

IPHNET

**MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. N. 231
PARTE SPECIALE
SEZIONE B**

Delitti informatici e trattamento illecito di dati (art. 24–*bis* del D. Lgs. n. 231/2001)



INDICE

1. Premessa	3
2. Le fattispecie di cui agli artt. 24 (limitatamente alla frode informatica) e 24-bis del D. Lgs. n. 231/2001	3
3. Processi sensibili, funzioni coinvolte e valutazione del rischio.....	4
4. Logiche comportamentali di ordine generale.....	4
5. Procedure specifiche	4
6. Flussi verso l'Organismo di Vigilanza.	5



IPHNET

1. Premessa.

L'art. 24–bis è stato introdotto, nel corpo del D. Lgs. n. 231/2001, dalla L. n. 48/2008, di ratifica della c.d. Convenzione Cybercrime, firmata a Budapest il 23 novembre 2001. L'introduzione di tale tipologia di reati nel novero delle fattispecie idonee a generare la responsabilità dell'ente non è privo di conseguenze pratiche, constatato che l'uso di strumenti informatici è diffuso in ogni realtà aziendale.

L'art. 1 della citata Convenzione stabilisce che per "sistema informatico" deve intendersi qualsiasi dispositivo o qualsiasi gruppo di dispositivi tra loro interconnessi o collegati, uno o più dei quali, in base ad un programma, eseguono l'elaborazione automatica dei dati.

La principale caratteristica di un "sistema informatico" è dunque l'esecuzione automatizzata di operazioni. Per "dato informatico", la stessa Convenzione intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma che ne permetta l'elaborazione con un sistema informatico. Tale definizione fa riferimento sia ai dati in senso stretto, sia ai programmi, in quanto i primi costituiscono le informazioni che vengono generate e salvate attraverso l'utilizzazione dei secondi.

2. Le fattispecie di cui agli artt. 24 (limitatamente alla frode informatica) e 24–bis del D. Lgs. n. 231/2001.

L'art. 24 del D. Lgs. n. 231/2001 così dispone:

"1. In relazione alla commissione dei delitti di cui agli articoli [omissis] 640–ter se commesso in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

2. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità; si applica la sanzione pecuniaria da duecento a seicento quote".

L'art. 24–bis del D. Lgs. n. 231/2001 così dispone:

"1. In relazione alla commissione dei delitti di cui agli articoli 615–ter, 617–quater, 617–quinquies, 635–bis, 635–ter, 635–quater e 635–quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615–quater e 615–quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491–bis e 640–quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, e dei delitti di cui all'articolo 1, comma 11, del decreto–legge 21 settembre 2019, n. 105, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

IPHNET

3. Processi sensibili, funzioni coinvolte e valutazione del rischio.

Sono individuabili i seguenti “processi sensibili”:

- scorretto utilizzo di credenziali di accesso alle risorse fisiche ed informative del Sistema Informatico Aziendale;
- scorretto uso di personal computer, *tablet*, *smartphone* o altri dispositivi che permettono il collegamento a internet affidati all'utente;
- scorretto uso di *software* della società o personali;
- scorretto uso della rete della società;
- scorretto uso di database ed archivi della società;
- scorretto uso della posta elettronica;
- scorretto uso della rete internet e dei relativi servizi;
- scorretto uso delle postazioni autogestite collegate alla rete della società;
- indebita duplicazione o copiatura di opere intellettuali protette dal diritto d'autore;
- comunicazioni inveritiere o reticenti nell'ambito del perimetro di sicurezza nazionale cibernetica.

Quanto agli artt. 24 (limitatamente alla frode informatica) e 24–*bis* del D. Lgs. n. 231/2001, le specifiche aree di rischio sono meglio dettagliate nel documento di analisi del rischio redatto ai fini dell'implementazione del Regolamento UE 2016/679 (c.d. GDPR).

Quanto all'art. 25–*novies* del D. Lgs. n. 231/2001, sussiste un'area di rischio con riferimento ai reati in materia di diritto d'autore previsti dagli artt. 171, 171 *bis* e 171 *ter* della L. n. 633/1941. Non sussiste, invece, alcun rischio con riferimento ai reati di cui agli artt. 171 *septies* LDA – in quanto la società non è produttore o importatore di supporti – e 171 *octies* LDA – che si riferisce alle trasmissioni ad accesso condizionato.

In considerazione dell'attività svolta dalla società e dell'importante impegno di strumenti informatici, il rischio è stimato come “medio”.

Sono funzioni esposte al rischio della commissione dei reati trattati nella presente parte speciale:

- l'Organo Amministrativo;
- il Responsabile del Servizio ICT;
- i Dirigenti e Responsabili delle funzioni;
- i collaboratori che utilizzano i sistemi informatici della Società.

4. Logiche comportamentali di ordine generale.

La società si ispira alle logiche comportamentali di ordine generale descritte nel Codice Etico.

A titolo esemplificativo:

- è vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, a titolo individuale o concorsuale, integrino, direttamente o indirettamente, le fattispecie di reato menzionate ai punti 2 e 3;
- compiere qualunque tipo di operazione che esponga a rischio la sicurezza della rete informatica della società.

Gli organi sociali, i dipendenti, i collaboratori ed i consulenti della società che utilizzino strumenti informatici aziendali devono:

- tenere un comportamento corretto, nel rispetto delle norme di Legge e delle procedure interne, in tutte le attività che importino l'uso dei sistemi informatici;
- osservare rigorosamente tutte le norme poste dalla Legge a tutela dell'integrità dei sistemi informatici ed a tutela dei dati personali;
- assicurare il regolare funzionamento dei sistemi informatici, attenendosi alle procedure impartite;
- dare seguito con tempestività alle prescrizioni impartite in materia di uso dei sistemi informatici.

IPHNET

5. Procedure specifiche.

L'Associazione:

- ha provveduto a formalizzare le nomine richieste dal Regolamento UE 2016/679 (c.d. GDPR);
- ha aggiornato le proprie informative, rendendole conformi al Regolamento UE 2016/679 (c.d. GDPR);
- ha redatto il registro dei trattamenti;
- ha nominato il Responsabile della Protezione dei Dati personali (DPO);
- ha adottato una politica del sistema integrato di sicurezza UNI ISO 27001 E 27701, nel **Modello di Governance per la Privacy e Cybersecurity**.

Nell'espletamento delle proprie attività, gli organi sociali, i dipendenti, i collaboratori ed i consulenti della società, ognuno secondo il proprio ambito di attività e competenza, devono rispettare:

- le previsioni contenute nel "Manuale del sistema di gestione integrato", nonché nelle procedure ed istruzioni operative che compongono il "sistema di gestione integrato";
- i regolamenti, le procedure e le determinazioni dirigenziali eventualmente adottati dalla società;
- ogni altra disposizione comunitaria ovvero di Legge o di regolamento, anche di futura emanazione, eventualmente rilevante ai fini della prevenzione dei reati oggetto della presente Parte Speciale.

6. Flussi verso l'Organismo di Vigilanza.

L'Organismo di Vigilanza:

- dovrà essere notiziato, almeno trimestralmente, di eventuali disfunzioni o lacune del sistema informatico;
- dovrà essere tempestivamente notiziato dell'eventuale nomina o sostituzione del/i consulente/i informatico/i e/o dell'eventuale variazione degli accordi contrattuali in essere con lo/gli stesso/i;
- potrà chiedere al/i consulente/i informatico/i di predisporre un *report* riassuntivo delle attività svolte;
- dovrà essere tempestivamente notiziato della nomina/sostituzione dei Responsabili del Trattamento dei Dati nonché degli Addetti al Trattamento dei Dati;
- dovrà essere tempestivamente notiziato di eventuali segnalazioni relative ad un uso scorretto dei dati personali;
- almeno una volta all'anno chiederà al DPO di predisporre un *report* riassuntivo delle attività svolte.

Fermo restando il potere di attivarsi con specifici controlli anche a seguito di eventuali segnalazioni ricevute, l'Organismo di Vigilanza può provvedere a:

- effettuare controlli a campione sull'uso dei sistemi informatici da parte degli utenti;
- effettuare colloqui informativi con il consulente informatico;
- compiere ogni controllo diretto a verificare la sicurezza dei sistemi informatici e della rete informatica.

L'Organismo di Vigilanza potrà procedere ad acquisizioni documentali o colloqui con il personale della società, sia sulla base delle informazioni ricevute sia per svolgere accertamenti ulteriori.