Vincenzo Apa, Giovanni Caruso, Piercarlo Felice, Damiano Marinelli

D.Lgs 231/2001: la responsabilità amministrativa degli enti

Addendum 2020.

1. L'introduzione della Legge 157 del 19 Dicembre 2019: I nuovi reati fiscali

1.2. La confisca "allargata" per i reati tributari.

1.3. Possibili sinergie tra Decreto Legislativo 231/01 e *GDPR-General Data Protection Regulation*

1.4. La funzione del DPO nel GDPR e dell'OdV nel modello organizzativo 231: vigilanza sulla compliance

1.1 L'introduzione della Legge 157 del 19 Dicembre 2019: I nuovi reati fiscali

Il Senato, in una delle sue ultime sedute, per l'anno 2019, e precisamente in quella del 17 dicembre, ha, senza non poche trepidazioni politiche ed istituzionali, dato il via libera definitivo alla Legge di conversione, con le opportune modifiche, al D.L. 26 ottobre 2019, n. 124[1], recante "Disposizioni urgenti in materia fiscale e per esigenze indifferibili" (c.d. Decreto fiscale).

Tra le più rilevanti novità poste dal sopracitato decreto, senza dubbio, vi sono, anche quelle relative all'introduzione nell'alveo della Responsabilità amministrativa degli enti, anche alcuni delitti tributari, che entrano nei cd "reati presupposto", propri del D.lgs 231/01.

Va però precisato che l'efficacia, e quindi la relativa punibilità, delle modifiche in materia penale previste dal decreto-legge era stata *ab initio* posticipata al momento dell'entrata in vigore della legge di conversione (art. 39, comma 3, d.l. 124/2019).

In ogni caso, a prescindere dall'astratta fattispecie di reato, configurabile a norma del decreto in esame, è indubbio che tale nuova impostazione legislativa, atta a contrastare i fenomeni di evasione ed elusione fiscale, non sarà di poco conto, sia per le aziende che già in passato hanno scelto di dotarsi di un modello di organizzazione, gestione e controllo, ma anche, e specialmente, agli enti che avevano, spesso anche per ragioni preclusione di colpevolezza scelto di non dotarsi di alcun modello organizzativo, ma che con l'ampliamento delle fattispecie di reato, che ad oggi, indiscutibilmente, ampliano notevolmente i soggetti intrinsecamente oggetto di presupposto di reati, che dovranno ora, valutarne l'effettiva adozione.

Per gli Enti che hanno scelto di dotarsi di un MOG ex lege 231/01, sarà quindi necessario procedere alla loro urgente modifica al fine di renderli efficaci anche con riferimento alla prevenzione delle nuove fattispecie penal-tributarie.

Prima di entrare in rassegna, con le nuove singole fattispecie di reato, di seguito si elencano le maggiori modifiche di natura penal-tributario che riguarderanno il D.lgs 231/01:

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;

[1] https://www.gazzettaufficiale.it/eli/id/2019/10/26/19G00134/sg

b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 2-*bis*, la sanzione pecuniaria fino a quattrocento quote;

c) per il delitto di dichiarazione fraudolenta mediante altri artifici previsto dall'art. 3, la sanzione pecuniaria fino a cinquecento quote;

d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;

e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 2-*bis*, la sanzione pecuniaria fino a quattrocento quote;

f) per il delitto di occultamento o distruzione di documenti contabili previsto dall'art. 10, la sanzione pecuniaria fino a quattrocento quote;

g) per il delitto di sottrazione fraudolenta al pagamento di imposte previsto dall'art. 11, la sanzione pecuniaria fino a quattrocento quote. Se l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Nei casi sopra esposti, le sanzioni inflitte all'ente sono quelle interdittive, a norma dell'art. 9, comma 2, lettera *c* (divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio), lettera *d* (esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi) e lettera *e* (divieto di pubblicizzare beni o servizi).

Tuttavia, l'introduzione dei reati tributari tra gli illeciti in grado di determinare la responsabilità "amministrativa" da reato dell'ente è destinata a cambiare la prospettiva dalla quale guardare a questi aspetti della gestione aziendale.

Se fino ad oggi, infatti, aree di attività come quelle menzionate venivano analizzate in quanto fonti di rischio indiretto o "strumentale", in grado di ospitare condotte volte ad occultare o preparare la commissione di reati quali – a titolo esemplificativo – il riciclaggio, la corruzione tra privati o le illecite operazioni sul capitale sociale, con l'entrata in vigore della modifica legislativa le stesse dovranno invece essere studiate ed affrontate, con riferimento ai reati tributari, come aree a rischio "diretto".

In altre parole, l'intero sistema di procedure e protocolli già delineato nell'ambito di queste attività dovrà essere sottoposto a revisione, al fine di verificarne l'idoneità preventiva con specifico riferimento agli illeciti richiamati dal nuovo art. 25-quinquiesdecies, D.lgs. 231/2001.

Veniamo, dunque, alle novità apportate dalla riforma.

L'inasprimento sanzionatorio, della legge 157/2019 si pone in totale controtendenza rispetto alla riforma del 2015 viene evidenziata in una duplice direzione. In primo luogo si elevano le condizioni edittali di pena per molti di questi reati, con ricadute per alcuni di essi anche sui termini di prescrizione; in secondo luogo si abbassano le soglie di punibilità previste, così estendendosi l'area di rilevanza penale dell'evasione fiscale.

Entrambi questi effetti, tuttavia, sono stati smorzati dalle modificazioni apportate dalla legge di conversione, che in questo senso ammorbidisce l'effetto innovativo della riforma. Sotto il primo profilo, si segnala che l'innalzamento delle pene per i reati di cui agli artt. 4 e 5 d.lgs. 74/2000, pur confermato, è stato ridimensionato (*infra*, § 2.3 e § 2.4). Sotto il secondo profilo, il prospettato abbassamento delle soglie di punibilità, mantenuto all'art. 4, non viene invece confermato rispetto ai reati di omesso versamento *ex* art. 10-*bis* e 10-*ter*, le cui soglie rimangono pertanto invariate (*infra*, § 2.7). Inoltre, le suindicate novità volte ad irrigidire il sistema penaltributario vengono controbilanciate da un ampliamento dell'ambito applicativo della causa di non punibilità dell'art. 13, comma 2, che viene estesa anche ai reati di cui agli artt. 2 e 3 (*infra*, § 2.8).

In riferimento al reato di "*dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*" (art. 2): i) la pena viene elevata dalla reclusione da un anno e sei mesi a sei anni a quella della reclusione da 4 a 8 anni; ii) viene introdotto un comma 2-*bis* in forza del quale il previgente trattamento sanzionatorio (reclusione da un anno e sei mesi a sei anni) viene mantenuto nella sola ipotesi in cui l'ammontare degli elementi passivi fittizi sia inferiore a 100.000 euro[2]. Siffatto irrigidimento sanzionatorio viene tuttavia contemperato dall'applicabilità, esclusa prima della presente riforma, della causa di non punibilità di cui all'art. 13, comma 2 in caso di pagamento del debito tributario (*infra*, § 2.8).

Da una lettura più approfondita della norma si potrà notare come sia stata implicitamente confermata dal legislatore la scelta di configurare la fattispecie di cui all'art. 2 come reato "senza soglia", vale a dire sanzionabile, il comportamento delittuoso, a prescindere dall'importo dell'imposta evasa. Della legittimità costituzionale di tale scelta, al metro del principio di ragionevolezza e uguaglianza dell'art. 3 Cost., aveva di recente dubitato il Tribunale di Palermo, il quale aveva pertanto sollecitato il sindacato della Consulta,

[2] Un'analoga rimodulazione al "ribasso" di pena legata all'entità della passività fittizia era già stata prevista (con una soglia di euro 154.937,07) al terzo comma della disposizione, che venne però rimossa ad opera d.l. 13 agosto 2011, n. 138, convertito, con modificazioni, dalla l. 14 settembre 2011, n. 148.

lamentando in sostanza che il delitto in esame non fosse assoggettato alle medesime soglie di punibilità contemplate dall'art. 3 (dichiarazione fraudolenta mediante altri artifici).

Con la sentenza n. 95 del 2019, la Corte costituzionale[3] ha tuttavia ritenuto infondata la questione di legittimità costituzionale. Nella sentenza si osserva che «tramite la norma censurata, il legislatore ha inteso "isolare", nell'ambito dell'ampia gamma dei mezzi fraudolenti utilizzabili a supporto di una dichiarazione mendace, uno specifico artificio, al quale viene annesso, sulla base dell'esperienza, uno spiccato coefficiente di "insidiosità" per gli interessi dell'erario». Questa «precisa strategia, espressiva dell'ampia discrezionalità del legislatore in materia di politica criminale» non può essere considerata manifestamente irragionevole o arbitraria «tenuto conto del particolare ruolo che la fattura e i documenti ad essa equiparati sul piano probatorio dalla normativa fiscale assolvono nel quadro dell'adempimento degli obblighi del contribuente, nonché della capacità di sviamento dell'attività accertativa degli uffici finanziari che l'artificio in questione possiede».

Viene intensificato il trattamento sanzionatorio del reato di "*dichiarazione fraudolenta mediante altri artifici*" (art. 3): si passa dalla pena della reclusione da un anno e sei mesi a sei anni alla pena della reclusione da 3 a 8 anni. Non viene in questo caso toccata la soglia di punibilità.

La legge di conversione ha invece apportato alcune modificazioni alle novità relative al reato di "*dichiarazione infedele*" (art. 4).

Viene confermata la riduzione delle soglie di punibilità previste tanto alla *lettera a* (ove la soglia di imposta evasa passa da 150.000 a 100.000 euro), quanto alla *lettera b* della norma (ove la soglia degli elementi attivi sottratti all'imposizione è ridotta da tre milioni a due milioni di euro). Quest'ultima viene quindi riportata esattamente a quella vigente ante riforma 2015, mentre la soglia di punibilità di cui alla *lettera a*, pure abbassata, viene mantenuta ad un livello comunque superiore a quello precedente al 2015, quando cioè si attestava sui cinquantamila euro.

La legge eleva inoltre la cornice edittale della norma, smorzando però in questo caso l'intervento previsto nel decreto-legge. Quest'ultimo prevedeva che si passasse dalla reclusione da uno a tre anni alla reclusione da 2 a 5 anni, mentre la legge di conversione ha assestato la cornice da un minimo di 2 anni ad un massimo di 4 anni e sei mesi.

Il decreto-legge viene altresì modificato nella parte in cui prevedeva l'abrogazione della disposizione di cui al comma 1-*ter* dell'art. 4, disposizione in forza della quale si escludeva la punibilità delle "valutazioni" che, singolarmente considerate, differissero in misura

[3] https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2019&numero=95

inferiore al 10% da quelle corrette, precisando altresì che gli importi compresi in tale percentuale non fossero computati ai fini del superamento delle soglie di punibilità. Sarebbe stata così rimossa una disposizione che di fatto riproduceva in relazione alla sola dichiarazione infedele il disposto dell'abrogato art. 7, comma 2, d.lgs. 74/2000[4] e che aveva destato più di una perplessità per il fatto di limitare quantitativamente delle valutazioni in un ambito nel quale – in forza del disposto del comma 1-*bis* del medesimo articolo 4 – esse sembrano già escluse dall'area di rilevanza penale.

Viene confermato e quindi mantenuto in vigore il comma 1-*ter*, prevedendo però che le valutazioni non debbano essere "singolarmente" considerate, bensì "complessivamente" considerate.

Per il reato di "*omessa dichiarazione*" (art. 5), viene confermato l'inasprimento sanzionatorio il cui minimo edittale viene raddoppiato, portandolo dai precedenti 2 anni, e il cui massimo edittale – previsto tanto al comma 1, quanto al comma 1-*bis* – fino ai 5 anni.

Il testo del decreto legge, prevedeva un numero di anni pari a 6, dunque, a seguito dell'approvazione viene meno la possibilità di ricorrere alle intercettazioni (art. 266 c.p.p.), fermo restando l'idoneità a consentire l'applicazione della misura cautelare della custodia in carcere (art. 280, comma 2, c.p.p.).

Viene altresì confermato l'inasprimento sanzionatorio per il reato di "*emissione di fatture o altri documenti per operazioni inesistenti"* (art. 8), nella cui formulazione ante riforma la pena della reclusione variava da un anno e sei mesi a sei anni, elevandola a quella della reclusione da 4 a 8 anni; con la precisazione – inserita in un nuovo comma 2-*bis* – che la pena rimane invece quella della reclusione da un anno e sei mesi a sei anni «se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila». Lo stesso vale per il reato di "*occultamento o distruzione di documenti contabili"* (art. 10), ove si passa dalla pena della reclusione da un anno e sei mesi a sei anni ad una cornice che va da un minimo di 3 anni a un massimo di 7 anni di reclusione.

La legge di conversione ha invece posto nel nulla le prospettate modifiche delle soglie di punibilità dei reati di omesso versamento (artt. 10-*bis* e 10-*ter*).

Il decreto-legge prevedeva infatti che, nel reato di "*omesso versamento di ritenute dovute o certificate*" (art. 10-*bis*), la soglia di 150.000 euro venisse abbassata a 100.000 euro; mentre nel

[4] Con la precisazione che, a differenza che nell'art. 7, al comma 1-ter dell'art. 4 si faceva riferimento genericamente alle valutazioni e non solo a quelle "estimative".

reato di "*omesso versamento di IVA*" (art. 10-*ter*) la soglia di 250.000 euro venisse portata a 150.000 euro.

Un simile intervento avrebbe determinato la platea di soggetti a verifica penale relativamente a siffatte condotte illecite, laddove la stessa era invece stata fortemente ridimensionata solo quattro anni prima dalla già citata riforma del 2015. Si rammenterà infatti che, fino ad allora, la soglia era fissata sia all'art. 10-*bis* che all'art. 10-*ter* nella misura di 50.000 euro; misura che era stata nel 2015 triplicata all'art. 10-*bis* e quintuplicata all'art. 10-*ter* con conseguente *abolitio criminis* parziale.

L'attuale Governo voleva inizialmente ridurre l'effetto di depenalizzazione prodotto da quella riforma, attestando il confine dell'area di rilevanza penale ad un livello mediano, che avrebbe determinato la necessità di fare applicazione della regola della c.d. legge intermedia *ex* art. 2, comma 2, c.p.. Questo intento è stato però neutralizzato dagli emendamenti al decreto confluiti nella legge di conversione, che lascia pertanto invariate le soglie di punibilità di cui agli artt. 10-*bis* e 10-*ter*.

Una novità, non originariamente contemplata nel decreto legge, è quella relativa alla causa di non punibilità del pagamento del debito tributario di cui all'art. 13, comma 2 che viene estesa anche ai reati di dichiarazione fraudolenta di cui agli artt. 2 e 3 (mentre era in precedenza riferita ai soli reati di omessa o infedele dichiarazione di cui agli artt. 4 e 5).

Anche i reati di cui agli artt. 2 e 3, dunque, non saranno punibili se i debiti tributari, comprese sanzioni e interessi, siano stati estinti mediante integrale pagamento degli importi dovuti, a seguito del ravvedimento operoso o della presentazione della dichiarazione omessa entro il termine di presentazione della dichiarazione relativa al periodo d'imposta successivo, sempreché il ravvedimento o la presentazione siano intervenuti prima che l'autore del reato abbia avuto formale conoscenza di accessi, ispezioni, verifiche o dell'inizio di qualunque attività di accertamento amministrativo o di procedimenti penali.

Si conferma in questo modo la tendenza politica a favorire istituti volti a valorizzare la "resipiscenza" del contribuente, *sub specie* di pagamento all'erario delle somme dovute in conseguenza dell'evasione fiscale. Pagamento che, come si osserverà tra un attimo, è altresì utile ad evitare, ove integrale, o a ridimensionare, ove parziale, il sequestro e la confisca.

1.2. La confisca "allargata" per i reati tributari.

Dopo aver analizzato i "nuovi reati" tributari, occorre far riferimento ad un importante modifica in materia di confisca per ciò che attiene ai siffatti reati.

Difatti, risulta essenziale, all'interno del novellato assetto penal-tributario, l'introduzione di un nuovo art. 12-*ter*, che prevede l'applicabilità della c.d. confisca allargata *ex* art. 240-*bis* c.p. in caso di condanna o patteggiamento per una serie di delitti indicati dalla norma stessa (artt. 2, 3, 8, 11), allorché l'evasione fiscale superi una certa entità valoriale (100.000 euro o 200.000 euro, a seconda dei casi).

La novella di cui all'art. 240-*bis* c.p, norma confluita recentemente nella misura precedentemente prevista dall'art. 12-*sexies* l. 356/1992, ha ad oggetto il denaro, i beni o le altre utilità di cui il condannato non riesce a giustificare la provenienza e di cui, anche per interposta persona fisica o giuridica, risulta essere titolare o avere la disponibilità a qualsiasi titolo in valore sproporzionato al proprio reddito, dichiarato ai fini delle imposte sul reddito, o alla propria attività economica.

Questa confisca, dunque, consiste in una forma di ablazione fondata essenzialmente sulla sproporzione patrimoniale, sproporzione che permette una presunzione *iuris tantum* di origine illecita dei beni, secondo un meccanismo di accertamento non dissimile da quello proprio della confisca di prevenzione di cui al c.d. codice antimafia (d.lgs. 159/2011).

Questa peculiare forma di confisca "allargata", più in particolare, sarà applicabile in caso di condanna o patteggiamento:

a) per il delitto previsto dall'art. 2, quando l'ammontare degli elementi passivi fittizi è superiore a 200.000 euro (non più 100.000, come prevedeva il testo del decreto-legge);

b) per il delitto previsto dagli art. 3, quando l'imposta evasa è superiore a 100.000 euro (non più anche per l'art. 5, come prevedeva il testo del decreto-legge);

c) per il delitto di cui all'art. 8, quando l'importo non rispondente al vero indicato nelle fatture o nei documenti è superiore a 200.000 euro (non più 100.000 come prevedeva il testo del decreto-legge);

d) per il delitto di cui all'art. 11, comma 1, quando l'ammontare delle imposte, delle sanzioni e degli interessi è superiore a 100.000 euro;

e) per il delitto di cui all'art. 11, comma 2, quando l'ammontare degli elementi attivi inferiori a quelli effettivi o degli elementi passivi fittizi è superiore a 200.000 euro (non più 100.000 come prevedeva il testo del decreto-legge).

Diversamente da quanto prevedeva il testo del decreto-legge, dunque, rimangono esclusi dall'ambito applicativo della confisca allargata (non solo i reati di omesso versamento *ex* artt. 10-*bis* e 10-*ter*, già esclusi dal decreto, ma anche) i reati di cui agli artt. 4, 5, 10 e 10-*quater*. Inoltre la soglia di evasione legittimante la confisca viene, in relazione agli artt. 2, 8 e 11, comma 2, portata a 200.000 euro, in rialzo rispetto ai 100.000 euro indicati nel decreto.

Pur ridimensionando l'operatività della nuova misura di confisca patrimoniale, la legge di riforma conferma la definizione di un regime differenziato all'interno di ogni singola fattispecie incriminatrice: superata la soglia di rilevanza penale del fatto, per far scattare l'operatività della confisca allargata è necessario superare un'ulteriore soglia. Vi sarà dunque una duplice fattispecie di condotte sottoposte. Da un lato, quelle di cui al *solo* regime "ordinario" della confisca prevista dall'art. 12-*bis*, e un'altra relativa a condotte più gravi (oltre le soglie dall'art. 12-*ter*) rispetto alle quali sarà applicabile *anche* la confisca c.d. allargata di cui all'art. 240-*bis* c.p. S

Un limite all'operatività della confisca inoltre desumibile dallo stesso art. 240-*bis* c.p., che contiene una clausola in base alla quale "*in ogni caso il condannato non può giustificare la legittima provenienza dei beni sul presupposto che il denaro utilizzato per acquistarli sia provento o reimpiego dell'evasione fiscale, salvo che l'obbligazione tributaria sia stata estinta mediante adempimento nelle forme di legge*"[5].

L'inciso è volto ad escludere dall'oggetto della confisca allargata quanto l'imputato abbia già restituito all'erario, evitando una duplicazione di apprensione del provento illecito. Tale precauzione – proprio nell'ambito dei reati tributari – era già adottata nel diritto vivente in forza di un consolidato indirizzo giurisprudenziale, ed era stata addirittura "rafforzata" dal legislatore del 2015 prevedendo, al secondo comma dell'art. 12-*bis*, che la confisca sia esclusa non solo per la parte che il contribuente ha effettivamente già versato all'erario, bensì anche per quella che "si impegna" a versare. A seguito dell'odierna riforma, tuttavia, la rilevanza dell'*impegno* a pagare l'imposta evasa *ex* art. 12-*bis*, comma 2, sembrerebbe poter operare solamente in relazione alla confisca "ordinaria" prevista da quello stesso articolo,

---

5 https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=6&art.versione=1&art.codiceRedazionale=18G00046&art.dataPubblicazioneGazzetta=2018-03-22&art.idGruppo=0&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=0

mentre per la confisca allargata introdotta all'art. 12-*ter* sembrerebbe rilevare solamente l'*effettiva* restituzione all'erario.

Ci sembra peraltro verosimile (e auspicabile) che la giurisprudenza continui, anche in questo settore, a circoscrivere l'applicabilità in concreto della confisca in esame mediante il ricorso al requisito della c.d. "ragionevolezza temporale". Attraverso questo "limite implicito", il momento di acquisizione del bene di valore sproporzionato non dovrebbe risultare eccessivamente lontano dall'epoca di realizzazione del reato per cui è intervenuta condanna.

La nuova forma di confisca, per espressa previsione normativa, si applicherà "esclusivamente alle condotte poste in essere successivamente alla data di entrata in vigore della legge di conversione". Sembrano volersi così scongiurare eventuali applicazioni giurisprudenziali in senso retroattivo di quella che – a torto o ragione – viene ancora generalmente qualificata come misura di sicurezza, pertanto non soggetta al divieto di retroattività *in malam partem*. Proprio in ragione di tale qualificazione, peraltro, la presente "clausola di irretroattività" potrebbe essere interpretata nel senso di non ostare alla possibilità che la confisca, pur applicata a condotte poste in essere *dopo* l'entrata in vigore della legge, vada a colpire cespiti acquisiti in epoca *anteriore* alla medesima data. In questo senso, chi commetta un delitto tributario sopra la soglia indicata dall'art. 12-*ter* in epoca *successiva* all'entrata in vigore della presente riforma dovrebbe mettere in conto che gli sarà applicabile una confisca che è in grado di colpire anche acquisti di valore sproporzionato effettuati *precedentemente*, seppur – come si è accennato – entro il limite implicito della ragionevolezza temporale.

1.3 Possibili sinergie tra Decreto Legislativo 231/01 e *GDPR-General Data Protection Regulation*

Il D.Lgs 231/01, ha introdotto il concetto di responsabilità amministrativa delle persone giuridiche, secondo cui i reati commessi dal singolo individuo nell'interesse oppure a vantaggio dell'azienda comportano un coinvolgimento penale dell'ente stesso. L'obiettivo finale è certamente quello di evitare che venga commesso il reato e ciò può essere reso possibile grazie all'adozione di un modello organizzativo efficace che tra l'altro, se idoneo, è in grado di sollevare la persona giuridica da responsabilità in caso di reato.

Vogliamo evidenziare come il D.Lgs 231/01 ed il GDPR siano due mondi solo apparentemente lontani, sia per quanto riguarda i contenuti, sia per quanto riguarda la loro struttura.

Il *General Data Protection Regulation* "GDPR", è un regolamento europeo che ha l'obiettivo di uniformare le leggi degli stati membri dell'UE in merito al trattamento dei dati personali. Con la sua entrata in vigore, le aziende hanno dovuto dotarsi di un *modello organizzativo privacy*, ovverosia l'insieme degli adempimenti relativi alla privacy che una società deve implementare al fine di effettuare un trattamento dei dati sicuro, nel rispetto di quanto previsto dalle normative di riferimento.

L'adozione del modello organizzativo privacy, che risponde a diverse normative che regolano e disciplinano la materia privacy, implica diversi adempimenti da rispettare, tra cui – a titolo esemplificativo – i seguenti:

- Definizione ruoli e responsabilità privacy interni ed esterni;
- Predisposizione del registro del titolare dei trattamenti;
- Predisposizione del registro del responsabile del trattamento (qualora si trattino dati anche da responsabile e non solo da titolare);
- Data Breach policy;
- Retention policy;
- DPIA (valutazione di impatto e rischio del trattamento dati effettuato);
- Regolamento di utilizzo degli strumenti informatici;
- Compliance sito web.

In aggiunta alla normativa sopra indicata, particolare rilievo hanno anche i differenti provvedimenti di emanazione del EDPB (European Data Protection Board), organo deputato a garantire l'applicazione coerente della normativa a livello europeo.

In linea generale, proprio in considerazione che alcune violazioni presupposte dalla responsabilità amministrativa delle imprese riguardano tipicamente aspetti connessi al trattamento dei dati, il più delle volte personali, appaiono evidenti dei punti di contatto tra il D.Lgs 231/01 e il GDPR.

Sia con il Regolamento Ue 2016/679 che con il Decreto 231/01, viene posta particolare attenzione sul concetto di "responsabilizzazione". Si tratta di un termine solo all'apparenza generico, ma in realtà importantissimo perché pone l'accento sul fatto che un ente e tutte le figure in esso coinvolte debbano necessariamente adottare comportamenti idonei alla prevenzione del reato. Sia in ambito privacy che in quello amministrativo quindi non ci sono scuse, le giuste precauzioni sono un ottimo punto di partenza.

La struttura del Decreto 231/01 prevede infatti che, qualora l'azienda abbia adottato e successivamente attuato un modello organizzativo idoneo a prevenire i reati, possa essere considerata innocente rispetto all'illecito commesso da una figura apicale.

Anche per quanto riguarda il Regolamento Ue 2016/679 risulta necessario adottare misure finalizzate ad assicurarne la corretta applicazione. Uno dei concetti più rilevanti introdotti con il GDPR è certamente il principio dell'accountability, che prevede -appunto- la responsabilizzazione del titolare di un trattamento dati nonché l'adozione da parte dello stesso di misure tecniche e operative per salvaguardarli.

La grandissima novità nel campo del trattamento dei dati personali introdotta con il nuovo regolamento consiste proprio nel fatto che sia il titolare a decidere le modalità, le garanzie ed i limiti del trattamento dei dati, nel rispetto della normativa.

In entrambi i casi, per poter ottenere il risultato finale -ovvero la prevenzione della commissione di un illecito (reato o trattamento inidoneo dei dati)- bisogna analizzare i possibili fattori di rischio. Individuarli, infatti, risulta essenziale per il passaggio dalla pura e semplice teoria alla pratica, grazie all'adozione di misure tecnico-amministrative utili (tra l'altro) a dimostrare l'effettiva responsabilizzazione da parte dell'ente.

In definitiva, l'obiettivo comune dei due strumenti è la prevenzione del reato. Al fine di evitare la commissione di illeciti, è quindi necessario definire un organo di controllo interno:

1. DPO, la cui sigla identifica il ruolo del "Data Protection Officer", per quanto riguarda il mondo della privacy. Si tratta di un professionista, dotato di competenze giuridiche, informatiche, di analisi e risk management. Il suo compito principale è quello di organizzare la gestione ed il trattamento dei dati personali, nel rispetto delle normative privacy nazionali ed europee.

2. OdV o meglio "Organismo di Vigilanza". Come dice il nome stesso, è una figura molto importante nel contesto della normativa, ideata per consentire che il MOG venga effettivamente applicato e rispettato e che risulti funzionale alla prevenzione del reato.

Anche in riferimento ai delitti informatici del D.Lgs 231/01 e alla violazione dei dati, si evidenzia un punto di contatto tra le due normative, non fosse altro che il decreto legislativo 231/2001 prevede tra i reati alcuni delitti informatici strettamente connessi al trattamento illecito dei dati personali. Proprio per questo motivo alcuni modelli organizzativi 231, elaborati da associazioni o enti, prevedono tra i soggetti da coinvolgere nella stesura e nell'applicazione del codice di comportamento un "responsabile privacy".

Entrambe le normative condividono alcuni princìpi fondamentali, tra i quali:

· **Responsabilizzazione**: come già detto nel caso del D.Lgs 231/01, entrambe le normative puntano sull'adozione di misure finalizzate alla corretta applicazione del regolamento. Nel caso del GDPR, si parla appunto di principio di accountability.

· **Risk Approach**: entrambi i sistemi prevedono l'analisi dei processi, delle attività e dei ruoli per mappare i possibili fattori di rischio ai danni dei dati personali delle persone e configurare le ipotesi di reato. Si effettua perciò un approccio inverso, partendo dal rischio per individuare le modalità di prevenzione.

· **Centri di Imputazione di Attività**: entrambe le normative prevedono l'istituzione di organismi che accentrino lo svolgimento di diverse attività: tra queste, un'unità interna di vigilanza preposta alla verifica del rispetto delle regole e una di formazione del personale.

· Alcuni **reati ai danni dei dati personali** contenuti nel GDPR sono già presenti nel Decreto 231/01, tra i quali:

1. *Associazione per delinquere* (art 24-ter d.lg. 231)-I delitti in tema di privacy (che non possono essere ascritti in quanto tali ad una persona giuridica) possono costituire reati-scopo di un'associazione per delinquere. In questo modo potrebbe essere contestato all'ente il delitto associativo finalizzato, ad esempio, al trattamento illecito di dati personali. Sto parlando di scenario possibile, tralasciando in questa sede il tema della fondatezza di tale addebito (come è noto parecchio osteggiata perché si risolverebbe nell'aggiramento del principio di tassatività dei reati-presupposto).

2. *Riciclaggio/Autoriciclaggio* (art 25-octies d.lg. 231) - Il trattamento illecito di dati personali può procurare un profitto o, almeno, un risparmio di spesa all'ente: tali proventi illeciti potrebbero essere impiegati in attività lecite. Di recente la Cassazione ha ritenuto configurabile a carico di un ente l'autoriciclaggio dei proventi di un'estorsione (altro reato non presupposto).

3. *Prevenzione dei reati informatici* (art 24-bis d.lg. 231) - Il sistema di organizzazione, gestione e controllo in tema di privacy rileva in modo importante sulla prevenzione dei reati informatici. Sotto questo profilo trattasi di sistema che va opportunamente richiamato nel (e coordinato con il) Modello organizzativo.

Si possono declinare, quindi i punti di contatto tra le due normative nei seguenti aspetti:

- Prevenzione e valutazione dei rischi attraverso un'attenta analisi di processi, attività e ruoli. E' la previsione di un'organizzazione da parte della società al fine di evitare la commissione di condotte illecite (ciascuna materia ha le sue previsioni di illeciti);
- Individuazione, come secondo passo, delle misure di prevenzione o rimedi;

- Formazione e istruzione, per consentire a tutto il personale una corretta applicazione delle misure preventive in senso pratico
- Organizzazioni di controllo, per verificare l'effettivo rispetto delle regole. E' la previsione di un organismo deputato ad operare un controllo sull'effettiva ed efficace implementazione della compliance ed il suo mantenimento nel tempo: tali organi sono, per l'ambito compliance 231 l'Organismo di Vigilanza (OdV – sempre obbligatorio per tutte le società che adottino un Modello Organizzativo); per l'ambito compliance privacy il Data Protection Officer (DPO – non obbligatorio per tutte le realtà, ma necessario solo per le realtà più complesse secondo specifici criteri di valutazione). Nello svolgimento delle proprie funzioni l'OdV tratta dati personali, in ipotesi anche sensibili. In particolare, ma non solo, nella gestione del whistleblowing. Il Data Protection Officer è interlocutore importante dell'OdV, alla stregua del RSPP e dei Responsabili dei sistemi di gestione aziendale. Problematico, invece, il suo inserimento nell'OdV alla luce dei compiti che gli spettano: costituisce punto di contatto con il Garante, è direttamente accessibile dagli interessati e, soprattutto, deve monitorare le modalità di trattamento da parte del Titolare e del Responsabile (e, quindi, dovrebbe monitorare anche il trattamento effettuato dall'OdV);
- mappatura dei rischi e individuazione delle modalità per mitigare l'insorgenza del rischio oltre che le conseguenze del danno, nel caso in cui l'evento non sia stato scongiurato. Una "medesimezza" di impianto è ravvisabile nella impalcatura del regolamento europeo: anche qui si impone una mappatura, stavolta dei trattamenti nonché un'analisi dei rischi, distinti a seconda del loro grado, e anche delle possibili conseguenze per l'interessato. A questa analisi segue l'individuazione delle misure di rimedio. Constatiamo, poi, la necessità di pianificare la formazione e l'istruzione in ordine al rispetto degli standard relativi al trattamento e alle misure di sicurezza. Si evidenzia l'individuazione di un centro di sorveglianza molto importante, che è rappresentato dalla funzione del responsabile della protezione dei dati;
- alcuni reati presupposto della sanzione della responsabilità amministrativa delle imprese riguardano tipicamente aspetti connessi a flussi informativi, ancorchè non si tratti di dei reati (già) previsti dal decreto legislativo 196 del 2003 (incidenter, è ancora aperta la questione del sistema sanzionatorio penale relativo al regolamento europeo 2016/679). In effetti decreto legislativo 231/2001 prevede tra i reati presupposto alcuni delitti informatici e connesse fattispecie di trattamento illecito dei dati. Non a caso, proprio per tale ragione, alcuni modelli organizzativi 231, elaborati da associazioni o enti esponenziali di categorie economiche, prevedono tra i soggetti da coinvolgere nella stesura e nell'applicazione dei modelli organizzativi del codice di comportamento proprio un non ben definito "responsabile privacy". Ciò a comprova del fatto che si tratta di un settore dal quale possono derivare falle e

comunque pericoli per la commissione di reati riconducibili ad una politica d'impresa e, pertanto, tali da provocare una reazione sanzionatoria a carico dell'impresa stessa.

Altri punti di contatto sono ravvisabili, innanzitutto, nel fatto che si individuano centri di imputazione di attività, alcune delle quali di sorveglianza, altre di formazione. Una volta adottato il Modello 231 o privacy, l'impresa deve agire su due fronti:

Formazione: dopo aver predisposto la documentazione di riferimento è fondamentale formare il personale che opera all'interno dell'Organizzazione al fine di diffondere una "cultura 231" o una "cultura privacy" e rendere fattiva l'adozione delle regole e dei controlli predisposti.

Vigilanza: si deve approntare un sistema di vigilanza sul rispetto delle regole che la Società si è data, anche tramite la nomina degli organi deputati a tale verifica (ODV e DPO). Nel Modello Organizzativo 231 sono previste, per il caso di violazione delle prescrizioni contenute nello stesso (e nel Codice Etico che ne è parte integrante), l'irrogazione di sanzioni disciplinari. Anche il Modello Privacy prevede la possibilità di sanzionare chi non rispetta le regole privacy in esso definite.

Con particolare riferimento al tema della responsabilità, è utile richiamare la Convenzione del Consiglio d'Europa sulla criminalità informatica, nella quale si evidenzia come l'impatto dei crimini informatici compiuti all'interno delle aziende, non produce più solo effetti con riguardo ai profili di responsabilità penale personale dell'autore del "crimine", ma determina un'altrettanta severa forma di responsabilità amministrativa in capo alle aziende, regolata appunto dal "Decreto 231". La sicurezza informatica si interfaccia con la tutela dei dati personali al punto che, il previgente Codice Privacy (D.lgs. n.196/03), in tema di tutela dei dati personali e, ora, il Regolamento UE 2016/679 (GDPR) stabilisce obblighi specifici e generali che si sostanziano nell'obbligo necessitato, da parte del titolare e/o del responsabile del trattamento dei dati, di implementare una serie di "adeguate" misure di sicurezza da definire in base ad un'accurata analisi dei rischi (o valutazione d'impatto sulla protezione dei dati personali). Nonostante l'intervenuta abrogazione delle misure "minime di sicurezza", di cui all'Allegato B al previgente Codice Privacy, a nostro avviso le stesse riacquistano vigore nell'indirizzare il titolare del trattamento o e/o i responsabili esterni del trattamento dei dati personali (e aggiungerei "aziendali") all'adozione degli standards di sicurezza richiesti dal GDPR al punto tale da divenire *conditio sine qua* non per lo svolgimento delle attività di trattamento dei dati. All'interno dell'azienda, al giorno d'oggi, i rischi correlati al crimine informatico sono di grande

rilevanza; si pensi che la maggior parte dei processi aziendali sono informatizzati e per di più esternalizzati; l'assistenza tecnica od i servizi di cloud computing ne sono un chiaro esempio. Difatti, il d.lgs. 231 prevede che tra l'autore materiale del reato e l'ente non debba intercorrere necessariamente un rapporto di lavoro subordinato, rilevando la subordinazione alla direzione o vigilanza di uno dei soggetti in posizione apicale, la quale è rinvenibile anche nei rapporti coni collaboratori esterni/consulenti. Questi ultimi devono essere nominati responsabili del trattamento, come nel caso dell'amministratore di sistema in outsourcing, del fornitore di servizi cloud o del manutentore del sito web aziendale e come tali devono attenersi alle istruzioni loro fornite dal titolare. È rinvenibile in tali rapporti quel vincolo di subordinazione alla vigilanza e direzione dei soggetti apicali, richiesto dall'art. 5 del D.lgs. 231, per l'insorgere della responsabilità amministrativa dell'ente.

In particolare, le aziende devono valutare ex ante l'affidabilità di tali consulenti/fornitori nonché prevedere, nei contratti conclusi con gli stessi, un'apposita clausola che regoli le conseguenze delle violazioni alle norme del D.lgs. 231/01.

La prevenzione dei reati informatici, al fine di evitare di incorrere nella citata responsabilità, passa attraverso la predisposizione di misure di sicurezza fisica, logica ed organizzativa. La sensibilizzazione della dirigenza e dei dipendenti, la loro formazione, le azioni di monitoraggio ed audit sono solo alcuni dei punti chiave per assicurare l'azienda dalle gravi ripercussioni previste dal D.lgs. 231/01.

Per difendersi l'azienda ha vari strumenti che riducono il rischio di commissione di reati ed illeciti, i più efficaci dei quali sono l'adozione di un valido ed efficace modello di organizzazione e gestione e di una privacy policy.

Il rispetto della normativa privacy, prevedendo l'applicazione di misure di sicurezza adeguate, consente appunto di prevenire la commissione dei reati presupposti previsti dal D.lgs. 231/01; le policy ed i modelli organizzativi sono efficaci ed assumono valore esimente, solamente se concretamente attuati e se portati a conoscenza di dipendenti e stakeholders.

Tutto quanto sopra esposto si può rinvenire esaminando un'importante sentenza della Suprema Corte di Cassazione n. 22313 del 03 novembre 2016 che ha cassato, con rinvio, la sentenza della Corte d'Appello territoriale,

Il caso è stato il seguente: "*alcuni ispettori, durante una verifica in banca, per accertare il rispetto delle disposizioni interne in materia di uso e sicurezza del materiale informatico assegnato ai dipendenti, rilevavano files potenzialmente dannosi nel pc aziendale in uso ad un dipendente. Pertanto, i dirigenti della società provvedevano ad emettere un provvedimento disciplinare nel quale*

reclamavano come la condotta del dipendente avesse "esposto la banca ai rischi conseguenti l'acquisizione del proprio sistema informativo di file che potrebbero comportare un coinvolgimento e sanzioni ai sensi del Decreto Legislativo n. 231 del 2001".

Il caso è di particolare interesse, oltre che per l'attualità e per la forte connessione con i profili di responsabilità amministrativa dell'ente rispetto alla condotta penalmente rilevante del dipendente, soprattutto perché, anche nell'adozione di provvedimenti disciplinari di contestazione di illeciti, l'organo di vertice ha dimostrato consapevolezza di un eventuale coinvolgimento dell'azienda, con conseguenti severe sanzioni a carico della stessa.

Per concludere, se finora si è assistito ad un'inspiegabile ritrosia degli organi di vertice delle aziende (e, con essi, dei dipendenti, dei collaboratori) nel dotarsi di modelli organizzativi identificati nel decreto 231, l'attuale scenario - anche grazie alla laboriosa opera di diffusione di tematiche legate alla prevenzione degli illeciti penali in comparti produttivi - fa ben sperare in un costante e consistente sviluppo della Compliance normativa nei particolari e sensibili ambiti che fanno capo, in particolar modo, ai reati informatici e alla tutela della salute dei lavoratori ritenendo, in tal guisa, "presidiate" le principali aree di responsabilità nei confronti di assets fondamentali di un'azienda.

Da qui emerge sempre più forte l'esigenza di divulgare queste regole che proteggono gli enti solo se vi è consapevolezza di tale azione difensiva e dei danni – a volte irreparabili – a cui si incorre senza l'adozione di modelli organizzativi, di gestione e controllo, soprattutto nel tutelare l'asset più importante e che fa gola a criminali o semplicemente a concorrenti che, slealmente, intendono condurre un'attività più o meno organizzata: il patrimonio informativo!

1.4 La funzione del DPO nel GDPR e dell'OdV nel modello organizzativo 231: vigilanza sulla compliance

Nel lungo processo di adeguamento delle imprese al GDPR, gli organi di vigilanza dei modelli organizzativi 231 hanno monitorato il processo di adattamento alle nuove disposizioni. È importante, altresì, definire correttamente la relazione che intercorre tra il DPO e l'organismo di vigilanza, identificando i ruoli e le competenze di queste due figure fondamentali all'interno della struttura organizzativa e gestionale dell'azienda: solo così si può evitare di incorrere in possibili conflitti di interesse.

In primis, occorre fare riferimento al fatto che le imprese per potersi adeguare alla nuova normativa in materia di tutela dei dati personali hanno dovuto rivedere la compliance interna finalizzata a garantire la protezione dei dati e delle informazioni personali che trattano e conservano.

Precisamente, è il titolare del trattamento che ha il compito di attuare gli adempimenti previsti dalla normativa ed è sempre quest'ultimo a dover provare di aver posto in essere le iniziative necessarie per assicurare l'adeguamento delle policy interne alla nuova disciplina.

La necessità di provare l'avvenuto adeguamento della compliance aziendale alle nuove prescrizioni privacy ha portato le imprese a introdurre una sorta di dossier privacy, detto anche modello organizzativo privacy, che, appunto, racchiude tutti gli adempimenti necessari ad assicurare la riservatezza ed il più elevato grado di tutela per i dati personali trattati nelle società.

Un modello che è simile a quello che va predisposto ed aggiornato per rispettare il D.lgs. 231/2001. Ma vediamone gli aspetti più salienti.

La prima fase è la revisione dell'organigramma aziendale, prestando cioè attenzione alla presenza delle nomine esistenti e alla descrizione dei nuovi compiti assegnati al titolare, al responsabile del trattamento, agli incaricati al trattamento.

A ciò si accompagna la verifica circa l'obbligatorietà, per i casi espressamente indicati dalla normativa (ossia quando il trattamento è svolto da un'autorità pubblica o da un organismo pubblico ad eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali oppure 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), o la mera opportunità, negli altri casi, di nominare un Data Protection Officer (DPO).

Quanto sopra detto sembra rispondere pienamente al criterio della Segregation of Duties (Sod) che già governa il sistema 231, in base al quale occorre individuare distinte responsabilità in capo a ciascuna funzione descrivendone nel dettaglio i compiti affidati.

In questa ottica vi è l'obbligo di provvedere alla valutazione dei rischi privacy (una sorta di risk assessment privacy, definita DPIA: Data Protection Impact Assessment), destinato inevitabilmente a confluire in un documento riepilogativo delle analisi effettuate, in cui sono individuati i possibili rischi associati alle distinte attività svolte, passaggio che presuppone la previa disamina dei rispettivi processi aziendali nell'ambito dei quali sono trattati i dati (operazione di adeguatezza prognostica del trattamento).

In questa valutazione si deve tener conto dell'identità dei soggetti interessati al trattamento (ad esempio, dipendenti o fornitori), delle finalità del trattamento nonché delle tipologie (e.g. dati sanitari, anagrafici o altri) e delle categorie di trattamento entro le quali sono compresi i dati gestiti dall'azienda.

Sarà, ovviamente, necessario garantire a questo documento un costante aggiornamento in base agli eventuali mutamenti sia organizzativi che normativi in grado di incidere sul trattamento dei dati messi a disposizione delle imprese.

Un ruolo fondamentale in questo contesto è stato ed è svolto dall'organismo di vigilanza. Infatti, nel lungo processo di adeguamento al Regolamento UE 679/2016, gli organismi di vigilanza hanno monitorato il processo di adattamento alle nuove disposizioni ed hanno vigilato all'adeguamento del modello 231 eventualmente già adottato.

L'OdV nell'esercizio delle sue funzioni entra in contatto con una pluralità di dati personali, difatti la gestione di flussi informativi, le attività di controllo e vigilanza nonché le eventuali segnalazioni di condotte illecite portano inevitabilmente allo svolgimento di trattamenti di dati riferiti o riferibili a persone fisiche facenti parte del management aziendale (art. 6 D.lgs. 231/2001).

Nello svolgimento delle proprie funzioni l'OdV tratta dati personali, in ipotesi anche sensibili, in particolare, ma non solo, nella gestione delle importanti funzioni che l'art. 6 del decreto gli ha attribuito in merito alla nuova disciplina del whistleblowing[1].

Infatti, la normativa sul whistleblowing che ha introdotto la possibilità di segnalare reati, irregolarità e difformità garantendo l'anonimato del segnalante ha posto in capo all'OdV un ruolo fondamentale all'interno della disciplina della privacy.

Sono state introdotte specifiche modalità di presentazione delle comunicazioni circa eventuali violazioni riscontrate sui dati personali (data breach): sono previsti moduli distinti a seconda della tipologia di violazione riscontrata, l'individuazione di un ufficio responsabile per ricevere le segnalazioni oltre che l'individuazione di eventuali iniziative da intraprendere, a livello organizzativo e tecnico, capaci di porre rimedio alle irregolarità che si sono verificate.

Tale disciplina si applicherà esclusivamente in presenza di un valido modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001 e pone delle limitazioni riguardo "l'anonimato" del segnalante, qualora le informazioni risultino false (Direttiva 95/46/CE che sul punto non è molto difforme dal GDPR).

In tale ottica sembra evidente che la disciplina del whislteblowing che ha apportato modifiche significative al Mog 231 – prevedendo tra l'altro almeno un canale alternativo di segnalazione di illeciti, idoneo a garantire con modalità informatiche la riservatezza dell'identità del segnalante e misure idonee a tutelare l'identità del segnalante e a mantenere la riservatezza dell'informazione in ogni contesto successivo alla segnalazione – attribuendo un ruolo di primaria importanza all'OdV debba necessariamente integrarsi con il Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Si vede, quindi, come la disciplina del whistleblowing è strettamente collegata alla disciplina della Privacy. Il Garante per la protezione dei dati personali già nel 2009 aveva posto la sua attenzione sulla disciplina del whistleblowing, evidenziando un problema nel sistema disciplinare. Il Garante, ha dunque, sollecitato la disciplina del whistleblowing, evidenziando anche i punti che questa avrebbe dovuto specificare. I due punti cardine della disciplina possono essere cosi riassunti: a) la disciplina si applica solo alle società che hanno adottato un Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001; b) la disciplina pone delle limitazioni riguardo "l'anonimato" del segnalante, se le informazioni risultano false (direttiva 95/46/CE che sul punto non è molto difforme dal Regolamento GDPR). Sembra evidente, che la disciplina del whislteblowing, deve integrarsi con il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Secondo il GDPR, dunque, la disciplina del whistleblowing dovrà necessariamente rispettare i seguenti punti: a) definire esaustivamente i ruoli attribuiti ai vari attori coinvolti nella procedura anche dal punto di vista dell'organigramma privacy; b) garantire adeguate misure di sicurezza del dato personale e/o sensibile trattato; c) in caso di multinazionali, disciplinare le modalità di eventuali trasferimenti di dati tra Stati extra-europei; d) disciplinare il diritto di accesso del soggetto segnalato agli atti.

Proprio la peculiarità del ruolo svolto dall'organismo di vigilanza (in composizione mono soggettiva o plurisoggettiva) nell'ambito del trattamento dei dati personali, potrebbe erroneamente portarci ad associare tale figura a quella del titolare o del responsabile del trattamento previste dalla nuova normativa privacy.

Difatti, in assenza di uno specifico divieto normativo e alla luce della possibilità per il DPO di svolgere altri compiti e funzioni, appare spontaneo chiedersi se il medesimo possa ricoprire anche l'incarico di organismo di vigilanza per la stessa realtà, in presenza delle qualità professionali e della conoscenza specialistica richieste.

In assenza di una normativa specifica l'assioma "*tutto ciò che non è espressamente vietato è permesso*", a nostro parere, non può essere applicato al caso di specie in quanto, attribuire

ad una figura unica il ruolo di Responsabile per la protezione dei dati e di ODV andrebbe in contrasto con le linee guida pubblicate dal Working Party 29 e alla disposizioni indicative enunciate dalla stessa Autorità Garante italiana.

Inoltre, non si può non sottolineare che le caratteristiche specifiche delle due figure sottoposte all'odierna analisi determinerebbero moltissime situazioni di conflitto, nel caso in cui il duplice ruolo fosse affidato ad un unico soggetto in quanto l'unione di dette figure porterebbe alla sovrapposizione, in molti casi, della figura di controllore e controllato.

Tra le due figure citate non può esistere un'unione, essendo innegabile che il DPO ha, altresì, il compito di monitorare e verificare il trattamento dei dati posto in essere dall'ODV. Infatti, il DPO potrebbe trovarsi nella posizione di contestare o segnalare determinati trattamenti ovvero di verificare le misure di sicurezza adottate per il corretto trattamento.

Come se non bastasse, i due organi potrebbero confliggere in merito alla misure di sicurezza che il titolare del trattamento dovrebbe adottare al fine di evitare la commissione dei reati presupposto in ambito informatico.

Pertanto, è incerta la previsione che tale organo possa ricoprire il ruolo di titolare autonomo del trattamento, ossia di soggetto in grado di determinare finalità, mezzi e misure di sicurezza, in quanto i compiti di iniziativa e controllo propri dell'OdV non sono determinati dall'organismo stesso, bensì dall'organo dirigente nel modello di organizzazione, gestione e controllo.

In altre parole, gli aspetti relativi al funzionamento dell'OdV non sono determinati dall'OdV stesso, ma sono demandati alla dirigenza aziendale.

Pertanto, appare evidente che le due figure non sono sovrapponibili in quanto ricordiamo che il titolare autonomo del trattamento è il soggetto che determina finalità, mezzi e misure di sicurezza. E' difatti il D.Lgs. 231, e più in particolare l'Organo Dirigente che adotta il Modello, a determinare le finalità e confini del trattamento, non l'Organismo di Vigilanza. E stante il fatto che i dati personali raccolti dall'Organismo di Vigilanza sono nella quasi totalità dei casi conferiti all'azienda e da questa raccolti dall'OdV, è l'azienda stessa che ne determina finalità, mezzi e misure di sicurezza per la loro protezione. Né pensiamo che questo vada a ledere l'autonomia ed il potere d'iniziativa che sono propri dell'Organismo di Vigilanza.

Per lo stesso motivo pensiamo che possa essere esclusa l'assunzione dell'Organismo di Vigilanza ex D.Lgs.231 come contitolare del trattamento ai sensi del GDPR 2016/679 in quanto ne deriverebbe una complicazione difficilmente gestibile considerare Organismo di

Vigilanza ed Azienda contitolari. Crediamo che difatti i contitolari devono, per mezzo di un contratto scritto, decidere se e come ripartire le responsabilità rispetto agli obblighi relativi al Regolamento GDPR UE 679/2016 ed una sintesi del contratto tra i contitolari deve essere messo a disposizione delle persone interessate.

Pensiamo, in definitiva, che i due soggetti debbano cooperare al fine di garantire la giusta attenzione a criticità e violazioni eventualmente rilevate nei diversi ambiti aziendali.

A sostegno dell'incompatibilità tra queste due figure vi è poi l'attribuzione all'ODV della nomina di responsabile esterno del trattamento.

Appare, ad oggi, consolidato l'assunto alla luce del quale l'Organismo di Vigilanza, in ambito privacy, ricopra il ruolo di responsabile esterno, nonostante una dottrina minoritaria lo qualifichi ancora come titolare autonomo in ragione dei requisiti d'indipendenza e di autonomia.

Tuttavia, grazie ad un'interpretazione estensiva del provvedimento del 19 luglio 2018 emesso da Garante della Privacy ("*il sistema delle responsabilità in tema di salute e sicurezza dei lavoratori ivi delineato ha rilevanza ai soli fini degli adempimenti in materia di salute e sicurezza dei dipendenti, restando salva la titolarità dei relativi trattamenti e l'imputazione delle eventuali conseguenti responsabilità in capo all'amministrazione interessata*") appare indiscutibile che l'ODV debba essere inquadrato come responsabile del trattamento ex art. 28 GDPR.

Ci pare questa l'interpretazione più confacente per i membri esterni degli Organismi di Vigilanza ex D.Lgs.231. Difatti il Responsabile del Trattamento è, ai sensi del Regolamento UE GDPR 2016/679, il soggetto che tratta ed elabora i dati personali per conto del titolare del trattamento.

Trattandosi di un soggetto distinto dal titolare, che deve però essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, è opportuno che il titolare del trattamento assegni questo incarico ai membri dell'Organismo di Vigilanza ex D.Lgs.231 tramite apposita lettere in cui assume tutte le cautele del caso, anche in termini di competenze e misure messe in atto dal responsabile del trattamento.

Nel caso invece di membri interni dell'Organismo di Vigilanza sembrerebbe senz'altro l'interpretazione più corretta considerare Organismo di Vigilanza ex D.Lgs.231 come autorizzato al trattamento ai sensi del GDPR 2016/679. Stà di fatto che è troppo

semplicistico estenderla tout court all'Organismo di Vigilanza per il solo fatto che l'art. 6 del D.Lgs.231 lo definisce 'organo dell'ente'.

Difatti nel caso di membri esterni risulta problematico , e di certo non cautelativo per l'azienda, considerare 'autorizzati' soggetti esterni che operano con propri strumenti informatici e, nella maggior parte dei casi, trasferiscono e trattano i dati sugli archivi personali o del proprio studio.

Una via di uscita potrebbe essere quella di predisporre un facsimile di lettera di incarico come Responsabili del Trattamento, in alcuni casi personalizzata dalle singole Aziende, con la sottoscrizione reciproca della quale sarà regolarizzata la posizione ai sensi del Regolamento UE GDPR 2016/679.

Tuttavia, in merito all'ipotesi che individua l'organismo di vigilanza come responsabile del trattamento si ravvisano ulteriori perplessità.

In primis, la natura necessariamente interna all'ente dell'organismo di vigilanza come espressamente sancito dalla legge si contrappone con l'intrinseca esternalità del responsabile del trattamento, per il quale la nuova normativa prevede che possa essere anche un soggetto esterno all'organizzazione aziendale senza ripercussioni sulle modalità di trattamento dei dati personali.

Infatti, mentre l'organismo deve essere interno all'ente, soprattutto per garantire una vigilanza continua sul modello, un costante aggiornamento, una verifica della coerenza con la struttura organizzativa e il processo operativo, il responsabile del trattamento può benissimo garantire l'adempimento delle sue funzioni ricoprendo un ruolo esterno all'ente.

Al di là delle varie correnti in materia di identificazione o meno del ruolo delle due figure in disamina, appare utile una riflessione circa il rapporto tra la figura dell'Organismo di Vigilanza e quella del Responsabile della Protezione dei Dati.

Come è noto, gli illeciti legati a violazioni dei dati personali non rientrano esplicitamente nel novero dei reati per i quali si possa configurare la responsabilità dell'ente, motivo che potrebbe portare a considerare i due ambiti come compartimenti stagni. Ma se ci poniamo dal punto di osservazione dell'ente, le cose stanno in maniera diversa.

Il GDPR, infatti, richiede una valutazione dei rischi legati alla violazione dei dati personali trattati, per non menzionare l'eventuale valutazione di impatto aggiuntiva, esattamente come il D.Lgs. 231 01 richiede una valutazione dei rischi rispetto al coinvolgimento dell'ente nella commissione dei cosiddetti "reati presupposto": e quando si arriva a parlare di reati informatici (solo per citarne uno), alcune delle contromisure coprono evidentemente

entrambi gli ambiti. Possono quindi cambiare il tipo di lenti indossate, ma gli occhiali dell'analisi di rischio ormai sono un accessorio che ogni ente deve mettere nel proprio libro cespiti, come del resto avviene anche nel mondo della normazione volontaria, in cui – solo per citare alcuni esempi – le norme in materia di sicurezza informatica (ISO 27001), salute e sicurezza dei lavoratori (ISO 45001) e qualità dei servizi erogati (ISO 9001) richiedono la conduzione di una analisi che renda il management consapevole dei rischi cui è esposto in modo da metterlo nelle condizioni migliori per prendere decisioni sulle contromisure da adottare.

O, in altri termini, che renda insostenibile la posizione per cui "non ero a conoscenza di questo rischio".

In merito all'analisi di rischio ex D Lgs 231 01, assume particolare rilievo la sentenza Corte Cassazione Penale n.18842/201

"[…] Una volta accertata la commissione di determinati reati da parte delle persone fisiche che esercitano funzioni apicali, i quali abbiano agito nell'interesse o a vantaggio delle società, incombe sui predetti enti l'onere, con effetti liberatori, di dimostrare di aver adottata ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; in tal senso, la colpa di organizzazione, da intendersi in senso normativo, è fondata, nel sistema introdotto dal D lgs 231 01, sul rimprovero derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione dei reati previsti tra quelli idonei a fondare la responsabilità del soggetto collettivo, dovendo tali accorgimenti essere consacrati in un documento che individua i rischi e delinea le misure atte a contrastarli. […]".

Così si sono espressi i Giudici della Suprema Corte rispetto alla vicenda che ha interessato la Canditfrucht S.p.A., un'azienda leader nella produzione di succhi di frutta, olii essenziali, frutta candita, bucce essiccate, cellule, segmenti e private label, alla quale è stata imputata la gestione abusiva di ingenti quantitativi di rifiuti con riferimento al c.d. "pastazzo" di agrumi consistita nello smaltimento "in discariche abusive e in altri luoghi non autorizzati, tra Barcellona Pozzo di Gotto e le aree limitrofe" (Sentenza Cassazione Penale n. 18842/2019 depositata il 12 Marzo 2019)

La Corte di Cassazione, richiamando l'insegnamento delle Sezioni Unite (Sentenza n. 38343 del 24.4.2014 – Tyssenkrupp), ha ribadito a chiare lettere la fondamentale importanza dell'analisi di rischio e dell'esistenza di un documento in cui si consacri l'individuazione dei rischi e delle misure atte a contrastarli.

Il Modello di organizzazione, gestione e controllo ex D Lgs 231 01 non può prescindere da una completa, esaustiva analisi dei rischi di commissione del reato costantemente aggiornata: un'analisi che sia formalizzata, un'analisi che evidenzi e garantisca la tracciabilità della valutazione del rischio e, soprattutto, dell'individuazione delle misure di controllo atte a mitigare il rischio.

Un Modello di organizzazione, gestione e controllo ex D Lgs 231 01 che muove da un'analisi di rischio miope ovvero parziale rischia concretamente di impedire il superamento del vaglio di idoneità e, al contempo, un'analisi di rischio che non valuta correttamente la capacità delle misure di controllo esistenti di mitigare il rischio di commissione del reato rilevato rischia, concretamente, di impedire il superamento del vaglio di adeguatezza del Sistema 231.

Completezza, interdisciplinarietà, collaborazione tra professionisti di diversa formazione, costante aggiornamento sia rispetto alle evoluzioni normative sia rispetto alla fisiologica mutevolezza dell'azienda, accuratezza nella mappatura del sistema dei controlli esistenti e nell'analisi dello stesso rispetto ai rischi rilevati: questi sono alcuni dei principali fattori che garantiscono la costruzione di un resistente Sistema 231. Alcuni fattori, non tutti dal momento che la conduzione di una corretta analisi di rischio e l'implementazione di un Modello di organizzazione, gestione e controllo idoneo e adeguato, non bastano se non coesistono con un'efficace attuazione e un'effettiva vigilanza da parte dell'OdV.

Se andiamo poi ad analizzare la figura del Responsabile della Protezione dei Dati (RPD, art. 37 del GDPR), tra i compiti che gli sono affidati rientrano "almeno" (art. 39) la consulenza sugli obblighi derivanti dal GDPR, la sorveglianza circa l'osservanza del Regolamento, la fornitura – se richiesta – di un parere in merito alla valutazione di impatto, in forte analogia operativa con quelli che sono i compiti ormai consolidati dell'Organismo di Vigilanza.

Rimane a questo punto una interessante domanda: i ruoli di OdV e RPD sono sovrapponibili? La risposta potrebbe essere sì – a meno di espliciti divieti normativi – ma è sottoposta ad almeno due condizioni. La prima è la competenza tecnica specifica per ambito: un conto è conoscere la responsabilità amministrativa e le sue implicazioni, un altro è la normativa in materia di tutela dei dati personali, dove oltre al Governo abbiamo la figura del Garante che dispone dell'autorità per normare direttamente la materia. Il membro dell'OdV che fosse anche RPD dovrebbe garantire un adeguato aggiornamento su entrambi gli ambiti. La seconda è la capacità di relazione: se l'OdV ha un ruolo di sicura interfaccia con le controparti interessate dal modello di organizzazione e gestione, il RPD (ancora una volta secondo l'art. 39) ha istituzionalmente quello di fungere da punto di contatto con l'autorità di controllo, con la quale è tenuto a cooperare. Se si pensa al tema

delle segnalazioni circa le violazioni del modello o le lacune del sistema di controllo per la protezione dei dati (es. reclami) è più che auspicabile che le due funzioni, se fisicamente separate, cooperino strettamente per definire le specifiche regole di ingaggio.

In ultima analisi, le strutture degli ultimi dettati normativi mettono la Direzione dell'ente nella posizione facilitata di dover dialogare allo stesso modo con soggetti diversi, favorendo l'opportunità di investire in strumenti di gestione che consentano – se opportunamente tarati – la realizzazione di interessanti economie di scala, nonché di facilità di comprensione e attuazione da parte degli utenti. Non dimentichiamoci, infatti, che regole e controlli sia in ambito di responsabilità amministrativa che di tutela dei dati personali impattano direttamente sul lavoro quotidiano tanto del Megadirettore Naturale di fantozziana memoria quanto (rispettando la cinematografica similitudine) dell'ultimo degli inferiori: e tanto più controlli e regole sono chiare, motivate e comprensibili, tanto più è alta la probabilità che vengano correttamente applicate.

E se consideriamo il rischio derivante dall'applicazione delle sanzioni nei due ambiti, non è un fattore da sottovalutare.

Analizziamo adesso i possibili rapporti tra Il DPO e i principali Organi Societari, ovvero il Collegio Sindacale e l'Organismo di Vigilanza (…), e funzioni organizzative, tenuto conto che il DPO si delinea come una figura di controllo di secondo livello, volta a supervisionare e gestire le norme sulla protezione dei dati e le tecniche utilizzate per attuarla.

Il Collegio Sindacale, è chiamato a vigilare (con atti di ispezione e controllo) sull'osservanza della Legge, dello Statuto e dei principi di corretta amministrazione, con particolare riguardo all'assetto organizzativo, amministrativo e contabile; vigila sul concreto funzionamento dell'organizzazione In alcune fattispecie (2409 bis 3°comma C.C.) esercita il controllo contabile.

Il DPO potrebbe, pertanto, riportare al Collegio Sindacale, periodicamente, un'informativa sul trattamento dei dati che abbia impatto sulla corretta amministrazione dell'organizzazione. Inoltre potrebbe informare il Collegio sull'aderenza delle politiche dell'organizzazione al Regolamento ed alle norme correlate al fine di scongiurare violazioni e, se pertinente, rendere noti i mezzi attraverso cui la protezione dei dati personali è svolta.

L'obiettivo del rapporto tra DPO e Collegio Sindacale è quello di contribuire a permettere a quest'ultimo una valutazione sull'amministrazione, sul rispetto dello statuto e sull'assetto organizzativo. A sua volta, il Collegio Sindacale potrà esprimere un parere sulla collocazione organizzativa del DPO al fine di valutarne l'indipendenza rispetto alle proprie funzioni, così come previsto dal GDPR.

L'organismo di Vigilanza, in conformità all'art. 6(1) del Decreto Legislativo 231/2001, ha il compito di vigilare sul funzionamento e l'osservanza del Modello di Organizzazione, Gestione e Controllo e di curare il suo aggiornamento.

L'introduzione della figura del DPO deve attivare l'Organismo di Vigilanza (ODV), il quale deve collaborare con esso al fine di aggiornare il Modello per le materie inerenti il trattamento e la protezione dei dati. In primis, è necessario valutare l'impatto che il nuovo Regolamento ha sul Modello adottato nell'organizzazione; quindi, calandosi nell'operatività dell'organizzazione, è necessario valutare i trattamenti adottati ad esempio alla luce dei reati informatici (Art 24 bis - Delitti informatici e trattamento illecito dei dati).

A regime, come nel rapporto con il Collegio Sindacale, il DPO informa periodicamente l'Organismo di vigilanza sui trattamenti in essere e sulla prevenzione di eventuali reati. Lo informa tempestivamente in caso di deviazioni dalla norma o di vere e proprie violazioni.

Da quanto sopra ipotizzato, il DPO si conferma essere, pertanto, una figura di controllo di secondo livello centrata sul monitoraggio del corretto trattamento dei dati all'interno della azienda, cui l'ODV deve rivolgersi per avere informazioni sul trattamento dei dati, sia a livello di adempimenti normativi, sia a livello, più tecnico, di predisposizione delle sicurezze per il corretto trattamento.

In sintesi, dunque, il DPO:

- è una Persona fisica, o giuridica, con compiti di – dipendente o consulente – con conoscenza specialistica, capacità e indipendenza;
- deve disporre di risorse necessarie, agire in autonomia (non ricevere istruzioni), riferire al vertice gerarchico;
- ha il compito di informare e fornire consulenza, sorvegliare, cooperare con autorità, fungere da punto di contatto ;
- non può rivestire un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali;
- non risponde personalmente in caso di inosservanza del GDPR;
- svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda, e contribuisce a dare attuazione a elementi essenziali del GDPR quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e la comunicazione delle violazioni di dati personali;
- deve essere coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Assicurare il tempestivo e immediato coinvolgimento del DPO, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del GDPR e

promuoverà l'applicazione del principio di privacy fin dalla fase di progettazione incontra periodicamente (almeno una volta l'anno) l'OdV per riferire su stato attuazione privacy, da valutare relazione scritta;

- incontra periodicamente (almeno una volta l'anno) l'OdV per riferire su stato attuazione privacy, da valutare relazione scritta;
- segnala tempestivamente all'OdV criticità emerse e violazioni anche non notificate ma oggetto di fattispecie 231;

DPO e OdV collaborano per aggiornare il MOG e per garantire la riservatezza delle segnalazioni destinate all'OdV. Entrambi sono caratterizzati da:

- **Indipendenza e autonomia**
- **Garanzia confidenzialità informazioni**
- **Relazione annuale al vertice gerarchico**
- **Manifestazione dissenso**
- **Inamovibilità salvo giustificato motivo**
- **Configurazione delle responsabilità**

In base a quanto sopra analizzato, possiamo concludere sostenendo che, alla luce della recente normativa sulla privacy, il titolare del trattamento, il responsabile ed il Data Protection Officer (quando designato) risultano essere interlocutori importanti dell'OdV, alla stregua del RSPP e dei Responsabili dei sistemi di gestione aziendale che, quindi, dovrebbero monitorare anche il trattamento dei dati effettuato dall'OdV nella sua funzione di organo di controllo e vigilanza del modello organizzativo adottato dall'ente (articoli 6 e 7 del D.lgs. 231/2001).

Altro aspetto di collegamento tra la 231 e il Regolamento UE 679/2017 è riscontrabile con riguardo all'articolo 24-bis del D.lgs. 231/2001 rubricato Delitti informativi e trattamento illecito dei dati e cioè, nella previsione nei c.d. reati-presupposto di alcuni delitti informatici e fattispecie connesse di trattamento illecito di dati.

Tali fattispecie prevedono e puniscono ipotesi strettamente legate ad aspetti rientranti nella disciplina della privacy, intesa non solo quale tutela dei dati personali bensì tutti i dati quali per esempio, l'accesso abusivo a sistemi informatici (articolo 615-ter c.p.), l'approvazione e diffusione abusiva di codici di accesso (art. 615-quater c.p.), il danneggiamento di informazioni, dati, programmi informatici (art. 640-bis c.p.) nonché di sistemi informatici (art. 640-quater c.p.).

Appare evidente che si tratta di ipotesi delittuose che possono essere poste in essere laddove sia carente ovvero non dimostrabile una corretta ed adeguata tutela dei dati personali

trattati in ambito aziendale mentre al contrario, una documentata osservanza della relativa normativa, tanto in materia 231 quanto soprattutto di privacy, costituirebbe valida esimente a riguardo.