



SealedMedia ed il D.LGS 231/2001

sealed[media][®]



1. PREMESSA

Il presente documento si prefigge lo scopo di analizzare come l'utilizzo di una soluzione di protezione persistente della documentazione quale SealedMedia possa aiutare Enti ed Aziende al rispetto di quanto previsto dal D.Lgs 231/2001.

2. BREVI CENNI SUL D.LGS 231/2001

Il Decreto Legislativo 8 giugno 2001, n. 231, recante "*Disciplina della responsabilità amministrativa delle persone giuridiche, della società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n.300*" ha introdotto per la prima volta nel nostro ordinamento la responsabilità degli enti in sede penale, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

Destinatari della normativa sono gli enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica. L'ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti e, in definitiva, gli interessi economici dei soci, i quali, fino all'entrata in vigore della legge in esame, non pativano conseguenze dalla realizzazione di reati commessi, con vantaggio della società, da amministratori e/o dipendenti.

L'innovazione normativa non è di poco conto, in quanto **né ente, né i soci della società o associazioni possono dirsi estranei al procedimento penale per reati commessi a vantaggio o nell'interesse dell'ente.**

Ciò, ovviamente, determina l'interesse di quei soggetti (soci, associati, ecc.) che partecipano alle vicende patrimoniali dell'ente, al controllo della regolarità e della legalità dell'operato sociale.

Questa nuova responsabilità sorge soltanto in occasione della realizzazione di determinati tipi di reati da parte di soggetti legati a vario titolo all'ente e solo nell'ipotesi che la condotta lecita sia stata realizzata *nell'interesse o a vantaggio* di esso. Dunque, non soltanto allorché il comportamento illecito abbia determinato un vantaggio, patrimoniale, per l'ente, ma anche nell'ipotesi in cui, pure in assenza di tale concreto risultato, il fatto-reato trovi ragione *nell'interesse* dell'ente.

Gli enti rischieranno sanzioni pecuniarie fino a € 1.550.000,00.=, sanzioni interdittive quali l'interdizione dall'esercizio dell'attività, la revoca di licenze o autorizzazioni, il divieto di stipulare contratti con la pubblica amministrazione, l'esclusione di agevolazioni, finanziamenti, il divieto di pubblicizzare beni e prodotti oltre che la confisca del bene oggetto del reato e la pubblicazione della sentenza. Anche in ipotesi di trasformazione dell'ente, una eventuale fusione o scissione non farà comunque venir meno la responsabilità per fatti antecedenti all'operazione finanziaria.

L'articolo 6 del Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede una forma specifica di esonero da detta responsabilità qualora l'Ente dimostri che:

- a) l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione del fatto, *modelli di organizzazione e di gestione* idonei a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato a un **organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo**;
- c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione e gestione;
- d) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Il Decreto prevede, inoltre che – in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati – i modelli di cui alla lettera a), debbano rispondere alle seguenti esigenze:



- 1) individuare le attività nel cui ambito esiste la possibilità che vengano commessi i reati previsti dal Decreto;
- 2) prevedere specifici controlli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- 3) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- 4) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello che dovrà garantire indipendenza ed autonomia dai vertici dell'ente, professionalità e continuità di azione;
- 5) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

3. LA VALIDITÀ DEL SOFTWARE SEALEDMEDIA

Ciò premesso, si rileva che SealedMedia può costituire un ottimo elemento che agevoli l'implementazione e la difesa dei protocolli organizzativi a carattere informatico previsti nel citato D.Lgs. 231/01.

In effetti il Decreto legislativo prevede che, in caso di reato commesso da proprio dipendente o da proprio soggetto apicale, l'ente non risponde se a) prova che sono stati adottati ed efficacemente attuati, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi, b) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione.

Tali modelli devono rispondere alle seguenti esigenze:

- a) individuare le attività nel cui ambito possono essere commessi reati;
- b) **prevedere sistemi diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;**
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli.

Come appare chiaro dalla lettura del Decreto, la effettiva portata esimente di un sistema organizzativo di carattere informatico volto a prevenire la estensione delle conseguenze amministrative di reato all'ente, trova la sua origine nella effettività e nella concreta applicazione di standard comportamentali e di flussi informativi chiari e verificabili all'interno dell'azienda, tali da costituire un efficace sistema di controllo per i comportamenti potenzialmente a rischio reato.

In particolare, l'utilità di un sistema di sicurezza informatico come SealedMedia pare in grado di garantire, in ogni momento:

- 1) l'immodificabilità di un documento, di un flusso o di un tracciato, garantendo la possibilità di lettura e di modifica a determinati soggetti abilitati;
- 2) la possibilità di operare una selezione su alcuni documenti destinati a far parte di una banca data riservata e non accessibile;
- 3) la possibilità di tracciare l'accesso da parte di eventuali soggetti non autorizzati ed i loro tentativi di modifica od accesso al documento de quo;
- 4) la possibilità di tenere traccia contestualmente degli interventi autorizzati, dei tempi di intervento, dei termini finali per la possibilità dell'intervento o dell'accesso;
- 5) la possibilità di impedire totalmente l'accesso e gestire in forma differenziata i documenti "riservati".



Sul piano operativo, l'utilità del sistema di protezione e tracciabilità SealedMedia ai fini di una soddisfacente implementazione di un valido sistema procedurale, può essere dimostrata con i seguenti schemi esemplificativi:

- a) gestione protetta dei file relativi alla partecipazione a gare pubbliche: il prodotto potrebbe costituire un valido deterrente per la modifica in corso d'opera di offerte o ribassi di offerta in fase di aggiudicazione (**Direzione Gare/Direzione legale**);
- b) gestione protetta dei file relativi a contratti con la P.A. comprendente anche le fasi di gestione dei contatti informatici diretti con esponenti della P.A. (**Direzione Acquisti**);
- c) gestione protetta dei file relativi alle procedure di assunzione del personale al fine di verificarne il rispetto dell'iter (**Direzione del Personale**);
- d) gestione protetta dei file dei contributi e dei finanziamenti erogati dallo Stato o dalla Comunità Europea (**Direzione del Personale/Direzione Fiscale**);
- e) gestione protetta di file relativi alla gestione ed al controllo delle risorse finanziarie (**Direzione Amministrativa/Controllo di gestione**);
- f) gestione protetta dei file inerenti gli adempimenti amministrativi ed i rapporti con gli enti previdenziali e le autorità fiscali (**Direzione Amministrativa**);
- g) gestione protetta dei file di rapporti con enti ed organismi nazionali: Banca d'Italia, CO.N.SO.B., Borsa, Autorità Centrali di Governo (**Direzione Rapporti Istituzionali**);
- h) gestione protetta dei file dei servizi di tesoreria (**Direzione Amministrazione/Finanza**);
- i) gestione protetta dei file relativi a rapporti con la Magistratura e le Autorità di Pubblica Sicurezza e gestione del Contenzioso (**Direzione Affari Legali**);
- j) gestione protetta dei file relativi agli Acquisti societari (**Direzione Acquisti**);
- k) gestione protetta dei file relativi al controllo del budget di spesa (**Direzione Pianificazione e Controllo**);
- l) gestione protetta dei file relativi alla predisposizione delle comunicazioni a soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della Società (bilancio d'esercizio e bilancio consolidato corredati dalla relativa relazione sulla gestione), relazioni trimestrali e semestrale, ecc.) (**Direzione Amministrazione**);
- m) gestione protetta dei file relativi alla predisposizione dei prospetti informativi (**Direzione Affari Societari**);
- n) gestione protetta dei file relativi gestione dei rapporti con la società di revisione contabile in ordine all'attività di comunicazione da parte di quest'ultima a terzi relativa alla situazione economica, patrimoniale o finanziaria (**Direzione Comunicazione/Investor Relations**);
- o) gestione protetta dei file relativi alla gestione e comunicazione di notizie/dati verso l'esterno (rapporti con investitori istituzionali, comunicati *price sensitive*) (**Direzione Comunicazione/Investor Relations**).

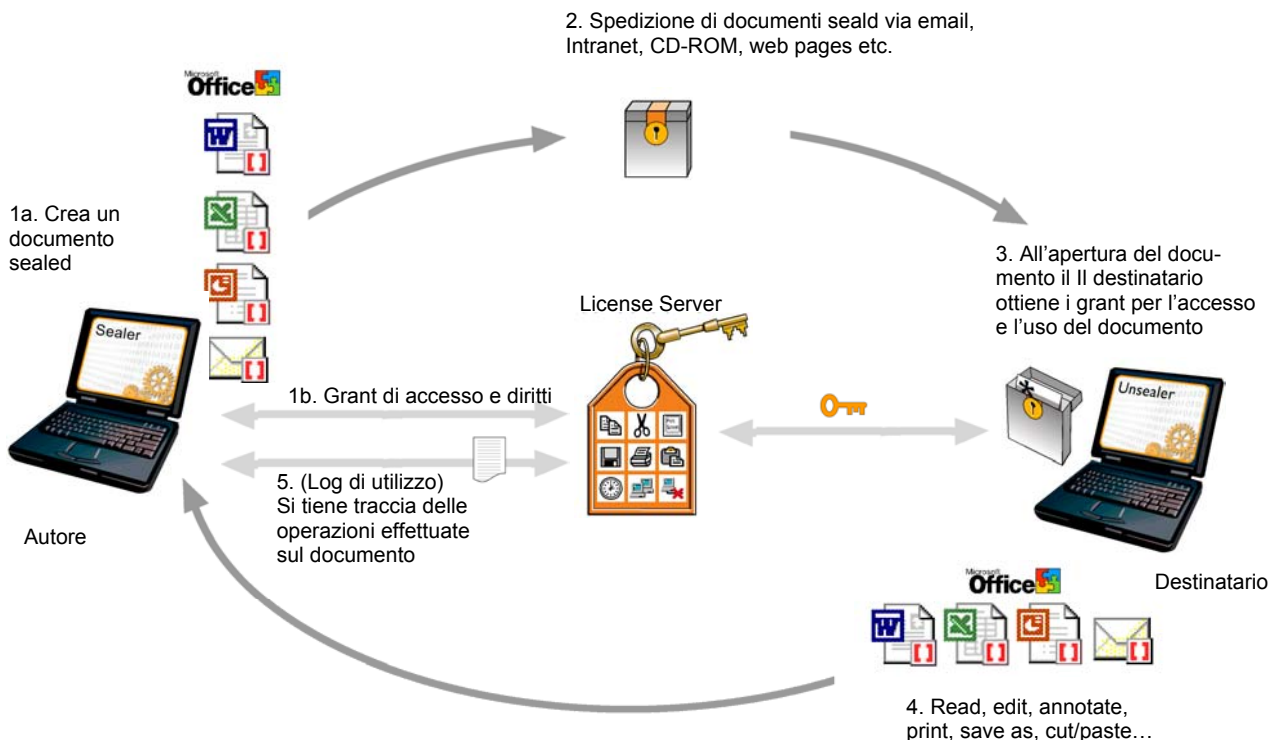


4. SEALEDMEDIA

SealedMedia e' una soluzione informatica che permette la protezione (attraverso criptazione) della documentazione riservata consentendo solo ad utenti autorizzati di avere accesso ai documenti protetti e di utilizzarli secondo modalit  predefinite. Ad esempio pu  non consentire di copiare o modificare o salvare il file se l'utente non e' debitamente autorizzato. Queste autorizzazioni possono essere variate nel corso del tempo anche dopo che il documento e' stato distribuito. Tutto ci  permette di realizzare un controllo puntuale e sostanzialmente non eludibile circa l'utilizzo della documentazione riservata nel suo intero ciclo di vita: dalla fase di redazione a quella di obsolescenza. I formati supportati sono: E-mail (Microsoft® Outlook® e Lotus Notes®), Microsoft® Word®, Microsoft® Excel®, Microsoft® PowerPoint®, Adobe® PDF and HTML, in aggiunta a vari formati immagine, video ed audio.

4.1 COME FUNZIONE SEALEDMEDIA

1. L'autore redige un documento riservato con uno strumento di produttivit  (Es. Word).
2. Il documento viene sigillato (criptato) utilizzando la tecnologia SealeMedia; le modalit  di fruizione riservate ai futuri utenti (grant) sono state preventivamente memorizzate in un server. Detti grant cos  come la lista dei potenziali fruitori del sistema vengono infatti preconfigurati (una tantum) durante la fase di set-up della soluzione.
3. Il documento, cos  sigillato, pu  essere quindi inviato ad altri utenti utilizzando i sistemi gi  in uso presso l'organizzazione (e-mail, cartelle condivise, web site, CD-ROM, "memorie USB",...).
4. Per poter utilizzare il documento sigillato l'utente destinatario dovr  aver installato l'Unsealer (un plug-in di circa 2.5 MB, scaricabile gratuitamente dal sito www.sealedmedia.com ed autoinstallante). L'Unsealer provveder  a richiedere all'utente destinatario appropriati nome utente e password, e quindi verificher  la sua identit  ed i grant a lui riservati, collegandosi automaticamente al license server, quindi consentir  all'utente stesso di aprire il documento e ne permetter  l'utilizzo nel rispetto dei grant a lui assegnati, ad esempio potrebbe non permettergli di effettuare "copia/incolla" o "salva col nome".
5. Il License Server mantiene automaticamente traccia di ogni utilizzo del sistema, e pertanto e' possibile ricostruire l'intera "storia" di documento verificandone ad esempio chi ha avuto accesso al file, da quale postazione di lavoro, per quanto tempo, quali operazioni sono state effettuate...



Per ulteriori informazioni su SealedMedia si pu  consultare il sito di DaMan S.r.l., unico distributore italiano delle tecnologie SealedMedia: www.daman.it, oppure contattare DaMan S.r.l. allo 06-65970236 o via mail info@daman.it