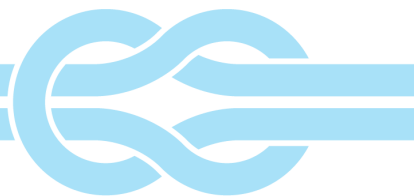


**Modello di Organizzazione,
Gestione e Controllo
ex Decreto Legislativo n.
231/2001**

*Parte Speciale “Sez. B”
Delitti informatici e
trattamento illecito di dati
(art. 24-bis del Decreto)*



1. Funzioni e obiettivi della Parte Speciale

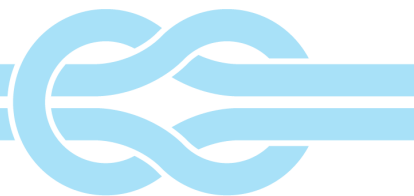
La Parte Speciale del presente Modello si propone di:

- individuare, previa descrizione delle fattispecie incriminatrici, le attività aziendali nel cui ambito potrebbero essere commessi reati rilevanti ai sensi del D.Lgs. 231/2001;
- evidenziare ai Destinatari del Modello le condotte che potrebbero comportare l'applicazione, nei confronti del Consorzio PSL, delle sanzioni previste dal D.Lgs. 231/2001;
- disciplinare i comportamenti richiesti ai Destinatari del Modello, al fine specifico di prevenire la commissione dei reati di cui alla presente Sez. B di Parte Speciale.

Obiettivo finale della Parte Speciale, pertanto, è la costruzione di un insieme strutturato di regole, oggetto di costante aggiornamento e monitoraggio, che non possa essere aggirato se non fraudolentemente, venendo così in rilievo, in tale ultima ipotesi, l'esimente da responsabilità di cui all'art. 6, comma 1, lett. c) del Decreto.

La presente Parte Speciale esamina nel dettaglio i Delitti informatici e trattamento illecito dei dati - art. 24 bis del Decreto - esemplificando le condotte che potrebbero integrarli in considerazione delle attività svolte dal Consorzio PSL.

La preventiva attività di “*Risk Assessment*” ha evidenziato un **rischio medio** per tali tipologie di reati in relazione allo svolgimento dell'attività del Consorzio.



2. Delitti informatici e trattamento illecito di dati: le fattispecie

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

La fattispecie punisce chiunque si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, o vi si mantiene senza averne diritto. La condotta può essere commessa sia da soggetti interni che esterni all'ente.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Questo reato consiste nella detenzione o diffusione, senza giustificazione, di codici, parole chiave o altri strumenti di accesso a sistemi informatici protetti, al fine di trarne un utilizzo illecito.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinqües c.p.)

Punisce chi diffonde, consegna o installa programmi informatici progettati per danneggiare o interrompere il funzionamento di un sistema informatico o telematico.

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

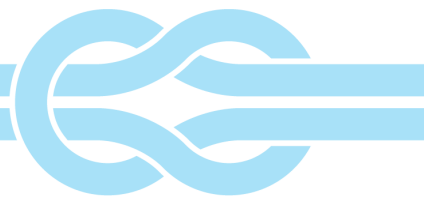
Questo reato punisce chi intercetta, impedisce o interrompe comunicazioni informatiche o telematiche tra più soggetti, senza autorizzazione.

Installazione di apparecchiature per intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinqües c.p.)

La fattispecie riguarda la produzione, l'installazione o l'utilizzo di strumenti destinati a intercettare o interrompere comunicazioni telematiche.

Estorsione di cui all'art. 629 comma 3 c.p.

Punisce chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinqües ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

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

Punisce chiunque danneggia informazioni, dati o programmi informatici altrui, rendendoli inservibili o compromettendone l'uso.

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

Consiste nell'alterazione o distruzione di un sistema informatico o telematico, con conseguente grave danno per il titolare.

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

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 procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

Danneggiamento di sistemi informatici di pubblica utilità (art. 635-quinquies c.p.).

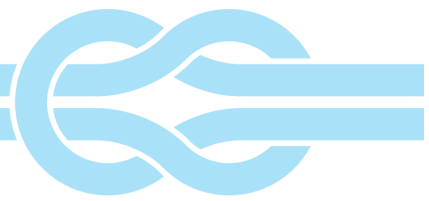
Fattispecie che riguarda il danneggiamento o l'interruzione di sistemi informatici o telematici destinati a un servizio pubblico o di pubblica utilità, con aggravante per i casi in cui il fatto metta in pericolo la sicurezza pubblica.

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

E' punita la condotta del soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a se' o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Documenti informatici (art. 491-bis)

La fattispecie prevede che se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.



3. Attività a rischio, misure di prevenzione e divieti specifici

➤ **Art. 24 bis del D.Lgs. 231/2001**

Attività a rischio:

1. Gestione di dati sensibili per clienti pubblici e privati:

- Trattamento e conservazione di dati sensibili legati alle pratiche fiscali, tributarie o contabili.
- Rischio di accesso abusivo a sistemi informatici aziendali o di terzi.

2. Utilizzo di sistemi informatici aziendali per la gestione delle attività:

- Rischio di utilizzo non autorizzato, alterazione o perdita di dati aziendali e dei clienti.

Misure di prevenzione:

- Politiche di sicurezza informatica: Introduzione di firewall, antivirus e sistemi di crittografia per proteggere i dati sensibili.
- Gestione degli accessi: Limitare l'accesso ai dati aziendali e dei clienti solo al personale autorizzato.
- Procedure di backup: Implementare sistemi di backup regolari per proteggere i dati in caso di attacchi o guasti.
- Formazione del personale: Sensibilizzazione sui rischi informatici e sull'importanza della protezione dei dati.

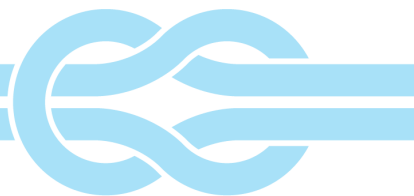
Divieti specifici:

1. È vietato **accedere abusivamente** a sistemi informatici aziendali o di terzi (clienti, enti pubblici o privati) senza autorizzazione, anche in presenza di credenziali valide.
2. È vietato **manipolare, alterare o distruggere dati** o programmi informatici aziendali, di clienti o di enti pubblici.
3. È vietato **installare o utilizzare un software non autorizzato** o non conforme alle politiche di sicurezza informatica aziendale.
4. È vietato **divulgare, copiare o trasferire dati sensibili** o riservati senza autorizzazione esplicita, incluse informazioni relative a clienti, fornitori o enti pubblici.
5. È vietato **diffondere virus o programmi dannosi** che possano compromettere la sicurezza dei sistemi informatici aziendali o di terzi.

4. Divieti trasversali alle fattispecie di Delitti informatici e trattamento illecito di dati

➤ ***Legalità e trasparenza***

- Ogni attività aziendale deve essere svolta nel pieno rispetto delle leggi, regolamenti e delle procedure interne (ISO 9001, ISO 45001, Modello 231, Codice Etico).



➤ **Diligenza e responsabilità nell'utilizzo dei sistemi informatici**

- Tutti i dipendenti, collaboratori e dirigenti devono agire con diligenza e responsabilità nello svolgimento delle loro mansioni, con particolare riferimento all'utilizzo dei sistemi informatici, evitando comportamenti che possano esporre il Consorzio a rischi di violazioni normative.

➤ **Divieto di comportamenti illeciti**

- È vietata ogni condotta finalizzata ad un utilizzo distorto o non autorizzato dei sistemi informatici al fine di ottenere indebiti vantaggi economici.

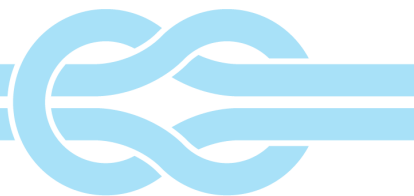
➤ **Riservatezza e protezione dei dati**

- I dati sensibili e riservati devono essere trattati in modo conforme alla normativa vigente (es. GDPR) e alle politiche aziendali, evitando accessi non autorizzati o divulgazioni indebite.

5. Aree sensibili nell'attività del Consorzio PSL

Di seguito un'analisi di rilevanza (sensibilità) delle singole Aree del Consorzio PSL rispetto ai reati presupposto di cui alla presente Sezione B.

AREA DI COMPETENZA	DENOMINAZIONE AREA NEL "SISTEMA 231"	SENSIBILITA' DELL'AREA
DIREZIONE GENERALE	A1	
RESPONSABILE DELLA SICUREZZA (RSPP) → Soggetto esterno	A2	
RESPONSABILE DEL SISTEMA DI GESTIONE INTEGRATO (Compliance)	A3	
RESPONSABILE GARE/TENDER - RESPONSABILE ACQUISTI	A4	
RESPONSABILE DIREZIONE OPERATIVA	A5	
RESPONSABILE AMMINISTRAZIONE E HR	A6	
RESPONSABILE COMMERCIALE E MARKETING → Soggetto esterno	A7	



Legenda:



Molto sensibile (Rischio elevato)



Abbastanza sensibile (Rischio medio)



Poco sensibile (Rischio basso)

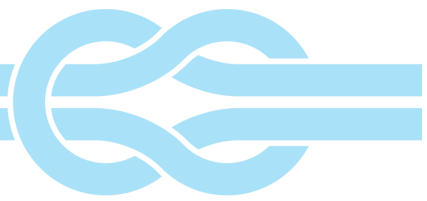
6. Presidi e procedure specifiche per attività a rischio

ATTIVITÀ A RISCHIO	PRESIDI E PROCEDURE
Gestione dei dati sensibili e informatici (per reati ex art. 24-bis)	• Protezione dei sistemi informatici: Implementare firewall, antivirus e sistemi di crittografia per proteggere i dati aziendali e dei clienti. Limitare l'accesso ai dati sensibili solo a personale autorizzato. Adozione di apposito Regolamento per l'utilizzo dei sistemi informatici aziendali. • Accesso ai sistemi: Ogni accesso ai sistemi aziendali deve essere autenticato e registrato. Implementare politiche di password sicure e aggiornamenti periodici dei sistemi e delle stesse password. • Monitoraggio dei log di accesso: Verifica regolare degli accessi ai sistemi aziendali e alle reti informatiche. • Formazione del personale: Organizzare corsi periodici per sensibilizzare i dipendenti sui rischi informatici e sulla gestione sicura dei dati.

7. Compiti dell'Organismo di Vigilanza

Al fine di assicurare il rispetto del Modello 231 e di prevenire il verificarsi di condotte idonee ad integrare i reati presupposto di cui alla presente Sezione B, l'Organismo di Vigilanza del Consorzio P.S.L. è tenuto a:

- Verificare periodicamente – ove necessario con il supporto di professionisti del settore IT - il livello di sicurezza del sistema informatico aziendale e le misure di volta in volta prese per il mantenimento del miglior standard di sicurezza;



- Esaminare eventuali segnalazioni specifiche e/o obbligatorie provenienti dagli organi di controllo o da terzi o da qualsiasi Responsabile di area ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute, anche ai sensi della disciplina del *Whistleblowing* di cui alla Direttiva UE 1937/2019, recepita con D.Lgs. 24/2023;
- Effettuare un monitoraggio periodico delle procedure aziendali di controllo al fine di suggerire alle competenti funzioni aziendali un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative;
- Verificare il rispetto delle indicazioni previste nelle procedure aziendali anche in relazione ai flussi informativi nei confronti dell'O.d.V.
- Pianificare audit periodici con i Responsabili delle diverse aree aziendali;
- Vigilare sull'efficacia e l'adeguatezza del Modello e proporre eventuali modifiche e/o aggiornamenti;
- Predisporre un piano formativo dedicato al personale aziendale in materia di Modello 231;
- Svolgere una regolare attività di reporting nei confronti del Consiglio di Amministrazione.