caso di violazione delle indicazioni prescritte dai programmi esaminati, gli stessi prevedono altresì un impianto sanzionatorio che appare possedere una valenza dissuasiva. Pertanto, l'AGCM ha riconosciuto loro una circostanza attenuante nella misura del 10%.

Nella medesima data [184], l'AGCM ha altresì accertato la sussistenza di condotte anticoncorrenziali nel mercato della vendita di energia elettrica, poste in essere da Enel S.p.a., Enel Energia S.p.a. e Servizio Elettrico Nazionale S.p.a..

183 AGCM 20.12.2018, I811 - FINANZIAMENTI AUTO, Provvedimento n. 27497. Il provvedimento è disponibile al seguente link: http://bit.ly/30pE4C3.

184 AGCM 20.12.2018, A511 - ENEL/CONDOTTE ANTICONCORRENZIALI NEL MERCATO DELLA VENDITA DI ENERGIA ELETTRICA, Provvedimento n. 27494. Il testo del provvedimento è disponibile al seguente link; http://bit.ly/2XDmVTy.

Nello specifico, le quali risultanze istruttorie testimoniano che il gruppo Enel ha illegittimamente utilizzato prerogative possedute unicamente in virtù della propria posizione di operatore integrato a monte con la distribuzione e, quindi, con la vendita in maggior tutela, quali i dati di contatto della base clienti tutelata, al fine di competere con i propri concorrenti nell'acquisizione di contratti di vendita dell'energia elettrica a condizioni di libero mercato. Anche in tale caso, l'AGCM ha ritenuto che il programma di compliance depositato dal gruppo Enel fosse idoneo a motivare la concessione di una specifica circostanza attenuante. Nel caso di specie, infatti, il programma di compliance, consistente in modifiche e miglioramenti di un programma preesistente, su cui il gruppo era più volte intervenuto per tenere conto delle best practices europee e internazionali, è stato sottoposto prima dell'invio della CRI, prevede il coinvolgimento del management, l'identificazione del personale responsabile del programma, l'organizzazione di attività di training, nonché la previsione di incentivi/disincentivi, sistemi di monitoraggio e di audit. I miglioramenti apportati in attuazione della procedura di revisione messa in atto dal gruppo nel 2016 sono stati valutati favorevolmente, in quanto indicavano una solida determinazione verso un controllo di legittimità delle condotte del gruppo sotto il profilo antitrust, utilizzando strumenti efficaci per raggiungere tale obiettivo (meccanismi di whistleblowing, previsioni di coinvolgimento obbligatorio dell'Unità Antitrust di gruppo, monitoraggio discrezionale da parte di quest'ultima sull'attività delle Unità di business, etc.). L'AGCM ha quindi concesso una riduzione dell'importo base della sanzione pari al 10%.

APPENDICE 01

Gli attori della privacy: ruoli e responsabilità dentro e fuori dall'azienda. Contiuità o rottura col passato?

Moderatori: Deborah Bolco (Pavia e Ansaldo), Mariangela Papadia (Pavia e Ansaldo), Eva Reggiani (Cleary Gottlieb Steen & Hamilton LLP)

Titolare del Trattamento e Responsabile del Trattamento

- Dai fatti alla qualificazione giuridica (e non viceversa): la "determinazione di finalità e mezzi dell'attività di trattamento"
- Gli accordi fra contitolari ex art. 26 del GDPR
  - ambito di applicabilità
  - contenuti dell'accordo e opponibilità a terzi

Organigramma *privacy* all'interno dell'azienda

- La sorte delle figure del responsabile c.d. interno del trattamento e dell'incaricato del trattamento
- Il *Data Protection Officer*
- L'Organismo di Vigilanza *ex* D. Lgs. n. 231/2001

I rapporti con le terze parti

- Qualificazione del ruolo della terza parte: responsabile del trattamento, titolare autonomo o contitolare?
- Il contratto ex art. 28 del GDPR e i contenuti minimi inderogabili
  - La figura del sub-responsabile del trattamento

APPENDICE 02

Marketing e profilazione, aspetti applicativi del GDPR

Moderatori: Andrea Mantovani (Cleary Gottlieb), Giacomo Gori (Cocuzza e Associati), Pietro Boccaccini (King&Wood Mallesons)

Quali sono le attività rilevanti ai fini dell'applicazione della disciplina del marketing e della profilazione

Principali novità nel GDPR

- L'ambito di applicazione territoriale della normativa
- Accountability e conservazione dei dati personali
- L'informativa agli interessati alla luce delle linee guida del Gruppo di Lavoro Articolo 29
- La base giuridica
    - Le caratteristiche del consenso nel GDPR
    - Quando può prescindersi dal consenso
    - Legittimo interesse e diritto di opposizione degli interessati

Il ruolo delle terze parti

- Qualifica delle terze parti e relativi adempimenti sotto il profilo dei rapporti contrattuali
- Questioni applicative in tema di cessione di *database*
-

Approccio del Garante

APPENDICE 03

La privacy nei rapporti di lavoro

Moderatori: Angela Berinati (A&A Studio Legale), Simona Custer (A&A Studio Legale), Marta Margiocco (Cocuzza e Associati)

Il trattamento dei dati personali dei dipendenti

- Collaboratori, dipendenti e familiari dei dipendenti: l'importanza delle informative e come redigerle
- Candidati: informativa e sezione "lavora con noi" del sito internet

Obblighi di istruzione del personale

- La formazione dei dipendenti
- La nomina dei designati

Privacy e profili giuslavoristici: i controlli datoriali

- Videosorveglianza e geolocalizzazione: dagli adempimenti privacy agli obblighi giuslavoristici
- Gli strumenti informatici aziendali: l'importanza della policy

APPENDICE 04

Privacy e OdV: l'impatto della disciplina privacy nell'attivitàdell'OdV, sui flussi informativi e sulle segnalazioni. Il ruolo del DPO

Moderatori: Micaela Barbotti (A&A Studio Legale), Manuela Bianchi (Castaldi-Partners), Roberto Tirone (Cocuzza e Associati)

ODV è un titolare o un responsabile del trattamento?

- La dottrina è divisa: ODV un titolare del trattamento attesa la sua autonomia organizzativa e ODV responsabile del trattamento atteso il suo inserimento nel contesto aziendale.
- Nomina a responsabile del trattamento/Regolamentazione autonoma del trattamento.

Verbali dell'ODV

- Informativa agli intervistati.
- Riservatezza delle informazioni raccolte.
- Modalità di conservazione dei verbali.
- Termine del trattamento, distruzione verbali e documenti correlati.

Whistleblowing

- Informativa privacy preventiva ai potenziali segnalatori.
- Riservatezza dei flussi informativi.
- Conservazione dei dati e mantenimento della riservatezza.

Rapporti tra ODV e DPO

Violazione delle misure di sicurezza privacy da parte dell'ODV

APPENDICE 05

Whistleblowing: la complessità di un sistema semplice

Moderatori: Tiziana Boneschi (LCA Studio Legale), Pietro Orzalesi (CastaldiPartners), Cecilia Pontiggia (Delotte Legal)

Evoluzione del contesto normativo di riferimento

- dalla Legge 190/2012 alla Legge 179/2017

La nuova disciplina

- in particolare, la tutela per il settore privato

Temi di attenzione

- regolamentazione/documentazione del processo, sicurezza informatica, rapporti con privacy e GDPR, implementazione nei gruppi multinazionali e confronto con le discipline locali, identificazione del destinatario delle segnalazioni e ruolo dell'Organismo di Vigilanza, strumenti di tutela della riservatezza dell'identità del segnalante e anonimato

Le diverse applicazioni pratiche

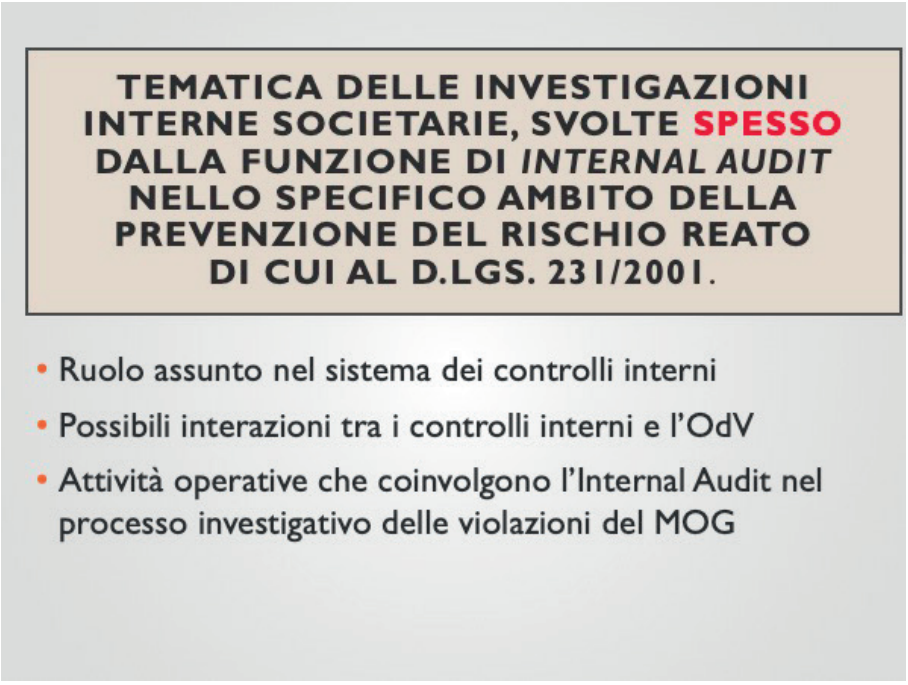
La nuova disciplina è stata recepita e come:

- Articolazione del sistema;
- Contenuti e modulistica;
- Canali;
- Gestione della segnalazione e feedback;
- Aggiornamento del Modello organizzativo adottato

APPENDICE 06

I rischi e i benefici derivanti dall'attività investigativa interna nel procedimento penale delle società

Moderatori: Antonio Bana (Studio Legale Bana), Francesca Chiara Bevilacqua (Gianni, Origoni, Grippo, Cappelli & Partners), Piero Magri (R&P Legal)



LE INVESTIGAZIONI INTERNE A SEGUITO DELLA NOTIZIA DI UN REATO PRESUPPOSTO

LE INDAGINI DIFENSIVE PENALI *EX* ART. 327-*BIS* C.P.P.

"L'ATTIVITÀ INVESTIGATIVA PREVENTIVA" *EX* ART. 327-*BIS* E 391 *NONIES* C.P.P.

PROFILI PROCESSUALI PENALI

- IL RUOLO DELL'INTERNAL AUDIT NEL PROCEDIMENTO PENALE DELLE SOCIETÀ
- I BENEFICI DERIVANTI DALL'ATTIVITÀ INVESTIGATIVA INTERNA NEL PROCEDIMENTO PENALE DELLE SOCIETÀ
- SPUNTI DI RIFLESSIONE SULL'ANALISI DEI PROFILI PROCESSUALI PENALI CHE POSSONO RIGUARDARE L'OPERATO DELL'*INTERNAL AUDITOR* NELLA PARTICOLARE CORNICE DEL PROCEDIMENTO PENALE AGLI ENTI
- DIFFICOLTÀ OPERATIVE CONNESSE ALL'ATTIVITÀ INVESTIGATIVA:
  - I CONTROLLI A DISTANZA E LO STATUTO DEI LAVORATORI
  - I PROFILI DI CONTROLLO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

COMPLIANCE PROGRAMS

1) Impegno proattivo nella prevenzione dei reati (previsione di una "*compliance defence*", fondata sulla auto-organizzazione interna)

Self reporting allo stato dei fatti illeciti

2) Rispetto delle regole societarie da parte di manager e dipendenti

Tema degli incentivi/disincentivi nei meccanismi di responsabilizzazione penale delle società e il ruolo delle investigazioni endo-aziendali, del *whistleblowing* e della cooperazione con le autorità penali

Profilo dal Codice di Procedura Penale nell'ambito dell'Attività di Polizia Giudiziaria nelle indagini preliminari:

Ad Iniziativa:
. Sommarie informazioni (Art. 350)
. Perquisizioni urgenti (Art. 352)
. Acquisizione di plichi e corrispondenza (Art. 353)
. Rilievi urgenti (Art. 354)

Delegata:
. Individuazione di persone o cose (Art 361)
. Interrogatorio indagato libero (Art. 370)
. Confronti (Art. 370)
. Sommarie informazioni (Art. 362)
. Perquisizione fuori dei casi urgenti (Art. 352)

Di assistenza:
. Notifica atti (Art. 148 2° comma e art. 151)
. Documentazione atti PM (Art. 373 6° comma)

Il concetto di *compliance* «reattiva»:

L'importanza della reazione delle società al presunto illecito

Gestione delle fasi critiche da parte del sistema di *compliance* aziendale:

- Il «perno» dell'OdV
- Costituzione di una *Task Force* (Es. Unione competenze **interne** con i legali e di *Internal Audit*, **esterne** con legali esterni, CT)
- *Sanity Check* delle procedure aziendali con eventuali revisioni/ampliamento delle procedure
- Audit interni VS indagini difensive
- Collaborazione alle indagini giudiziarie e diritto di difesa

GESTIONE DEI RAPPORTI CON L'AUTORITÀGIUDIZIARIA

GESTIONE DELLE INFORMZIONI PER L'A.G.

GESTIONE DEI DOCUMENTI PER L'A.G. (es. email, interviste…)

LINEE GUIDA SULLA REGOLAMENTAZIONE DELLE ATTIVITÀ DA SVOLGERE

. MODALITÀ DELLE SEGNALAZIONI

. MODALITÀ DI TRATTAMENTO DA PARTE DEGLI ORGANI PREPOSTI

. GESTIONE DELLA CRISI PER IL D. LGS. 231/2001 (INDAGINI INTERNE E RELATIVE COMUNICAZIONI)

. MODALITÀ DI DISCIPLINARE, FACILITARE E REGOLAMENTARE I FLUSSI INFORMATIVI TRA GLI ORGANI E LE FUNZIONI DELL'AZIENDA POTENZIALMENTE COINVOLTA PREDISPONENDO UNA SCALETTA DI CONTROLLO

CONTROLLO SU:

- COLORO CHE RICEVONO O POSSONO RICEVERE LE SEGNALAZIONI
- NATURA E AMBITO DELLE SEGNALAZIONI
- COLORO CHE HANNO LA RESPONSABILITÀ DI "GESTIRE" LE SEGNALAZIONI (FONDATEZZA)
- COLORO CHE SONO INTERESSATI DALLE INFORMAZIONI SEGNALATE
- COLORO CHE HANNO LA RESPONSABILITÀ DI PRENDERE GLI OPPORTUNI PROVVEDIMENTI
- POSSIBILI DEFINIZIONI PER ATTUARE AZIONI CORRETTIVE

TRE LIVELLI DI OPPORTUNITÀ:

Opportunità — DI DOCUMENTARE LE VERIFICHE SVOLTE CON RICOSTRUZIONE DI QUANTO ACCADUTO, CON TRACCIABILITÀ DELLE DECISIONI ASSUNTE (ARCHIVIAZIONE E SUA MOTIVAZIONE)

Opportunità — DI REGOLAMENTARE CON TEMPISTICHE E MODALITÀ LA COMUNICAZIONE, ANCHE ELETTRONICA E CARTACEA, LE SEGNALAZIONI RICEVUTE E E I RAPPORTI CON GLI ORGANI ESTERNI

Opportunità — DI UN TEMPESTIVO E COMPLETO REPORT AGLI ORGANISMI PREPOSTI

IL RUOLO DELL'ODV NELL'ESPLETAMENTO DELLE INDAGINI INTERNE

***MODUS OPERANDI* ODV**

QUALI FUNZIONI COINVOLGERE,

INTENSIFICARE E CURARE I RAPPORTI CON:

- ✓FIGURE APICALI
- ✓FIGURE CHE PRESIEDONO PROCESSI A RISCHIO
- ✓FUNZIONI DI CONTROLLO INTERNE
- ✓ORGANI DI CONTROLLO ESTERNI


Attività correlate alla gestione delle segnalazioni
Si suggerisce di affidare a un team dedicato o a un soggetto diverso da OdV (*internal audit*, consulenti esterni)
IL GIUDIZIO DELL'ODV DEVE ESSERE *AUTONOMO E INDIPENDENTE* NELLA VALUTAZIONE DEGLI ESITI.
Particolare attenzione alla scelta del consulente in termini di indipendenza e di professionalità
L'OdV può formulare considerazioni


La normativa disciplinante le investigazioni difensive preventive
L'affidamento del mandato difensivo al difensore consente di consolidare l'*attorney-client privilege*
Prevede l'opponibilità del segreto professionale alle autorità inquirenti

Lo svolgimento dell'attività da parte del difensore è sottoposto ad una peculiare tutela giudiziaria caratterizzata dall'applicabilità delle disposizioni in materia di segreto professionale *ex* art. 200 c.p.p. afferenti «*le garanzie di libertà del difensore*» statuite all'art. 103 c.p.p. oltre alla possibilità per il difensore

«*di non produrre in giudizio i verbali contenenti dichiarazioni sfavorevoli al cliente*».

APPENDICE 07

Whistleblowing: la complessità di un sistema semplice

Moderatori: Tiziana Boneschi (LCA Studio Legale), Pietro Orzalesi (CastaldiPartners), Cecilia Pontiggia (Delotte Legal)

Evoluzione del contesto normativo di riferimento

- dalla Legge 190/2012 alla Legge 179/2017

La nuova disciplina

- in particolare, la tutela per il settore privato

Temi di attenzione

- regolamentazione/documentazione del processo, sicurezza informatica, rapporti con privacy e GDPR, implementazione nei gruppi multinazionali e confronto con le discipline locali, identificazione del destinatario delle segnalazioni e ruolo dell'Organismo di Vigilanza, strumenti di tutela della riservatezza dell'identità del segnalante e anonimato

Le diverse applicazioni pratiche

La nuova disciplina è stata recepita e come:

- Articolazione del sistema;
- Contenuti e modulistica;
- Canali;
- Gestione della segnalazione e feedback;
- Aggiornamento del Modello organizzativo adottato

NOTE

NOTE

NOTE

NOTE

ASLA, Associazione Studi Legali Associati, editrice di questo Quaderno (*www.aslaitalia.it*), comprende circa cento fra i principali Studi nazionali e di affiliazione estera operanti in Italia (fra cui quelli a cui appartengono le curatrici e i co-autori del Quaderno stesso, sotto specificati), ove è stata constituita nel 2003 come organizzazione apolitica senza scopo di lucro, operando in particolare nel settore del diritto d'impresa e con il fine di promuovere e diffondere la cultura e le modalità più attuali dell'esercizio della professione legale in forma associata, organizzata e certificabile.

In particolare, hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Antonio Bana**, dello Studio Legale Bana di Milano (www.studiobana.it)

L'Avv. **Stefano Cancarini**, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

L'Avv. **Roberto Tirone**, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Francesca Chiara Bevilacqua**, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli& Partners (www.gop.it)

L'Avv. **Micaela Barbotti**, dello Studio Legale Associato A&A (www.albeeassociati.it)

L'Avv. **Pietro Orzalesi**, dello Studio Legale Associato CastaldiPartners (www.castaldimourre.com)

L'Avv. **Andrea Mantovani**, dello Studio Legale Associato Cleary Gottlieb Steen & Hamilton LLP (www.clearygottlieb.com)

L'Avv. **Eva Cruellas Sada**, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Eugenia Gambarara**, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

L'Avv. **Eva Reggiani**, dello Studio Legale Associato Cleary Gottlieb Steen & Hamilton LLP (www.clearygottlieb.com)

L'Avv. **Deborah Bolco**, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.it)

L'Avv. **Mariangela Papadia**, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.it)

L'Avv. **Giacomo Gori**, dello Studio Legale Associato Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Pietro Boccaccini**, dello Studio Legale Associato King & Wood Mallesons (www.kvm.com)

L'Avv. **Federica Dendena**, dello Studio Legale Associato SILS (www.silsitalia.it)

L'Avv. **Giulio Novellini**, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Tommaso Sala**, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

L'Avv. **Simona Custer**, dello Studio Legale Associato A&A (www.albeeassociati.it)

L'Avv. **Angela Berinati**, dello Studio Legale Associato A&A (www.albeeassociati.it)

L'Avv. **Marta Margiocco**, dello Studio Legale Associato Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Cecilia Pontiggia**, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)

L'Avv. **Tiziana Boneschi**, dello Studio Legale Associato LCA (www.lcalex.it)

L'Avv. **Piero Magri**, dello Studio Legale Associato R&P Legal (www.replegal.it)

L'Avv. **Laura Liguori**, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Luigi Zumbo**, dello Studio Legale Associato SILS (www.silsitalia.it)

Pubblicazione giuridica n° 15 di ASLA

A cura del Gruppo di lavoro sulla Corporate Compliance
Curatori: Irene Picciano e Antonio Bana
Editor: Ezio Rotamartir

Impaginazione ed elaborazioni grafiche: Ezio Rotamartir
Progetto grafico originale: Edoardo Steiner

www.aslaitalia.it

In particolare, hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Antonio Bana**, dello Studio Legale Bana di Milano (www.studiobana.it)

L'Avv. **Stefano Cancarini**, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

L'Avv. **Roberto Tirone**, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Francesca Chiara Bevilacqua**, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Micaela Barbotti**, dello Studio Legale Associato A&A (www.albeeassociati.it)

L'Avv. **Pietro Orzalesi**, dello Studio Legale Associato CastaldiPartners (www.castaldimourre.com)

L'Avv. **Andrea Mantovani**, dello Studio Legale Associato Cleary Gottlieb Steen & Hamilton LLP (www.clearygottlieb.com)

L'Avv. **Eva Cruellas Sada**, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Eugenia Gambarara**, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

L'Avv. **Eva Reggiani**, dello Studio Legale Associato Cleary Gottlieb Steen & Hamilton LLP (www.clearygottlieb.com)

L'Avv. **Deborah Bolco**, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.it)

L'Avv. **Mariangela Papadia**, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.it)

L'Avv. **Giacomo Gori**, dello Studio Legale Associato Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Pietro Boccaccini**, dello Studio Legale Associato King & Wood Mallesons (www.kvm.com)

www.aslaitalia.it

L'Avv. **Federica Dendena**, dello Studio Legale Associato SILS (www.silsitalia.it)

L'Avv. **Giulio Novellini**, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Tommaso Sala**, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

L'Avv. **Simona Custer**, dello Studio Legale Associato A&A (www.albeeassociati.it)

L'Avv. **Angela Berinati**, dello Studio Legale Associato A&A (www.albeeassociati.it)

L'Avv. **Marta Margiocco**, dello Studio Legale Associato Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Cecilia Pontiggia**, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)

L'Avv. **Tiziana Boneschi**, dello Studio Legale Associato LCA (www.lcalex.it)

L'Avv. **Piero Magri**, dello Studio Legale Associato R&P Legal (www.replegal.it)

L'Avv. **Laura Liguori**, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Luigi Zumbo**, dello Studio Legale Associato SILS (www.silsitalia.it)

ASLA, **Associazione Studi Legali Associati**, *www.aslaltalia.it*, editrice di questo Quaderno, comprende circa cento fra i principali Studi nazionali e di affiliazione estera operanti in Italia (fra cui quelli a cui appartengono le curatrici e i co-autori del Quaderno stesso, sopra specificati), ove è stata constituita nel 2003 come organizzazione apolitica senza scopo di lucro, operando in particolare nel settore del diritto d'impresa e con il fine di promuovere e diffondere la cultura e le modalità più attuali dell'esercizio della professione legale in forma associata, organizzata e certificabile.

ASLA
Associazione Studi Legali Associati