I Modelli Organizzativi con riguardo alle nuove tecnologie informatiche ed alla tutela dei dati personali

Matteo Colombo

Esperto in materia di Privacy e D.Lgs. 231/2001,
Amministratore Delegato di Labor Project

Il D.Lgs. 231/01

Il D.Lgs. 8/6/2001 n. 231 ha introdotto la previsione di una responsabilità amministrativa e diretta dell'ente collettivo per reati commessi nel proprio interesse o a proprio vantaggio da parte delle persone fisiche ad esso legate, soggetti apicali e soggetti sottoposti alla direzione e vigilanza di questi ultimi.

La norma introduce la responsabilità in sede penale della società che va ad aggiungersi a quella della persona fisica. Si applica a:

- Società di capitali e di persone
- Associazioni anche prive di personalità giuridica
- Enti pubblici economici

La Società può incorrere in gravi sanzioni a meno che si tuteli mediante l'adozione e l'efficace attuazione di un modello organizzativo idoneo a prevenire i reati indicati dalla legge.

Principi cardine del D.Lgs. 231/01

La società risponde in sede penale in aggiunta alla persona fisica

SE

1. è stato commesso uno dei REATI previsti dal Decreto da SOGGETTI in posizione apicale o sottoposti all'altrui direzione

2. ciò è stato fatto NELL'INTERESSE o A VANTAGGIO della società

3. la società non abbia attuato un MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO effettivo ed efficace per la prevenzione dei reati

I soggetti che possono attivare la responsabilità dell'ente

Soggetti apicali

Rapporto di rappresentanza

Consiglio di Amministrazione; Amministratore delegato, procuratori amministratori, direttori generali, direttori di divisione

Soggetti sottoposti

Rapporto di direzione

dipendenti, lavoratore subordinato o equiparato, collaboratori, agenti, distributori, consulenti

Se il reato è commesso da un soggetto apicale o da un soggetto sottoposto alla direzione o alla vigilanza dei primi

Configurabilità della Responsabilità "penale" della Società

Le nozioni di interesse e vantaggio

Interesse

finalizzazione della condotta all'utilità della società

Ex-ante

Vantaggio

concreta acquisizione di una utilità per la società

Ex-post

L'interesse o il vantaggio devono intendersi come "**potenziale o effettiva utilità**, ancorché non necessariamente di carattere patrimoniale, derivante all'ente dalla commissione del reato presupposto" (Tribunale di Milano, sez. XI, udienza 28 aprile 2008).

Reati presupposto

- Delitti nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 D. Lgs. 231/01);
- Delitti informatici e trattamento illecito di dati (art. 24-bis. D.Lgs. 231/01);
- Delitti di criminalità organizzata (art. 24-ter D. Lgs. 231/01)
- Delitti contro la fede pubblica (art. 25-bis D. Lgs. 231/01);
- Delitti contro l'industria e il commercio (art. 25-bis.1 D. Lgs. 231/01), della legge 23 luglio 2009, n. 99);
- Reati societari (art. 25-ter D. Lgs. 231/01);
- Delitti in materia di terrorismo e di eversione dell'ordine democratico (art. 25-quater D. Lgs. 231/01);
- Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1 D. Lgs. 231/01);

Reati presupposto (segue)

- Delitti contro la personalità individuale (art. 25-quinquies D. Lgs. 231/01);
- Abusi di mercato (art. 25-sexies D.Lgs. 231/01);
- Reati in materia di **salute e sicurezza sui luoghi di lavoro** (art. 25-septies D. Lgs. 231/01);
- Reati di riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/01);
- Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/01);
- Induzione a non rendere dichiarazioni all'autorità giudiziaria (art. 25-decies D.Lgs. 231/01)
- Reati transnazionali (art. 10 l. 146/06).
- Reati ambientali (art. 25-undecies D.Lgs. 231/01)

Elenco dei "delitti" informatici articolo 25-sexies

- 420: attentato a impianti di pubblica utilità compreso il danneggiamento o la distruzione di sistemi informatici o telematici di pubblica utilità
- 491-bis: falsità in un documento informatico pubblico o privato
- 615-ter: accesso abusivo ad un sistema informatico o telematico
- 615-quater: detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- 615-quinquies: diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- 617-quater: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- 617-quinquies: installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.
- 635-bis: danneggiamento di informazioni, dati e programmi informatici
- 635-ter: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- 635-quater: danneggiamento di sistemi informatici o telematici
- 640-quinquies: truffa del certificatore di firma elettronica.

Esempio di fattispecie

Accesso illegale, intenzionale e senza diritto, a tutto o a parte di un sistema informatico (art. 615 ter c.p.).

1. Chi accede ad un sistema protetto da misure di sicurezza;
2. Chi accede nel sistema legittimamente ma vi si mantiene contro al volontà espressa o tacita di chi ha il diritto ad escluderlo.

Sanzione da cento a cinquecento quote.

Valore della quota va da €. 258,23 a €. 1549,37 sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione.

Hackeraggio & Virus

- L'art. 615 C.P. così formulato offre un aiuto alla difesa contro un comportamento illegittimo ma diffuso nel mondo delle comunicazioni informatiche quali il cosiddetto hackeraggio.

- Virus: Offre tutela anche a chi subisce danni da chi mette in circolazione un programma informatico – proprio o di terzi – idoneo al danneggiamento di un sistema informatico o telematico, dati o programmi o idoneo a creare interruzione totale o parziale del sistema.

Le sanzioni

Le sanzioni per gli illeciti amministrativi dipendenti da reato sono:

- La **sanzione pecuniaria** (fino a 1,5 Mln €)
- La **sanzione interdittiva** (anche in via cautelare)
  - interdizione esercizio attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la pubblica amministrazione;
  - esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
  - divieto di pubblicizzare beni o servizi;
- La **confisca**;
- La **pubblicazione della sentenza**.

Esonero dell'ente da responsabilità

L'ente non risponde degli illeciti amministrativi dipendenti da reato, se prova che:

- sono stati predisposti ed efficacemente attuati, prima della commissione del fatto, modelli di organizzazione gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- è stato istituito un organo di vigilanza, dotato di autonomi poteri di iniziativa e di controllo, con il compito di vigilare sul funzionamento e l'osservanza dei modelli di organizzazione (art. 6, comma 1, lett. b);
- il reato sia stato commesso eludendo fraudolentemente i modelli organizzativi.

L'elusione fraudolenta

La società deve dimostrare che:

- ha posto in essere procedure/policy utili a prevenire il reato che si è verificato;
- la commissione del reato è stata possibile solo attraverso una condotta non rispettosa delle procedure/policy interne adottate dalla società, così eludendo i sistemi di controllo interno.

- Però attenzione: A dover preoccupare le aziende è la circostanza che la responsabilità stessa possa essere imputata anche nelle ipotesi in cui non venga rintracciato l'autore materiale del reato.

- Ne consegue che la mancata individuazione del soggetto attivo del reato, non infrequente in materia di criminalità informatica, possa non far comprendere esattamente all'organo giudicante le motivazioni dello stesso e quindi determinare un'attribuzione di responsabilità anche quando l'autore del reato abbia agito per fini esclusivamente personali e non nell'interesse del suo datore di lavoro.

Cosa inserire nel Modello?

Labor Project®
consulenza operativa per l'impresa

ESEMPIO DI PARTE SPECIALE:

- **Regolamentazione**: il processo di gestione del server e del sito internet dell'azienda è definito da una policy interna sull'utilizzo degli strumenti informatici consegnata ad ogni dipendente al momento dell'assunzione. Il Responsabile IT si occupa del controllo sui dispositivi HD & SW e della creazione dei profili utente che sono necessari per tracciare l'accesso ai terminali da parte dei dipendenti e dei form per le vendite degli agenti. Una società esterna si occupa, invece, della gestione del sito, dei profili e-mail, della mailing list e delle news che di volta in volta vengono inserite sul sito della Società.

Esempio Principi del Modello

- **Segregazione dei compiti:** il processo prevede la separazione dei compiti:
  - Esecuzione: Responsabile IT, Società esterna;
  - Controllo: Responsabile IT;
  - Autorizzazione: Presidente.

- **Tracciabilità:** tutta la documentazione relativa alla gestione delle risorse informatiche viene archiviata dal CED. La Società Esterna, poi, si occupa di applicare alcune misure di sicurezza previste da contratto (sicurezza fisica).

- **Procure e deleghe:** le funzioni, i compiti e i poteri di intervento affidati alla società esterna sono regolati da apposito contratto.

- **Protocolli di controllo specifici:** Politica aziendale di utilizzo strumenti informatici; rispetto della normativa per la protezione dei dati personali con riferimento alla conservazione dei dati informatici.

Esempi

In particolare - a titolo esemplificativo – si riportano di seguito:

Occasioni di realizzazione della condotta

- Connessione a *internet* o salvataggio di *files* sul *server* aziendale o sul disco fisso del singolo *computer*;
- Gestione degli archivi informatici;
- Scambio di *e-mail* interne.

Finalità della condotta

- Fruizione e/o scambio, a qualsiasi titolo, di materiale pornografico.
- Danneggiamento di archivi informatici.

Esempi di modalità di realizzazione della condotta

- Salvataggio di immagini o filmati pedopornografici sul server aziendale o sul disco fisso dei singoli computer aziendali;
- Invio e ricezione di materiale pornografico attraverso e-mail;
- Introduzione abusiva e/o danneggiamento di archivi o sistemi informatici.

COSA FARE

NORMATIVA PRIVACY

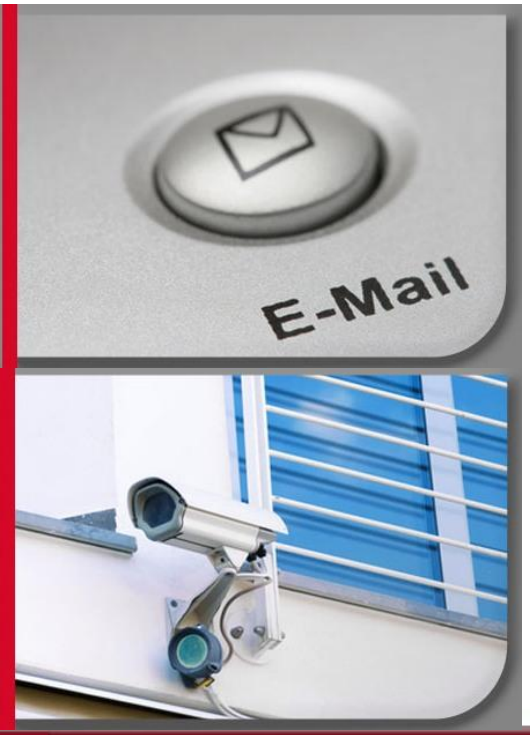
OBBLIGHI DEL CODICE PRIVACY

D.Lgs. 196/03

- ADOTTARE MISURE MINIME DI SICUREZZA All. tecnico B
- FORNIRE INFORMATIVE ART. 13 (INTERNE ED ESTERNE)
- NOMINARE INCARICATI (art. 30) E RESPONSABILI (art. 29)
- REGOLE SCRITTE PER TRATTAMENTI CARTACEI
- REVISIONE ANNUALE DEI DOCUMENTI
- ISTRUZIONI AGLI INCARICATI

NORMATIVA PRIVACY

OLTRE IL CODICE PRIVACY



- **Autorizzazioni Generali**
- **Deliberazione n. 53 Linee Guida dati personali di lavoratori 23 novembre 2006**
- **Provv. Lavoro: linee guida per posta elettronica e internet - 1 marzo 2007**
- **Provv. su Amministratori di Sistema 27 novembre 2008**
- **Provv. su videosorveglianza 08 aprile 2010**

M.O.S.P.

Il **Modello Organizzativo Sicurezza Privacy** (MOSP) è una misura idonea di sicurezza che comporta da parte delle aziende l'impegno a regolamentare attraverso uno specifico documento tutti i principali aspetti relativi alla sicurezza ed alla Privacy.

IMPORTANTE: può essere un documento che affianca il modello esistente attraverso richiami specifici. Tenendo questi aggiornato viene automaticamente aggiornato il Modello 231

Grazie per l'attenzione

Labor Project srl

Via Brianza n. 65 – 22063 Cantù (CO)

www.laborproject.it

info@laborproject.it