Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Ordine degli Avvocati di Torino

Ordine degli Ingegneri della Provincia di Torino

Tavolo di lavoro congiunto "Protezione dei dati personali – GDPR

Organismo di Vigilanza e G.D.P.R.

Aspetti penali

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»

Ordine Avvocati di Torino

Claudio Strata - *Avvocato*

TaxLawPlanet™ *Webinar*

- L'introduzione della responsabilità amministrativa degli enti ha rappresentato una svolta epocale, in quanto le società sono divenute possibili destinatarie di **conseguenze penali** derivanti da un reato commesso da un proprio soggetto (apicale o sottoposto a controllo), **nell'interesse o a vantaggio dell'ente.**

- Un'efficace adozione del Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/2001, che permette alla società di andare esente da tale responsabilità, presuppone **l'individuazione di un Organismo di Vigilanza**, preposto a sorvegliarne l'attuazione.

- L'art. 6 del D.lgs. 231/2001 enuncia il ruolo dell'OdV, che ha *"il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento"*, in qualità di ente ***"dotato di autonomi poteri di iniziativa e di controllo".***

- Considerata la delicatezza del ruolo, i membri dell'OdV devono essere dotati di **"indipendenza e autonomia"**, al fine di prevenire il compimento di atti illeciti.

- L'attività di vigilanza, così come impostata, implica che l'Organo di controllo sia destinatario di una **mole immensa di informazioni**, reperita dai flussi informativi, dalla documentazione di supporto e dai modelli che offrono la "fotografia" di ogni area.

- Nello svolgimento della propria attività, dunque**, l'OdV tratta una moltitudine di dati personali, anche di carattere particolare (di cui agli artt. 9 e 10 G.D.P.R.), come notizie su eventuali illeciti commessi.**

- Come esempi di trattamento possiamo citare:
  - **Flussi informativi** in conformità agli obblighi di informazione nei confronti dell'OdV, deputato a vigilare sul funzionamento e l'osservanza dei modelli
  - Risultati delle **attività di vigilanza e audit** effettuate
  - **Segnalazione di fatti** che potrebbero configurarsi quali ipotesi di reato imputabili all'ente (c.d. whistleblowing)

- Data la mole di dati – estremamente delicati – a cui abbiamo accennato, nasce il problema di **qualificare l'OdV ai sensi del G.D.P.R.,** ossia come titolare, responsabile o mero incaricato al trattamento. Questo rileva per stabilire la **responsabilità dei membri dell'OdV.**

- A seconda della qualificazione giuridica, infatti, muta anche il titolo della responsabilità.
  - **TITOLARE**: in tal caso l'OdV dovrebbe porre in essere tutte le misure organizzative e di compliance previste dal G.D.P.R. Si troverebbe pertanto nell'obbligo di adottare un registro dei trattamenti, organizzare e gestire i flussi di dati, garantirne la sicurezza, effettuare una DPIA, nominare un DPO, segnalare un data breach…
  - **RESPONSABILE**: se così qualificato, l'OdV dovrebbe agire conformemente alle istruzioni fornite dal titolare del trattamento, che in questo caso sarebbe la società, perdendo così il ruolo di autonomia e indipendenza che gli è proprio...

Sul punto, il Garante ritiene che:

- Quanto alla qualifica come **titolare**: l'OdV non può essere autonomo titolare del trattamento, considerato che i suoi compiti di iniziativa e controllo non sono determinati dall'organismo stesso, bensì dalla legge che ne indica i compiti e dall'organo dirigente che nel modello di organizzazione e gestione definisce gli aspetti relativi al funzionamento compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza (art. 6, commi 1 e 2 d.lgs. n. 231/2001).
- Quanto alla qualifica come **responsabile**: l'OdV non può essere considerato tale in quanto non si tratta di ente distinto dal titolare. Nel caso dell'OdV, eventuali omessi controlli in ordine all'osservanza dei modelli predisposti ricadono semplicemente sull'ente stesso.

In conclusione…

"Sulla base delle valutazioni sopra riportate, si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongono siano interni o esterni, debba essere considerato **"parte dell'ente".**

Il suo ruolo - che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di "autonomi poteri di iniziativa e controllo" - si svolge **nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione dei modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti.**

Lo stesso ente, nell'ambito dei compiti e delle funzioni affidate all'OdV, designerà - nell'ambito delle misure tecniche e organizzative da porre in essere in linea con il principio di accountability (art. 24 del Regolamento) - **i singoli membri dell'OdV quali soggetti autorizzati** (artt. 4, n. 10, 29, 32 par. 4 Regolamento; v. anche art. 2-quaterdecies del Codice).

Tali soggetti, in relazione al trattamento dei dati degli interessati, dovranno attenersi alle istruzioni impartite dal titolare affinché il trattamento avvenga in conformità ai principi stabiliti dall'art. 5 del Regolamento.

Lo stesso titolare sarà tenuto ad adottare le misure tecniche e organizzative idonee a garantire la protezione dei dati trattati, assicurando contestualmente all'OdV l'autonomia e l'indipendenza rispetto agli organi di gestione societaria nell'adempimento dei propri compiti secondo le modalità previste dalla citata normativa".

Responsabilità penale dei membri dell'OdV

La qualifica giuridica dell'OdV si riflette anche sulla possibile sussistenza di responsabilità in capo al medesimo. Si ritiene non sia possibile riconoscere in capo all'OdV una posizione di garanzia da cui far discendere un obbligo giuridico di impedire la commissione di reati o la perpetrazione di trattamenti illeciti di dati, in quanto semplicemente destinatario dell'obbligo di **vigilare** sul rispetto delle procedure dettate dal Modello.

Pertanto**, l'Organismo non risponde penalmente ai sensi dell'art. 40/2 c.p. per i reati commessi nell'interesse o a vantaggio dell'ente**, in quanto questa può esistere solo ove sia individuabile una fonte – normativa o contrattuale – dell'obbligo giuridico.

Il Parere del Garante, sul punto, riporta che "*non può essere imputata una responsabilità penale in ordine all'eventuale commissione di reati rilevanti ai sensi del d.lgs. n. 231/2001 nel caso di omessi controlli, posto che tale Organismo, pur avendo funzioni di vigilanza e controllo,* ***non è dotato di alcun potere impeditivo nei confronti degli eventuali autori del reato****, così che, anche in caso di inerzia dell'OdV, la responsabilità ricade sull'ente che non potrà avvalersi della scriminante di cui all'art. 6/1 d.lgs. 231/2001*".

"*Similmente, l'OdV non ha l'obbligo di denuncia all'Autorità giudiziaria in relazione agli illeciti di cui viene a conoscenza a causa e nell'esercizio delle sue funzioni (obbligo che grava invece sull'ente all'uopo informato dall'OdV) né è l'organismo investito di poteri disciplinari nei confronti degli autori degli illeciti, poteri che rimangono in capo all'ente ai cui vertici aziendali l'OdV è tenuto a segnalare le violazioni accertate, proponendo, al contempo, l'adozione delle necessarie sanzioni*".

- E' la società stessa, in quanto titolare del trattamento, che è sottoposta al dovere di integrare gli strumenti di ***compliance*** **normativa in ambito *privacy*** e **i modelli di gestione e organizzazione contemplati dagli artt. 6 e 7 del D.lgs. 231/2001**, idonei ad escludere la c.d. "colpa organizzativa" in capo all'ente per reati commessi da soggetti che rivestono funzioni apicali o subordinate al suo interno.

- **L'impostazione comune è fondata sulla gestione del rischio al fine di prevenire la commissione di reati, in un caso, e di violazioni dei diritti e delle libertà dei soggetti i cui dati vengono trattati, nell'altro.**

Conseguenze:

- necessità per le imprese di rivedere con una certa urgenza gli strumenti di *compliance* interna per conformarsi agli oneri e agli obblighi imposti dal Legislatore Europeo in chiave di tutela della *privacy*.

- analisi volte alla **mappatura dei rischi** che l'esercizio dell'attività può comportare; rischi che, in relazione al GDPR, riguardano le violazioni nel trattamento dei dati, e, rispetto al Decreto 231, la commissione di reati presupposto nell'interesse o a vantaggio dell'ente.

Ottica del "prevenire è meglio che curare", in entrambi i settori.

→ analogia tra i profili connessi alla responsabilità dell'ente che colposamente abbia omesso di predisporre una struttura societaria funzionale ad evitare la commissione di *data breaches* o di reati ex D.Lgs. 231/2001, la quale, in entrambi i casi, determina l'irrogazione di pesanti sanzioni pecuniarie nei confronti dell'impresa e viene invece esclusa, o attenuata, qualora l'ente o il titolare del trattamento abbia predisposto adeguate misure di prevenzione.

→ In materia di privacy: **responsabilità come accountability – eventuali sanzioni di tipo amministrativo irrogate dal Garante della Privacy**

→ In materia di 231: **responsabilità a titolo di "colpa organizzativa" – eventuale responsabilità ex d.lgs. 231/2001 riconosciuta dal Giudice penale**

Le previsioni del Decreto 231, benché funzionali ad esonerare l'ente da responsabilità per reati commessi nel suo interesse e/o a suo vantaggio, dunque, erigono un **sistema di tutela "indiretta" anche per i diritti e le libertà dei titolari di dati personali soggetti a trattamento, andando così ad integrare gli adempimenti previsti dal GDPR in quest'ottica.**

L'OdV entra in gioco in quanto ha l'onere di vigilare sull'integrità ed efficacia COMPLESSIVE dei modelli aziendali.

Art. 24 bis: "Delitti informatici e trattamento illecito di dati"

- La società risponde quando viene commesso all'interno della stessa uno dei reati tassativamente elencati, qualora questo sia commesso nell'interesse o a vantaggio della persona giuridica, da soggetti che rivestono al suo interno funzioni apicali o non apicali.
- La responsabilità penale continua ad essere personale (art. 27 Cost.), in quanto l'autore di un reato non può che essere una persona fisica, dipendente della società.
- I delitti strettamente riguardanti la privacy (artt. 167 ss. c.p.) **non figurano tra i reati presupposto**.
- **La perpetrazione dei reati che rientrano nel catalogo, tuttavia, presuppone un data breach in quanto implica ugualmente un illecito/scorretto trattamento dei dati – ragion per cui le due diverse compliance sono strettamente interconnesse.**

ELENCO DEI REATI PRESUPPOSTO

- **Accesso abusivo ad un sistema informatico o telematico** (art. 615-ter c.p.): si configura quando un soggetto si introduce in un sistema informatico protetto da misure di sicurezza o vi si mantiene senza il consenso del titolare. La norma intende tutelare la riservatezza del c.d. domicilio informatico.

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (art. 615-quater c.p.): si configura quando, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente taluno si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza. In questo caso viene anticipata notevolmente la soglia della tutela penale, andando a proteggere già i codici di accesso.

- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** (art. 615-quinquies c.p.): la norma tutela il corretto funzionamento delle tecnologie informatiche e la loro salvaguardia, ad esempio, dai programmi-virus.
- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (art. 617-quater c.p.): viene tutelata la riservatezza delle comunicazioni informatiche e la sicurezza stessa del sistema informatico o telematico, in modo che non venga violato il rapporto fiduciario con il gestore della rete.
- **Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche** (art. 617-quinquies c.p.): la norma tutela la riservatezza, la segretezza e la libertà delle comunicazioni, informazioni o notizie trasmesse per via telematica o elaborate da sistemi informatici.

- **Reati di danneggiamento informatico**, previsti dagli artt. 635-bis, 635-ter, 635-quater e 635-quinquies c.p.. Essi presentano alcuni elementi costitutivi comuni: tutti questi reati sono posti a tutela della integrità dei beni informatici, come dati, informazioni e programmi, e del domicilio informatico e vanno ad individuare diverse condotte penalmente sanzionate, come la distruzione, il deterioramento, alterazione o soppressione di informazioni, dati, programmi informatici o sistemi informatici.

- **Documenti informatici** (art. 491-bis c.p.). Qualora le condotte previste in materia di "*Falsità in atti*" riguardino un documento informatico, pubblico o privato, avente efficacia probatoria, si applicano le disposizioni concernenti il falso in atti pubblici e in scritture private. Occorre inoltre precisare che per "documento informatico" deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica** (art. 640 quinquies c.p.)

WHISTLEBLOWING

- Importante accennare al Whistleblowing, sistema di segnalazione agli organi aziendali, da parte di organi ad essa appartenenti, di comportamenti illeciti
- Necessario assicurare al segnalante la **riservatezza** per evitare ritorsioni, da bilanciare con il diritto all'accesso ai dati da riconoscere al "colpevole" del comportamento illecito.
- Il modello organizzativo dovrà prevedere (l. 179/2017):
  - Uno o più canali che consentano a coloro che rappresentano o dirigono l'ente di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di **condotte illecite o di violazioni del modello di organizzazione e gestione dell'ente**
  - Almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche**, la riservatezza dell'identità del segnalante**
  - Misure idonee a tutelare la riservatezza dell'informazione e l'identità del segnalante, nei limiti in cui l'anonimato e la privacy siano opponibili per legge.