



trasferimento tecnologico e innovazione

231PS02

Rev. 00 del 2016-11-30

## **Parte speciale 2**

### **del Modello di organizzazione, gestione e controllo ai sensi del Decreto legislativo 231/2001**

**Reati informatici e trattamento illecito di dati - (art. 24 bis D.Lgs. 231/01)**

Rev. 00 del 30/11/2016

Ufficializzato da CDA con delibera n° 14 del 01/12/2016



trasferimento tecnologico e innovazione

## **MODELLO 231**

### **Parte Speciale 2**

#### **Sommario**

1. Delitti informatici e trattamento illecito di dati .....	3
2. Considerazioni esplicative .....	3
3. Individuazione delle attività sensibili .....	4
4. Misure atte a prevenire la commissione del reato.....	4



## MODELLO 231

### Parte Speciale 2

trasferimento tecnologico e innovazione

## 1. Delitti informatici e trattamento illecito di dati

A seguito della ratifica ed esecuzione, da parte dello Stato Italiano, della Convenzione del Consiglio d'Europa sulla criminalità informatica, il Legislatore, con Legge 18 marzo 2008, n. 48, ha introdotto nel Decreto Legislativo 8 giugno 2001 n. 231, l'art. 24 bis sui delitti informatici e trattamento illecito di dati. Le fattispecie di reato sono quelle previste dagli articoli 491 bis c.p. "Documenti informatici"; 615 ter c.p.

- "Accesso abusivo ad un sistema informatico o telematico";
- 615 quater c.p. "Detenzione e diffusione abusiva di codici d'accesso a sistemi informatici o telematici";
- 615 quinquies c.p. "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico"; 617 quater c.p. "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche";
- 617 quinquies c.p. "Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche";
- 635 bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"; 635 ter c.p. "Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità";
- 635 quater c.p. "Danneggiamento di sistemi informatici o telematici";
- 635 quinquies c.p. "Danneggiamento di sistemi informatici o telematici di pubblica utilità";
- 640 quinquies c.p. "Frode informatica del soggetto che presta servizi di certificazione di firma elettronica".

## 2. Considerazioni esplicative

L'estensione della portata del decreto 231/2001 alle altre tipologie di reati informatici, a seguito del recepimento nella l. 48/08 della convenzione di Budapest sul cybercrime, impone alle aziende di prendere in considerazione i rischi che possono derivare dal compimento di tali reati da parte dei dipendenti e che possono concretizzarsi in sanzioni pecuniarie ed interdittive.

Tali reati informatici sono più difficilmente accertabili rispetto agli altri reati inseriti nel decreto 231 sotto più ordini di considerazioni. In primo luogo, perché possono essere commessi da chiunque e non esistono delle aree o funzioni maggiormente a rischio, il che comporta la necessità di una vigilanza quanto mai difficile dovendo, in teoria, essere estesa a tutti i dipendenti. In seconda analisi tali reati, nella maggior parte dei casi, sono strumentali al raggiungimento di uno scopo ulteriore, per cui risulta difficile la loro individuazione fino a quando non si sia realizzato il fine ultimo.

L'art. 1 della Convenzione di Budapest chiarisce che per "sistema informatico" si considera "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati".

Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di un software che permette il loro funzionamento elaborando delle informazioni (o comandi).

Nel medesimo articolo è contenuta la definizione di "dato informatico", che descrive il concetto derivandolo dall'uso: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informativo di svolgere una funzione".



## MODELLO 231

### Parte Speciale 2

trasferimento tecnologico e innovazione

### 3. Individuazione delle attività sensibili

Atteso che l'utilizzo dello strumento informatico è da ritenersi imprescindibile nell'ambito di tutti i settori della società, le attività sensibili di reato in t<sup>2</sup>i sono:

- gestione della comunicazione su siti internet aziendali e di clienti;
- gestione degli accessi alla rete aziendale;
- gestione di accessi a siti web esterni (banca, regione);
- sviluppo software;
- installazione rete;
- utilizzo dei pc, accesso ai dati sul server e alle banche dati;
- gestione accessi a siti web / programmi della PA.

Le funzioni principalmente coinvolte nelle attività sopra elencate sono RIT, gli Addetti Web Content, i Programmatori, l'amministratore di rete, i tecnici di rete e per alcune attività tutto il personale di t<sup>2</sup>i.

### 4. Misure atte a prevenire la commissione del reato

Tra le misure per prevenire l'accadimento dei suddetti reati occorre citare oltre al Codice etico, anche il fatto che il Modello prevede procedure specifiche per la sicurezza delle informazioni e la tutela dei dati (inclusi quelli sensibili) tra cui il DPS ossia il Documento programmatico della sicurezza, ai sensi del D.lgs.196:2003 e smi, la PSD ossia la Procedura per la sicurezza dei dati informatici, il Documento riservatezza MNA e la PSI ossia la Procedura per la Gestione dei Sistemi Informativi.

In particolare è inoltre previsto che:

- siano identificate chiaramente, all'interno dell'organizzazione, figure dedicate all'inserimento dei documenti per la pubblicazione (settaggio di account) e/o a progetti specifici;
- l'accesso alla rete sia suddiviso tra aule, uffici, utenti generici e account personali e ci sia una chiara profilazione delle regole di posta elettronica e di connettività;
- per l'inserimento di dati in banche dati esterne, ogni funzione gestisca autonomamente, ma in modo regolamentato, ID e password;
- venga effettuato un censimento dei software installati attraverso uno specifico programma dedicato;
- sia presente un elenco software macro e un elenco dei software interni per la gestione interna;
- vi siano regole condivise per la gestione delle richieste e per la gestione di id e pw di accesso ai sistemi informatici e telematici;
- vi siano prassi condivise e conosciute per lo sviluppo di software;
- si utilizzi solo la firma digitale del Direttore e un unico indirizzo di posta elettronica certificata;
- vi siano regole per la tenuta sotto controllo dei codici di accesso ai sistemi esterni/banche dati (Regione/Intereg);
- vi siano prassi condivise e conosciute per le attività di erogazione dei servizi di hosting.