Rivista di contabilità pubblica riconosciuta di carattere culturale dal Comitato interministeriale di cui al d.P.C.M. 9 marzo 1957
Amministrazione e Contabilità dello Stato e degli enti pubblici
Fondata e diretta da Salvatore Sfrecola
Rivista scientifica riconosciuta dall'ANVUR nell'area 12 - ISSN 0393 - 5604
2021 - Anno XLII

LA VIGILANZA EX D.LGS. 231/01 E LA PRIVACY GDPR

dell'Avv. Vincenzo Candido Renna - *Corporate Ethics & Compliance Specialist* Cultore di diritto amministrativo: Università degli Studi "A.Moro" Bari.

ABSTRACT: Le questioni alle quali si cercherà di rispondere afferiscono ad un tema di particolare interesse alla luce delle novità intervenute in merito alla tutela dei dati personali introdotte dal Regolamento (UE) 2016/679 del Parlamento e del Consiglio europeo del 27.04.2016, di seguito denominato solo come GDPR (*General Data Protection Regulation)* e dal conseguente D.lgs. 10 agosto 2018 n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 679/16",* il quale ha opportunamente modificato il c.d. Codice della *privacy* (D.lgs. n. 196/03) abrogando e modificando il suo articolato allo scopo di conformarsi alle norme prevalenti del GDPR.

Definito il contesto normativo quale perimetro del nostro ragionamento, mi preme evidenziare che la "riservatezza" non si declina semplicemente nella sfera della "*privacy*", che pur corollario importante non funge da "*matrioska*" rispetto alla prima.

La riservatezza, infatti, specie se coniugata con l'attività di sorveglianza e controllo di un modello di organizzazione conforme al decreto legislativo 231/01, da parte di un Organismo di Vigilanza (in seguito solo "ODV"), assume un valore più ampio rappresentando un metodo di lavoro e uno strumento di gestione di informazioni e di dati.

La gestione implica una preliminare capacità di valutazione ed analisi dei dati allo scopo di pervenire ad una interpretazione aderente alle finalità precipue dell'attività di vigilanza proprie dell'ODV.

Di pari importanza sono le attività di conservazione del dato che si declinano nelle macrocategorie della registrazione, raccolta e dell'archiviazione.

Registrazione e archiviazione che rimandano ai concetti di tempo e spazio oltre che di sicurezza.

Il dato in sé diventa un valore in relazione alla possibilità di mobilità dello stesso e compete all'ODV assumere delle decisioni in riferimento a tale condizione rispetto alle informazioni scaturenti da un processo cognitivo di valutazione, che implica un giudizio di meritevolezza sul punto da parte di quest'ultimo, il dato in sé ha un valore proprio in funzione del livello di protezione che il "gestore" del dato intende attribuirli, sul punto di particolare interesse sono alcune teorie filosofiche tutt'altro che univoche e in continua evoluzione.[1]

Al momento il ragionamento proposto nei paragrafi che seguono sconta la mancanza di giurisprudenza sull'argomento esponendo l'opinione rappresentata, in questa breve nota, alla possibilità di future e auspicabili conferme ovvero a sempre possibili censure e smentite.

ABSTRACT: The questions to which we will try to answer relate to a topic of particular interest in light of the innovations regarding the protection of personal data introduced by Regulation (EU) 2016/679 of the European Parliament and Council of 27.04.2016, hereinafter referred to as only as GDPR (General Data Protection Regulation) and by the consequent Legislative Decree of 10 August 2018 n. 101 "Provisions for the adaptation of national legislation to the provisions of EU regulation 679/16", which appropriately modified the so-called Privacy Code (Legislative Decree No. 196/03), repealing and

[1] Nella sua formulazione classica (W. Sellars, Empirismo e filosofia della mente [1956], trad. it., Einaudi, Torino 2004) la critica del mito del dato suona così: se voglio poter usare i dati come base per una teoria, allora questi dati non sono indipendenti dalla teoria. Se viceversa pretendo che i dati siano indipendenti dalla teoria, allora non potrò mai usare un singolo dato per confermare o smentire una teoria. Come risultato: se voglio che una ontologia serva per una epistemologia, bisogna che l'epistemologia costruisca l'ontologia. Il discorso fila ma non tiene perché una ontologia costruita da una epistemologia è una epistemologia e non una ontologia, e una epistemologia che conosce una epistemologia non è nemmeno una epistemologia. Sostenendo che il dato è un mito, introduciamo implicitamente un mito ancora più insidioso: se vuoi che una ontologia serva per una epistemologia, bisogna che l'epistemologia informi l'ontologia; ma una ontologia informata da una epistemologia è una epistemologia – uno strano sapere cui, curiosamente, non corrisponde un essere. Ma una epistemologia informata da una epistemologia non è nemmeno una epistemologia: è riflessione o introspezione. Messo in questi termini sembra assurdo, ma basterà pensare a quanti sostengono che «non esistono soggetto e oggetto, esiste solo la relazione tra soggetto e oggetto». Bene, questi filosofi stanno dicendo, con il peggior argomento del mondo, che le ostriche non esistono e in effetti non esistono neanche loro, ma esiste solo un «mangiare l'ostrica». Buon appetito, ma resta misterioso perché, poco dopo, sarà chiesto proprio a loro, e non – per esempio – all'ostrica, di pagare il conto (sul peggior argomento del mondo: D. Stove, Idealism: a Victorian Horror Story (Part Two), in Id., The Plato Cult and Other Philosophical Follies, Blackwell, Oxford 1991, pp. 135-178.

modifying its article in order to comply with the prevailing rules of the GDPR.

After having defined the regulatory context as the perimeter of the reasoning, it is important to point out that "confidentiality" is not simply expressed in the sphere of "privacy", which although an important corollary does not act as a "matryoshka" compared to the first.

In fact, confidentiality, especially if combined with the surveillance and control activity of an organization model compliant with legislative decree 231/01 by a Supervisory Body (hereinafter only the SB), takes on a wider value, representing a working method and an information and data management tool.

The management implies a preliminary ability to evaluate and analyze the data in order to achieve an adherent interpretation to the main purposes of the supervisory activity of the SB.

Of equal importance are the data conservation activities which are divided into the macro-categories of registration, collection and archiving.

Recording and archiving that refer to the concepts of time and space as well as safety.

The data in itself becomes a value in relation to its possibility of mobility, the SB must make decisions in reference to this condition with respect to the information arising from a cognitive evaluation process, which implies a judgment of merit on the point by the latter. The data itself has its own value according to the level of protection that the "manager" of the data intends to attribute to it, on the point of particular interest there are some philosophical theories that are far from unique and in continuous evolution.

At the moment, the reasoning proposed in the following paragraphs discounts the lack of jurisprudence on the subject by exposing the opinion represented, in this short note, to the possibility of future and desirable confirmations or to always possible complaints and denials…

Sommario: 1. GDPR e D.lgs. 231/01; 2. ODV 231 e GDPR; 3. I flussi di comunicazione da e verso l'ODV; 4. Conclusioni.

1. GDPR e D.lgs. 231

Il GDPR prevede norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Il Regolamento protegge, dunque, i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali e fa sì che la libera circolazione dei dati personali nell'Unione non possa essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**.**

Di particolare rilievo è il passaggio da un impianto di tipo prescrittivo/autorizzatorio e da una concezione quasi "*dominicale"* del dato personale riveniente dal precedente sistema normativo regolato dalla Direttiva 95/46/CE e dal d.lgs. 30.06.2003, n. 196 (che richiedeva il consenso dell'interessato per il trattamento del dato personale e, al verificarsi di determinati presupposti, un sindacato *ex ante* da parte del Garante per la protezione dei dati) ad un approccio fondato sul rischio, che favorisce la libera circolazione dei dati.[2]

Il legislatore comunitario insegue il fine ultimo, *per un verso,* di *deburocratizzare* il trattamento dei dati per consentire la mobilità degli stessi e, *per altro verso,* di responsabilizzare il Titolare del trattamento, c.d. principio di *accountability.*

Al Titolare del trattamento si ascrive il dovere (*compliance*) di dimostrare di aver adottato idonee misure tecniche e organizzative per la protezione dei dati personali "gestiti" dalla propria organizzazione e di agire in conformità al GDPR.

Si coglie intuitivamente una stretta somiglianza tra il sistema di *compliance* GDPR e quello previsto dal d.gs. 231/01.

[2] A. De Nicola, L'Organismo di Vigilanza 231 nelle società di capitali, Giappicheli Editore, 2020, cap. VI, 147 ss.; G. Vasintoni, GDPR e Decreto 231: due "sistemi di gestione a confronto", in *Resp. Amm. Enti,* 2019, IV, 61 ss.

Anche in quest'ultimo sistema, per quanto diversamente orientato, incombe all'Ente, allo scopo di conseguire l'esimente da responsabilità, l'onere di provare di aver efficacemente adottato e attuato un Modello organizzativo idoneo a prevenire la commissione dei reati presupposto.

Altre importanti analogie derivano dall'applicazione in entrambi i sistemi di compliance dell'attività di *risk assessment*[3] ossia:

1. la individuazione dei principali processi/aree aziendali;
2. mappatura e identificazione dei rischi con una rappresentazione chiara e immediata del ventaglio delle minacce cui si può andare incontro;
3. valutazione qualitativa o quantitativa del rischio (*risk* scoring).

L'*assessment* è sempre propedeutico al modello organizzativo da adottare all'interno della propria organizzazione e consente *nel caso* della *compliance* GDPR di predisporre idonee procedure, azioni e presidi atti a tutelare i dati personali e *nel caso* del D.lgs. 231/01 e s.m.i. idonei a prevenire la commissione di uno dei reati presupposto inclusi nel catalogo del Decreto.

I due modelli si incontrano, altresì, sul terreno dei reati informatici (art. 24 – bis del D.lgs. 231/01) e più in generale in tema di *cybersecurity* (d.l. 21.09.2019 n. 105 poi convertito con L. 18.11.2019, n.133).

[3] Il GDPR alla "Sezione 3 Valutazione d'impatto sulla protezione dei dati e consultazione preventiva", "Articolo 35 Valutazione d'impatto sulla protezione dei dati", recita al comma 1: "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, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"
Lo standard ISO/IEC 29134: 2017 "Information technology — Security techniques — Guidelines for privacy impact assessment" fornisce utili linee guida per lo svolgimento della valutazione di impatto sulla protezione dei dati ("**privacy impact assessment"o PIA**), linee guida allineate alle indicazioni fornite dal Gruppo di Lavoro ex art. 29 in tema di Data Protection Impact Assessment (DPIA).
In particolare lo standard ISO 29134 considera la PIA come un processo che deve iniziare prima dell'effettuazione del trattamento dei dati personali, quando vi è ancora la possibilità di indirizzare il trattamento stesso. Tale processo considera anche l'impatto potenziale degli asset utilizzati per il trattamento dei dati quali altri processi, servizi IT e relativa infrastruttura IT (HW, SW, connettività in un'ottica di "privacy by design". Il risultato del processo di valutazione di impatto è quindi un report ("PIA Report").

Il richiamo esplicito delle *policy* GDPR consente al Modello Organizzativo ex D.lgs. 231/01 di fornire la c.d. prova di resistenza rispetto all'ascrivibilità per la c.d. *colpa organizzativa* dei reati presupposto, *per converso* molti presidi di tutela dei dati personali recuperano il lessico penalistico propri dei Modelli 231.

A sublimare questa sinapsi tra i due sistemi di *compliance* sovviene l'istituto del *whistleblowing*[4].

La tutela del *whistleblower* (segnalatore di presunti illeciti) si sostanzia, prima di tutto, nella particolare tutela accordata dalla legge ai dati personali connesse e in qualunque modo riferibili alle segnalazioni, sia dal lato attivo (segnalatore) che dal lato passivo (segnalato); il trattamento degli stessi rientra nell'alveo di pertinenza delle norme della *privacy* – GDPR e D.Lgs. 10.08.2018 n. 101 di recepimento, per cui la procedura del Modello 231 necessariamente nella fase della sua predisposizione si conformerà ai due principi: *data protection by design*[5] e *privacy by default*[6].

2. ODV 231 e GDPR

Le connessioni (sinapsi) tra i due sistemi di *compliance* "GDPR" e "231" non potevano escludere l'organismo di vigilanza (ODV) del Modello Organizzativo ex d.lgs. 231/01 (Mog 231).

4 Il «whistleblowing» è un sistema di segnalazioni di violazioni, da parte del dipendente o di un terzo interessato di un'organizzazione pubblica o privata, che ha il coraggio di denunciare atti corruttivi o irregolarità di cui sia venuto a conoscenza, utilizzando canali sicuri e indipendenti per tutelare la propria identità, essendo messi al riparo da eventuali ritorsioni e discriminazioni, conseguenti la segnalazione. L'istituto disciplinato dalla Legge 30 novembre 2017, n. 179 «Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato». L'istituto è ricompreso, altresì, dall'art. 6, comma 2-bis, 2-ter e 2-quater del D.lgs. 231/01. Da ultimo l'istituto è stato attinto dalla normativa comunitaria, segnatamente: DIRETTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione recepita dalla LEGGE 22 aprile 2021, n. 53 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020. (21G00063) (GU Serie Generale n.97 del 23-04-2021) Entrata in vigore del provvedimento: 08/05/2021.

5 Obbligo del Titolare di valutare l'impatto sul trattamento dei dati sin dalla fase di progettazione della procedura; impatto sul trattamento dei dati sin dalla fase di progettazione della procedura.

6 Obbligo del Titolare di trattare i dati personali limitatamente alle finalità previste e per il tempo strettamente necessario.

L'ODV svolge la funzione essenziale ai fini della efficacia esimente dalla responsabilità amministrativa (penale) del Mog 231 della vigilanza sul funzionamento di quest'ultimo nonché di verificare e monitorare la relativa osservanza e di curarne l'aggiornamento mercé l'esercizio di poteri di iniziativa e di controllo, affidategli all'atto della nomina dall'Organo Dirigente dell'Ente.[7]

Nell'esercizio delle sue funzioni l'ODV riceve e gestisce una mole di informazioni su diverse attività e diversi soggetti esecutori delle stesse o comunque diversi dati personali a questi ultimi collegati.

Dati personali che possono essere associati a informazioni c.d. sensibili[8] ovvero afferente allo *status* giudiziario[9].

Preliminarmente, occorre ascrivere in modo conforme al GDPR la qualificazione giuridica dell'ODV. Sul punto di particolare interesse, attesa la provenienza, il parere del 12 maggio 2020 del Garante per la protezione dei dati personali[10] che esclude la possibilità di

7 A. Addotti e S. Bozzolan, *"La Gestione della Compliance Sistemi normativi e controllo dei rischi",* LUISS University Press 2020, IV, I modelli Organizzativi 231 e la responsabilità da reato degli enti, 97 e ss.

8 Nell'Art.4 comma 1 lettera d, del GDPR, vengono definiti dati sensibili: "I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni filosofiche, religiose o di altro genere, le opinioni politiche, l'adesione a sindacati, partiti, associazioni od organizzazioni a carattere filosofico, religioso, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale." Con l'avvento di Internet, sono entrati a far parte dei dati sensibili anche le informazioni riguardanti la propria identità online, come gli indirizzi e-mail e il numero di telefono e la geo-localizzazione, che fornisce informazioni sui luoghi frequentati.

9 Con l'introduzione del Reg. UE 2016/679, il trattamento dei dati giudiziari deve avvenire soltanto nella ricorrenza di una delle basi giuridiche di cui all'art 6 par. 1 del GDPR e sotto il controllo dell'Autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. L'autorizzazione generale al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici n. 7/2016, alla luce della disciplina applicabile ai medesimi dati contenuta nel Regolamento e nel Codice (art. 10 Regolamento; 2-octies del Codice e art. 21 del d.lgs. n. 101/2018), ha cessato di produrre effetti giuridici alla data del 19 settembre 2018. Il Codice Privacy, come modificato dal D. Lgs 101, prevede ora che **solo una norma di legge possa abilitare al trattamento**, togliendo al provvedimento del Garante la possibilità di porsi come fonte autonoma di legittimazione; tale Decreto Ministeriale tutt'ora manca…

10 Si riportano le conclusioni del **parere U.0017347**: << *… si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongano 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. Tale posizione si intende ricoperta dall'OdV nella sua collegialità, tuttavia, non può prescindersi dalla necessità di definire anche il ruolo che, in base alla disciplina in materia di protezione dei dati personali, deve essere previsto per i singoli membri che lo compongono. Lo stesso ente, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta (ad esempio, l'accesso alle informazioni acquisite attraverso flussi informativi), designerà - nell'ambito delle misure*

riconoscere ai componenti dell'ODV la qualificazione di "Titolare" o "Responsabile" del Trattamento.

Per quanto l'ODV è dotato di autonomia e indipendenza rispetto al vertice aziendale non è possibile riconoscere a quest'ultimo la facoltà di determinare autonomamente le finalità del trattamento dei dati con cui il medesimo entra in contatto in ragione della propria attività. Ritenendo, peraltro, queste ultime collegate da un rapporto di mera strumentalità con le prevalenti finalità relative alla vigilanza e controllo ex decreto legislativo 231.

Oltre alla "Titolarità" del trattamento risulta attinta dalla risposta negativa anche l'altra ipotetica qualificazione: "Responsabile del Trattamento", in quanto quest'ultimo è per il GDPR un soggetto esterno all'Ente e che assume l'incarico solo a seguito di sottoscrizione di un accordo vincolante ex art. 28 GDPR, al contrario l'ODV è, senza dubbio, un organismo (o "ufficio") interno alla compagine dell'Ente.

Con riferimento ai singoli componenti dell'Organismo di Vigilanza in ipotesi di composizione collegiale dell'ODV, ovvero del solo componente nell'ipotesi monocratica, appare attagliarsi senza particolari dubbi la qualificazione di: "Soggetti Autorizzati" e, per questo fine, all'uopo designati ex art. 29 GDPR.[11]

Ecco perché l'Ente titolare, in relazione alla PIA presupposta, ha la facoltà di prescrivere all'ODV l'applicazione e il rispetto di

---

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>>.

[11] Art. 29 *GDPR: trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento<<Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri>>.*

particolari misure tecniche e organizzative atte a garantire la *compliance* al GDPR.

Di particolare importanza, inoltre, appare la relazione tra l'ODV e il DPO [12], la particolare rilevanza della funzione di quest'ultimo ai fini della *compliance privacy* in relazione alle molteplici connessioni con la *compliance* ex Decreto legislativo 231 implicano la necessità di ricomprendere tra i flussi documentali periodici indirizzati all'ODV anche le relazioni periodiche del DPO, anche in relazione alla possibilità di garantire un controllo sui reati informatici.

Per il principio di reciprocità l'ODV 231 dovrà informare con tempestività il DPO in relazione a criticità nell'applicazione della *compliance* GDPR che dovessero essere riscontrate nel corso dell'attività di vigilanza e controllo del Modello organizzativo ex Decreto legislativo 231.

3. I flussi di comunicazione da e verso l'ODV.

[12] L'Art. 39 GDPR elenca i principali compiti del DPO (Responsabile della protezione dei dati):

1. **Il responsabile della protezione dei dati** | DPO | è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento Privacy UE 2016/679 (GDPR), nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento Privacy UE 2016/679 (GDPR), di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il quadro sopra delineato ci consente di evidenziare come il profilo di autonomia e indipendenza propri dell'ODV consentono a quest'ultimo di esercitare le prerogative e facoltà proprie della funzione assumendo la responsabilità in ordine alla gestione dei dati acquisiti nel corso dell'attività di vigilanza e controllo.

L'ODV ai sensi dell'art. 6 co. 2, lett. d) è innanzi tutto destinatario di una serie di informazioni, report e documenti da parte del management e dei dipendenti dell'ente vigilato, per altro verso a sua volta, è tenuto con periodicità annuale ad informare l'Organo Amministrativo e il collegio sindacale mediante sulle attività svolte e, in particolare, sui fatti rilevanti ed eventuali criticità del Modello emerse nella propria attività di vigilanza.

La relazione deve contenere, almeno, le seguenti specifiche informazioni:

• la sintesi dell'attività e dei controlli svolti dall'Organismo di Vigilanza durante l'anno;

• eventuali carenze delle procedure operative attuative delle disposizioni del Modello;

• eventuali nuove aree delle attività dell'Ente a rischio di commissione di reati "231";

• la verifica delle segnalazioni ricevute da soggetti esterni o interni che riguardino eventuali violazioni del Modello e i risultati di tali verifiche;

• le procedure disciplinari e le eventuali sanzioni richieste ed applicate, inerenti le attività a rischio;

• una valutazione generale del Modello, con eventuali proposte di integrazioni e migliorie di forma e contenuto, sull'effettivo funzionamento dello stesso;

• eventuali modifiche del quadro normativo di riferimento;

• un rendiconto delle spese sostenute.

Appare opportuno, se non addirittura indispensabile, che i flussi informativi e le segnalazioni vengano conservate dall'Organismo di Vigilanza in una apposita banca informatizzata – il cui accesso agli altri soggetti aziendali sia puntualmente disciplinato dallo stesso Organismo di Vigilanza – gestita nel rispetto della normativa vigente e, soprattutto, conformemente alla *compliance* aziendale.

Da ciò deriva che l'ODV determina autonomamente ed insindacabilmente l'accessibilità delle informazioni gestite nell'esercizio delle funzioni di vigilanza e controllo del Modello organizzativo ex d.lgs. 231/01.

In questa possibilità discrezionale di negare l'accesso ad alcuni dati al *management* o personale dell'azienda vigilata si innesta la tematica in precedenza trattata del *whistleblowing,* che amplia l'obbligo di riservatezza delle informazioni acquisite dall'ODV a tutela del segnalante dei presunti illeciti.

Un regolamento relativo al funzionamento dell'ODV e la predisposizione di una procedura *ad hoc* per disciplinare modalità e termini di comunicazione di informazioni da e verso l'ODV costituiscono elementi fondamentali e caratterizzanti il Modello Organizzativo ex decreto legislativo 231, che in mancanza rischierebbe di non superare l'eventuale sindacato giurisdizionale circa l'idoneità del Modello ai fini del riconoscimento del valore esimente di quest'ultimo.

4. Conclusioni

L'attività di controllo e vigilanza della *compliance 231* da parte dell'ODV assegna a quest'ultimo il dovere di gestione di una serie di informazioni e documenti afferenti all'organizzazione e alle attività dell'Ente vigilato.

L'ODV è, altresì, "potenziale" destinatario di segnalazioni di "presunti illeciti" da parte dei *whistleblower,* oggetto di autonoma e sintetica trattazione nel precedente paragrafo 3.

Compete all'ODV gestire la mole di informazioni acquisite durante l'esercizio dell'attività di vigilanza con la diligenza richiesta per attività di controllo e quindi garantendo la segretezza delle informazioni in talune circostanze e costantemente un livello di riservatezza adeguato e conforme alle *policy* aziendali in materia di *privacy*.

L'obbligo di riportare periodicamente al Consiglio di Amministrazione e ad altri organi di *governance* dell'Ente Vigilato le risultanze dell'attività di vigilanza non limita o condiziona la facoltà da parte dell'ODV di tenere riservati documenti, dati personali e altre notizie acquisite nel corso delle attività e che non costituiscono dati utili per l'organo amministrativo per procedere ad assumere determinazioni e/o iniziative finalizzate a prevenire la commissione dei reati presupposto di cui al catalogo ex D.lgs. 231/01 e smi.