Herman Miller Limited, Filiale Italiana

Modello di Organizzazione, Gestione e Controllo

[ex D.Lgs. 231 del 2001]

P a r t e S p e c i a l e - 7 -

Edizione marzo 2025

PARTE SPECIALE – 7 –

Delitti Informatici

INDICE

PARTE SPECIALE - 7 -

1. Le fattispecie dei delitti informatici (art. 24 bis del D. Lgs. 231/2001)

Per quanto concerne la presente Parte Speciale, si provvede, nel seguito, a fornire una breve descrizione dei reati indicati nell'art. 24 bis del D. Lgs. 231/2001.

Si riporta di seguito il testo integrale dell'art. 24 bis del D. Lgs. n. 231/2001, aggiunto dall'art. 7 L. 18 marzo 2008, n. 48 "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" in vigore dal 5 aprile 2008, e modificato dall'art. 1 comma 11bis del D.L. 105/2019, convertito con modificazioni dalla L. 133/2019 e come da ultimo modificato dalla Legge n. 90/2024.

Art. 24 bis. (Delitti informatici e trattamento illecito di dati)

"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 duecento a settecento quote.

1-bis. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 635-quater.1 del codice penale, si applica all'ente la sanzione pecuniaria sino a quattrocento 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'art. 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). Nei casi di condanna per il delitto indicato nel comma 1-bis si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni".

La Legge n. 48 del 18 marzo 2008 (pubblicata sulla Gazzetta Ufficiale della Repubblica Italiana Supplemento Ordinario n. 80 del 4 aprile 2008) ha introdotto l'articolo 24 bis del D. Lgs. 231/2001 (rubricato: "Delitti informatici e trattamento illecito dei dati").

La Legge n. 90 del 28 giugno 2024, in vigore dal 17 luglio 2024, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" (c.d. "Legge sulla Cybersicurezza"), ha introdotto il nuovo reato di estorsione informatica e, dall'altro, ha aumento le attuali sanzioni (compresa l'applicazione delle sanzioni interdittive) per i reati informatici già in precedenza richiamati dal D. Lgs. 231/2001.

Con questo articolo vengono estese le fattispecie di reato previste dal D. Lgs. 231/2001.

L'art. 24 bis prevede che l'ente possa essere sanzionato in relazione ai delitti informatici e al trattamento illecito di dati, in particolare per quanto riguarda:

- Accesso abusivo ad un sistema informatico o telematico (615 ter c.p.)

L'articolo 615 ter del Codice penale punisce chiunque abusivamente si introduca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo. L'oggetto della tutela penale è la salvaguardia del "domicilio informatico" quale spazio ideale - ma anche fisico in cui sono contenuti i dati informatici - di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto.

Il delitto di accesso abusivo ad un sistema informatico si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa.

Per "sistema informatico" deve intendersi il complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (615 quater c.p.)

L'art. 615 quater del Codice penale punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, detenga, produca,

riproduca, diffonda, importi, comunichi, consegni o installi apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater c.p.)

L’art 617 quater del Codice penale punisce chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa.

Salvo che il fatto costituisca reato più grave, la stessa pena si applica a chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle suddette comunicazioni.

- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617 quinquies c.p.)

L’art. 617 quinquies del Codice penale punisce chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

- Danneggiamento di informazioni, dati e programmi informatici (635 bis c.p.)

Salvo che il fatto costituisca più grave reato, l’art. 635 bis del Codice penale punisce chiunque distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635 ter c.p.)

Salvo che il fatto costituisca più grave reato, l’art. 635 ter del Codice penale punisce chiunque commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

- Danneggiamento di sistemi informatici o telematici (635 quater c.p.)

Salvo che il fatto costituisca più grave reato, l’art. 635 quater del Codice penale punisce chiunque, mediante le condotte di cui all’articolo 635 bis del Codice penale, ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.

- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (635 quater 1 c.p.)

L’art. 635 quater 1 del Codice penale punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procuri, detenga, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

- Danneggiamento di sistemi informatici o telematici di pubblico interesse (635 quinquies c.p.)

Salvo che il fatto costituisca più grave reato, l’articolo in analisi punisce chiunque, mediante le condotte di cui all'articolo 635 bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compia atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento.

- Documenti informatici (491 bis c.p.)

L’art. 491 bis del Codice penale punisce le falsità previste dal capo III del Codice penale riguardanti un documento informatico pubblico o privato avente efficacia probatoria.

Le falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.)

L’art. 640 quinquies del Codice penale punisce il soggetto che presti servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

*

2. Funzione della Parte Speciale - 7 -

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, Dipendenti, nonché da Consulenti e *Partner* di Herman Miller Limited, Filiale Italiana, come già definiti nella Parte Generale, eventualmente coinvolti nei Processi Sensibili.

Obiettivo della presente Parte Speciale è che tutti i Destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi dei Reati in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

a) dettagliare Processi Sensibili e procedure che i Dipendenti, Destinatari e i Consulenti/*Partner* di Herman Miller Limited, Filiale Italiana sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'OdV e ai responsabili delle altre funzioni aziendali che con lo stesso cooperano gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica previste.

*

3. Processi Sensibili nell'ambito di questa Parte Speciale

Attraverso l'analisi dei processi della Società sono stati individuati i seguenti Processi Sensibili, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate:

I. Sicurezza Informatica

*

4. Regole generali

4.1 Il sistema in linea generale

Nell'espletamento delle attività inerenti all'uso e alla gestione dei sistemi informatici, oltre alle regole di cui al presente Modello, i Dipendenti, Destinatari e Consulenti/*Partner* di Herman Miller Limited, Filiale Italiana, nella misura necessaria alle funzioni dagli stessi svolte, devono in generale conoscere e rispettare le *policy* aziendali.

4.2 Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico dei Dipendenti, Destinatari e Consulenti/*Partner* di Herman Miller Limited, Filiale Italiana di:

– porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

– violare i principi e le procedure esistenti in azienda e/o previste nella presente Parte Speciale.

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività inerenti all'uso e alla gestione dei sistemi informatici;
2. tutelare la riservatezza, la segretezza e l'integrità dei sistemi informatici, delle reti e dei dati informatici.

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:

a) violare, o accedere illegalmente a, un sistema informatico ovvero un domicilio informatico;

b) violare la riservatezza degli utenti che utilizzano tecnologie informatiche;

c) violare norme di sicurezza con l'intenzione di ottenere illegalmente informazioni all'interno di un computer o di altro sistema informatico;

d) intercettare senza autorizzazione trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico;

e) danneggiare, cancellare, modificare o sopprimere, senza autorizzazione, dati informatici;

f) sottrarre, anche mediante riproduzione o trasmissione, dati, informazioni o programmi;

g) impedire, interdire o bloccare senza autorizzazione il funzionamento di un sistema informatico;

h) utilizzare strumenti o apparecchiature, ivi compresi i programmi per elaboratore, per compiere una delle condotte sopra indicate;

i) utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;

j) introdursi, alterare, possedere o sopprimere dati informatici derivanti da dati non autentici;

k) cagionare un danno ad altre persone introducendosi, alterando, cancellando e interferendo nel funzionamento di un sistema informatico.

4.3 Standard di controllo generali

Gli standard generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

Segregazione delle attività: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.

Esistenza di procedure/norme/circolari: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle Attività Sensibili nonché modalità di archiviazione della documentazione rilevante.

Poteri autorizzativi e di firma: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società.

Tracciabilità: ogni operazione relativa all'Attività Sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

*

5. Standard di controllo specifici

Qui di seguito sono elencati gli standard di controllo specifici relativi alle singole Attività Sensibili.

I. ***Sicurezza informatica****.*

La regolamentazione dell'attività prevede che le disposizioni in materia di sicurezza del sistema informatico e telematico adottate dalla Società includono:

- la definizione degli obiettivi, delle linee guida e degli strumenti normativi relativamente alla sicurezza informatica e telematica;
- le modalità di aggiornamento, anche a seguito di cambiamenti significativi;
- l'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti;
- i rapporti con gli outsourcer informatici;
- la definizione dei principi di classificazione dei dati e delle informazioni (confidenzialità, autenticità e integrità);
- la definizione di ruoli e responsabilità nel trattamento dei dati e delle informazioni.

*

6. I controlli dell'OdV

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'OdV effettua controlli a campione sulle attività potenzialmente a rischio di delitti informatici, diretti a verificare la corretta esplicazione delle procedure in relazione alle regole di cui al presente Modello e alle procedure interne in essere.

A tal fine, all'OdV viene garantito - nel rispetto della normativa vigente, per esempio in tema di *privacy* - libero accesso a tutta la documentazione aziendale rilevante.