GIURISPRUDENZA PENALE

I modelli 231 e la *compliance* aziendale sulla tutela dei dati personali. Aspetti comuni e divergenze a quattro anni di distanza dall'entrata in vigore del GDPR.

di ***Davide Costa***

Sommario. 1. Premessa. - **2.** L'approccio basato sulla valutazione dei rischi. - **3.** I codici di condotta. - **4.** I protocolli di formazione delle decisioni dell'organizzazione. - **5.** Gli organismi di vigilanza e le condotte successive alla violazione dei modelli. - **6.** Le eterogeneità tra i modelli. - **7.** Conclusioni.

1. Premessa.

Ad ormai quattro anni dalla pubblicazione del Regolamento Generale sulla Protezione Dati n. 679/2016 (di seguito GDPR), per le organizzazioni imprenditoriali si è resa sempre più imprescindibile la determinazione di un sistema di adempimenti volti ad adeguare i trattamenti dei dati personali delle persone fisiche ai principi delineati dall'art. 5 dal Regolamento [1].

La necessità di provare l'avvenuto adeguamento della *compliance* aziendale alle nuove prescrizioni privacy ha portato dunque le società a introdurre una sorta di "dossier *privacy*", il quale racchiude tutti gli adempimenti necessari ad assicurare la riservatezza ed il più elevato grado di tutela per i dati personali da esse trattati.

In particolare, a mente del principio di "responsabilizzazione" ("*accountability*"), colonna portante dell'impianto strutturale del GDPR, gli enti – nella persona del titolare del trattamento (infelice traduzione del termine *"data controller"*) - sono tenuti a predisporre ed implementare modelli di gestione aziendale ispirati ai criteri di "*risk - based approach*"- che potremmo definire "Modelli organizzativi *privacy*" - che tengano quindi conto dei rischi emergenti allorquando l'attività svolta si interfacci con operazioni su dati personali riconducibili alla definizione di "*trattamento*" ("*processing*") fornita dall'art. 4 n. 2) del Regolamento [2].

---

[1] In particolare, tra i principi cardine che regolano il trattamento dei dati personali contemplati dal GDPR si individuano quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza

[2] Ai sensi del GDPR, per "trattamento" si intende "*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*".

Si profila pertanto come inevitabile, quanto meno in astratto, il parallelismo tra i suddetti 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.
Invero, le due discipline manifestano tratti omogenei sotto differenti aspetti, sia come principi ispiratori che come contenuti specifici dei modelli, delineati secondo un'impostazione 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.
Allo stesso modo, non può tuttavia ignorarsi l'esistenza di numerose divergenze tra i due contesti, sia con riferimento alle peculiari finalità perseguite dalla normativa in materia di *privacy,* sia in relazione all'entità degli obblighi sussistenti in capo agli enti.
Occorre pertanto procedere ad una determinazione chiara delle affinità e delle differenze intercorrenti tra i due modelli, in modo da eliminare potenziali "zone grigie" tra le discipline e delimitare così gli ambiti di applicazione della normativa in materia di tutela dei dati personali e della legislazione sulla responsabilità degli enti dipendente da reato.

2. L'approccio basato sulla valutazione dei rischi.
In primo luogo, non può ignorarsi che entrambi i modelli puntano a prevenire il rischio di un trattamento illecito dei dati personali.
Il sistema di controllo ex D.Lgs 231, pur non prevedendo espressamente i reati contro la *privacy* di cui agli artt. 167 e seguenti del D.lgs. 196/2003 tra quelli in grado di determinare la responsabilità dell'ente, individua, invero, alcuni illeciti la cui perpetrazione presuppone, in numerosi casi, un *data breach*.
Si pensi, ad esempio, ad alcuni reati informatici quali quelli di cui agli artt. 615 *ter, 617 quinquies* e 635 *ter* c.p., considerati delitti presupposto dall'art. 24 *bis* del Decreto. Non può infatti negarsi l'elevato tasso di rischio per la riservatezza e l'integrità dei dati personali determinato dall'accesso abusivo ad un sistema informatico, così come dall'installazione di software (ad esempio il c.d. *trojan*) e altri programmi in grado di acquisire fraudolentemente comunicazioni informatiche o di danneggiare sistemi operativi,
Pertanto, le previsioni del Decreto 231, benché funzionali ad esonerare l'ente da responsabilità per reati commessi nel suo interesse e/o a suo vantaggio, 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.

Per quanto attiene alle specifiche omogeneità tra i due modelli sul piano strutturale, una prima connessione può individuarsi nella 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*. Orbene, tale necessità sottende certamente sforzi di natura economica e tecnica del tutto analoghi a quelli richiesti per l'aggiornamento dei modelli 231 nei casi di introduzione di nuovi reati tra quelli idonei a impegnare la responsabilità dell'ente, ultimi dei quali i delitti tributari previsti dagli artt. 2, 3, 8, 10 ed 11 del D.lgs. 74/2000 [3].
Muovendo oltre, come anticipato sopra, il principale elemento comune alle due discipline è indubbiamente costituito dalla centralità delle 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.
Un simile approccio, basato sull'assunto per cui "prevenire è meglio che curare", consente altresì di riportare sotto un comune denominatore 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 dl trattamento abbia predisposto adeguate misure di prevenzione.
Responsabilità che, giova ribadire, nella normativa in materia di *privacy* trova il proprio fondamento nella nozione di "*accountability",* mentre emerge in qualità di "colpa organizzativa" per quanto riguarda il Decreto 231.
Il *risk – based assessment* che accomuna i due impianti legislativi si evince dalla corrispondenza tra alcuni degli adempimenti previsti dal GDPR con quelli che costituiscono il contenuto dei modelli *ex* artt. 6 e 7 del Decreto 231.
In via generale, si pensi al rapporto di coincidenza tra gli obblighi in capo al titolare e al responsabile del trattamento previsti dagli artt. dall'art. 24 e 32 del GDPR - che impongono a questi ultimi di mettere in atto le misure tecniche e organizzative adeguate e proporzionate ai rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso ai dati personali al fine di garantire un idoneo livello di sicurezza e per poter dimostrare che il trattamento è effettuato conformemente al regolamento - e l'onere in capo all'ente di adottare ed

[3] La Legge n. 157 del 19/12/2019 di conversione del D.L. 26/10/2019, in attuazione della direttiva UE n. 1371/2017 (c.d. P.I.F.), ha infatti introdotto l'art. 25*quinquiesdecies* al Decreto 231, annoverando i reati tributari sopra indicati tra le fattispecie presupposto della responsabilità dell'ente.

efficacemente attuare, ad opera del proprio organo dirigente, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi, la cui prova esonera l'ente dalla responsabilità per il reato commesso (art. 6 c. 1 lett. A) del Decreto 231). Più specificatamente, l'art. 6 c. 2 lett. A) del Decreto prevede che l'attività di mappatura ed individuazione delle aree d'attività più sensibili e dei reati che potrebbero essere commessi sia *condicio sine qua non* dell'adeguatezza del modello.
Nell'ottica del GDPR, la centralità dell'analisi del rischio, oltre ad emergere nei predetti obblighi di cui agli artt. 24 e 32, può evincersi altresì nel contesto del c.d. "*Data Protection Impact Asssessment",* ossia nella valutazione d'impatto prevista dall'art. 35 che il titolare del trattamento deve effettuare "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".
Nel panorama dei comportamenti riconducibili all'approccio basato sul rischio che l'ente deve attuare per conformarsi tanto alla normativa *privacy* quanto al Decreto 231 rientrano inoltre il riesame, e l'eventuale aggiornamento, dei modelli, attraverso procedure di revisione delle misure tecniche e organizzative e delle garanzie necessarie per soddisfare i requisiti del regolamento nel corso del trattamento (artt. 24 e 35 GDPR) ovvero per assicurare l'efficace attuazione del modello a seguito di violazioni o di mutamenti nell'organizzazione (art. 7 c. 4 Decreto 231).

3. I codici di condotta.
Merita altresì sottolineare come entrambi gli impianti normativi prevedano che l'adeguatezza dei modelli ed il rispetto degli obblighi in capo all'ente ed al titolare del trattamento possono essere dimostrati mediante l'adesione a determinati codici di condotta (c.d. "codici etici") elaborati dagli organismi rappresentativi degli enti o dei titolari del trattamento ai sensi dell'art. 40 del GDPR.
Per completezza, è necessario che, ai fini della *compliance* normativa, dall'adesione ai codici di condotta vengano distinte le certificazioni rilasciate da appositi organismi a comprova della determinazione di sistemi organizzativi idonei a prevenire illeciti penali o a danno dei dati personali.
Tali certificazioni, infatti, presentano un diverso grado di efficacia in relazione ai due modelli.
Invero, se gli artt. 24 e 32 del GDPR prevedono espressamente che il titolare del trattamento può dimostrare l'osservanza degli obblighi e la predisposizione di garanzie appropriate per la tutela dei dati personali mediante il ricorso ai meccanismi di certificazione disciplinati dall'art. 42 del Regolamento (si pensi, ad esempio, alla certificazione ISO 27001, che ad oggi

rappresenta lo standard internazionale più rilevante di sicurezza delle informazioni e definisce le "*best practices",* i requisiti logici, fisici e organizzativi necessari per impostare e gestire un sistema di gestione della sicurezza delle informazioni) [4].
Viceversa, è ormai principio assodato in giurisprudenza quello per cui le certificazioni rilasciate da istituti quali la International Standard Organization non possono ritenersi equivalenti ai modelli 231 ai fini di esonerare l'ente dalla responsabilità per reati commessi nel suo interesse e/o a suo vantaggio.[5]

4. I protocolli di formazione delle decisioni dell'organizzazione.
Tornando ai punti di contatto tra i due modelli ispirati al *risk-based approach*, deve constatarsi che entrambe le legislazioni si preoccupano di indicare (se non anche prescrivere obbligatoriamente) ai propri destinatari di adottare protocolli standardizzati per la formazione e l'esecuzione delle decisioni dell'ente e/o del trattamento dati che garantiscano una conformità alla normativa, sia essa quella penale piuttosto che quella in materia di *data protection,* che sussista già a monte dell'intero procedimento decisionale.
Mentre il Decreto 231, tuttavia, si limita a suggerire all'ente di "*prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*" (art. 6 c. 2 lett. B), rimettendo agli organi sociali la determinazione del contenuto di tali protocolli (che certamente variano in relazione al tipo di attività svolta e ai reati commettibili in seno ad essa), il Legislatore Europeo ha individuato in modo specifico, generale e valido per tutti i trattamenti, le misure che i *controllers* ed i *processors* devono prendere per assicurare appropriata tutela ai dati dell'interessato.
In particolare, l'art. 25 del GDPR, nel prevedere che il titolare metta in atto misure tecniche e organizzative che "*per impostazione predefinita"* sono in grado di garantire che i dati siano trattati nel rispetto dei principi del regolamento, fornisce anche una classificazione specifica di tali misure, che vengono individuate nella pseudonimizzazione, nella minimizzazione, nella

[4] Ai sensi dell'art. 42, "*Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario*".
[5] Sul punto v. Cass. Pen. Sez. VI, n. 41768 del 13/09/2017, in materia di infortuni sul lavoro e reati ambientali, secondo cui "*non possono essere ritenuti equivalenti ai modelli richiesti dal D.Lgs. n. 231 del 2001, perchè non contenevano l'individuazione degli illeciti da prevenire unitamente alla specificazione del sistema sanzionatorio delle violazioni del modello e si riferivano eminentemente al controllo della qualità del lavoro nell'ottica del rispetto delle normative sulla prevenzione degli infortuni sul lavoro o degli interessi tutelati dai reati in materia ambientale".*

previsione di limiti all'accesso nonché di tutti gli altri provvedimenti che possano garantire che vengano solo i dati personali necessari per ogni specifica finalità del trattamento.
I puntuali adempimenti così individuati dal Legislatore comunitario, che il titolare del trattamento deve "a priori" attuare prima di procedere a qualsiasi operazione sui dati personali, costituiscono manifestazione dei principi di "*privacy by design*" e "*privacy by default*" espressi dall'art. 25 del GDPR.
A ciò devono peraltro aggiungersi le misure "suggerite" dall'art. 32 del Regolamento nell'ottica di facilitare i destinatari degli obblighi nella predisposizione delle misure tecniche adeguate ai rischi per la sicurezza dei dati trattati; dette misure, invero, ricomprendono "*a) la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*".
Le prescrizioni del Regolamento acquisiscono, peraltro, una specificità ancora maggiore con riferimento alla già menzionata valutazione d'impatto che deve obbligatoriamente precedere i trattamenti di dati in situazioni particolarmente delicate.[6]

5. Gli organismi di vigilanza e le condotte successive alle violazioni dei modelli.

Le affinità tra la legislazione sulla responsabilità delle persone giuridiche e quella in ambito *privacy* non si limitano alla determinazione di modelli improntati sul medesimo *risk - based approach*.
Invero, ulteriori corrispondenze emergono altresì sul versante degli organismi di controllo previsti dal Decreto e dal Regolamento e sulla rilevanza delle misure adottate a seguito di una violazione dei modelli stessi.
In merito al primo aspetto, sia il Decreto 231 che il GDPR muovono dal principio secondo cui, rispettivamente, i modelli di prevenzione dei reati e le misure organizzative a tutela della liceità dei trattamenti dati non possono

[6] L'art. 35 del Regolamento prevede, infatti, che la valutazione d'impatto debba contenere almeno: "a*) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; d)le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione*".

considerarsi adeguati in assenza di idonei centri di imputazione di compiti di sorveglianza affinché gli strumenti di *compliance* siano adottati ed efficacemente implementati.
Tali centri di imputazione vengono identificati nell'Organismo di Vigilanza (di seguito Odv), in un caso, e nel Responsabile della Protezione Dati ("*Data Protection Officer* – di seguito DPO*)*, nell'altro.
Entrambi gli organismi presentano omogeneità non solo per la posizione di terzietà rispetto all'organizzazione imprenditoriale, ma anche in relazione all'autonomia ed ai poteri di controllo assegnati loro ed ai flussi di informazione che l'ente o i protagonisti del trattamento dati devono assicurare con i medesimi organismi, aventi ad oggetto, in particolare, le comunicazioni di eventuali violazioni dei modelli o dei rischi di commissione di reati o di *data breaches* (art. 6 c. 2 lett. B) del Decreto 231 e artt. 37 e 38 GDPR).
Le autorità di sorveglianza istituite dal GDPR e dal Decreto 231 non sono, comunque, pienamente convergenti.
Occorre infatti sottolineare che, nuovamente, il GDPR si preoccupa di determinare in maniera più coincisa e puntuale i poteri e le incombenze attribuite al DPO di quanto faccia il D.lgs. 231 per l'OdV.[7]
Inoltre, mentre la nomina di un OdV *ex* D.lgs. 231/2001 è necessaria al fine di soddisfare i requisiti minimi di adeguatezza del sistema organizzativo per tutti gli enti, il DPO, ai sensi dell'art. 37 c. 1, deve essere individuato soltanto all'interno di determinati contesti ovvero per particolari tipologie di operazioni su dati.
Infine, malgrado l'affinità delle funzioni di controllo sul corretto funzionamento dei modelli, la necessità di prevenire conflitti di interessi rende apparentemente inconciliabili le posizioni del DPO e dell'OdV: quest'ultimo, infatti, ben potrebbe trovarsi ad effettuare operazione su dati personali (ad es. di dipendenti dell'impresa) in qualità di responsabile del trattamento, e dovrà pertanto essere anch'esso, a sua volta, assoggettato alla vigilanza del DPO.

Come sopra anticipato, altro punto di coincidenza tra i modelli può individuarsi nelle conseguenze delle condotte tenute dall'ente e dal titolare del trattamento qualora vengano riscontrate violazioni che abbiano determinato la commissione di reati presupposto o *data breaches* in danno degli interessati.

[7] L'art. 39 GDPR specifica l'elenco delle attribuzioni del DPO, tra cui rientrano obblighi di informazione e formazione verso titolare e responsabile del trattamento, la sorveglianza sul rispetto del Regolamento, il rilascio di pareri, la cooperazione con l'autorità di controllo per tutte le questioni connesse al trattamento.

In entrambi i casi, infatti, l'entità delle, gravose, sanzioni pecuniarie potrà attenuarsi nei casi in cui il responsabile abbia provveduto ad eliminare le conseguenze dannose del reato o del trattamento illecito dei dati (o ad attivarsi in tal senso) e a risarcire i danni ai soggetti che abbiano subito conseguenze pregiudizievoli (v. art. 12 Decreto 231 e art. 83 c. 2 GDPR).

6. Le eterogeneità tra i modelli.

Le numerose, possibili, intersecazioni tra i modelli di cui all'art. 6 del Decreto 231 e le strutture organizzative in ambito *privacy* non devono, tuttavia, distogliere l'attenzione dalle rilevanti divergenze di fondo che connotano i due sistemi normativi, in parte già accennate nei passaggi precedenti.

In primo luogo deve infatti ribadirsi la maggiore specificità ravvisabile nelle previsioni del GDPR in merito alla struttura sulla quale devono improntarsi i modelli di organizzazione a protezione dei dati personali, diversamente dal D.lgs. 231/2001, che impone sì un contenuto minimo inderogabile dei modelli, lasciando però un più ampio spazio all'ente in relazione all'individuazione delle attività a rischio, alla gestione delle risorse economiche e all'adempimento degli obblighi di informazione all'OdV.

Una seconda, fondamentale, differenza, risiede inoltre nella portata applicativa dei modelli e nella loro capacità "deresponsabilizzante" per l'ente e per il titolare del trattamento.

Invero, ai sensi del D.lgs. 231/2001, l'ente risponderà solo dei reati commessi *nel suo interesse* e/o *a suo vantaggio* da coloro che rivestono posizioni di vertice al suo interno ovvero da chi è sottoposto alla direzione dei primi. Logica conseguenza di tale previsione sta nell'impossibilità di addebitare all'ente la colpa organizzativa in caso di illeciti perpetrati a suo danno, ovvero nel suo interesse o a suo vantaggio da soggetti estranei all'organizzazione imprenditoriale non sottoposti a direzione o vigilanza di coloro tramite i quali si manifesta la volontà della persona giuridica.

Diversamente, il GDPR, la cui *ratio* risiede nella sola tutela dei dati personali delle persone fisiche e non anche nella necessità di evitare che la persona giuridica sia utilizzata come strumento di commissione di reati rimanendo impunita, contempla l'assoggettabilità a sanzioni pecuniarie del titolare del trattamento in tutti i casi in cui gli sia addebitabile una violazione dei dati personali da lui processati derivante dall'assenza, o inefficacia, di adeguati strumenti di *data protection*. Ciò anche qualora essa si concretizzi in un danno per l'ente (si pensi ai casi di *cybercrime* che, oltre al furto di dati personali, determinano un danneggiamento anche i sistemi di IT della società stessa), ovvero qualora il *data breach* sia posto in essere da soggetti estranei ad esso.

Infine, non può ignorarsi la differente portata scriminante attribuita ai modelli 231, i quali, se adottati ed efficacemente attuati, consentono di assolvere l'ente dai reati commessi dai membri della propria organizzazione, seppur a

mente della diversa intensità dell'onere probatorio nel caso di reati commessi da soggetti apicali.[8]
Viceversa, il GDPR non contiene una declaratoria così netta, e lascia dunque aperti spiragli di responsabilizzazione anche del titolare del trattamento che abbia provveduto ad attuare un sistema di *compliance* in ambito *privacy* astrattamente idoneo a prevenire violazioni del Regolamento, potendo tale condotta, comunque, essere presa in considerazione dall'autorità nella procedura di commisurazione della sanzione ai sensi dell'art. 83.

7. Conclusioni.

Trasferendo le suesposte osservazioni sul piano pratico, risulta indubbiamente utile per tutte quelle organizzazioni, commerciali e non, destinatarie delle due normative, che negli anni hanno posto in essere ed attuato modelli organizzativi al fine di prevenire la commissione di reati presupposto *ex* D.lgs. 231/2001, recuperare il contenuto degli stessi e verificare in che misura essi siano adattabili alla tutela dei dati personali.
Simile scelta appare, peraltro, particolarmente opportuna in relazione alla mappatura dei rischi connessi all'ambito ICT dell'impresa, con specifica attenzione ai reati informatici, la cui portata offensiva, come evidenziato sopra, si estende spesso alla sicurezza ed integrità dei dati personali.
La ricerca di un coordinamento tra i due modelli, e, aspetto non secondario, l'obiettivo di contenere i costi che derivano dall'adozione di adeguati sistema di *compliance,* non devono tuttavia portare alla convinzione che il modello organizzativo 231 esaurisca in maniera completa tutti gli aspetti di programmazione e di formazione imposti dal GDPR, attesa anche la sostanziale differenza intercorrente tra i soggetti preposti al controllo sul corretto funzionamento dei modelli adottati, *rectius* l'OdV e il DPO.
Sarà dunque rimesso ad ogni realtà imprenditoriale, tenuto conto del tipo di attività svolta e dei rischi annessi, valutare se la struttura di fondo del modello adottato per la prevenzione dei reati presupposto sia eventualmente compatibile anche per l'adempimento delle obbligazioni previste in ambito *privacy,* ovvero se lo stesso debba essere aggiornato ed integrato per assicurare il massimo grado di salvaguardia dei dati soggetti al trattamento e conformarsi così ai principi statuiti dal Legislatore Europeo..

[8] L'art. 6 del D.lgs. 231/2001, in relazione ai reati commessi dagli apicali, rimette infatti in capo all'ente l'onere della prova dell'adozione e del corretto funzionamento del modello di organizzazione.