PARTE SPECIALE D

REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI

(ART. 24 BIS DEL D. LGS.231/01)

1. Le fattispecie di reato

La presente Parte Speciale riguarda i reati informatici di cui all'art. 24-bis del D.Lgs. 231/2001 e descrive le fattispecie rilevanti ai fini della responsabilità amministrativa di Assindustria S.r.l. Identifica inoltre le attività "sensibili" emerse dal *risk assessment*, indicando i principi comportamentali e i presidi di controllo per organizzare, gestire e svolgere correttamente tali attività.

2. Tipologie di reato

Si riportano di seguito una breve descrizione delle fattispecie di reato potenzialmente realizzabili nel contesto della Assindustria S.r.l.

FALSO IN DOCUMENTI INFORMATICI (art. 491-bis c.p.)

L'art. 491-bis c.p. estende le norme sulla falsità in atti pubblici e scritture private ai documenti informatici. Si applica ai documenti informatici aventi efficacia probatoria, equiparandoli a quelli tradizionali. La norma serve a colmare il vuoto normativo rispetto alla crescente digitalizzazione. Chi commette falsità su documenti informatici è punito come se la falsità riguardasse documenti cartacei.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (art. 615-ter c.p.)

L'articolo punisce chiunque si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, o vi si mantenga contro la volontà di chi ha il diritto di escluderlo. Il reato sussiste anche in assenza di danneggiamenti o sottrazioni di dati e prevede aggravanti se commesso da soggetti qualificati o con strumenti fraudolenti.

DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, CODICI E ALTRI MEZZI ATTI ALL'ACCESSO A SISTEMI INFORMATICI O TELEMATICI (art. 615-quater c.p.)

Il codice penale punisce chiunque, abusivamente, detiene, diffonde o comunica codici, parole chiave o altri strumenti idonei ad accedere a un sistema informatico o telematico protetto. Il reato si configura anche senza che avvenga un accesso effettivo, essendo sufficiente la disponibilità o la divulgazione non autorizzata degli strumenti.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (art. 617-quarter c.p.)

L'art. 617-quater c.p. prevede il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. È punito chi, fraudolentemente, intercetta comunicazioni relative a un sistema informatico o telematico, ovvero le impedisce o interrompe. La norma tutela la riservatezza e la libertà delle comunicazioni digitali.

DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE E DI ALTRI MEZZI ATTI A INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (art. 617-quinquies c.p.)

Il suddetto articolo punisce chi, al fine di procurare a sé o ad altri un vantaggio o di arrecare danno, installa apparecchiature o altri strumenti idonei a intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Il reato si configura anche se l'intercettazione non viene effettivamente realizzata, rilevando già l'installazione degli strumenti.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (art. 635-bis c.p.)

Il reato si configura quando un soggetto distrugge, deteriora o rende inutilizzabile un dato, un'informazione o un programma contenuti in un sistema informatico o telematico, compromettendo così il normale funzionamento del sistema. La norma tutela l'integrità e la disponibilità delle risorse informatiche.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI PUBBLICI O DI INTERESSE PUBBLICO (art. 635-ter c.p.)

Il reato punisce un soggetto quando distrugge, deteriora, danneggia o rende inaccessibile un sistema informatico o telematico, compromettendone il funzionamento. La norma tutela la sicurezza e l'affidabilità delle infrastrutture tecnologiche, prevedendo sanzioni per chi ne pregiudica l'integrità.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (art. 635-ter c.p.)

L'art. 635-quater c.p. sanziona chi, mediante le condotte previste dall'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, danneggia o distrugge strumenti o dispositivi informatici utilizzati per il trattamento, l'elaborazione o la trasmissione di dati. Il reato si configura quando tale danneggiamento impedisce o compromette l'utilizzo corretto di tecnologie destinate a gestire informazioni, proteggendo così la funzionalità e la sicurezza delle infrastrutture digitali.

DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (art. 635-quater c.p.)

La disposizione sanziona chi danneggia o distrugge strumenti o dispositivi informatici utilizzati per il trattamento, l'elaborazione o la trasmissione di dati. Il reato si configura quando tale danneggiamento impedisce o compromette l'utilizzo corretto di tecnologie destinate a gestire informazioni, proteggendo così la funzionalità e la sicurezza delle infrastrutture digitali.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICO INTERESSE (art. 635-quinquies c.p.)

L'art. 635-quinquies c.p. punisce chi alteri il contenuto di dati informatici o telematici mediante le condotte di cui all'art. 635-bis, con l'intento di danneggiare, travisare o compromettere l'integrità delle informazioni o il corretto funzionamento del sistema. Il reato si configura anche quando l'alterazione è finalizzata a ingannare o a causare danni a persone o enti.

FRODE INFORMATICA (art. 640-ter c.p.)

L'articolo punisce chi, mediante fraudolente modifiche di dati informatici o telematici, causa un danno patrimoniale a terzi. Il reato si configura quando il soggetto, alterando in modo illecito il contenuto di dati o informazioni, provoca un inganno che incide sui diritti patrimoniali altrui, con la finalità di ottenere vantaggi economici indebiti o di danneggiare l'altrui patrimonio.

FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA (art. 640-quinquies c.p.)

L'art. 640-quinquies c.p. punisce chi offre servizi di certificazione di firma elettronica violando gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Il reato si configura quando il soggetto, al fine di ottenere un ingiusto profitto per sé o per altri, o di causare danno a terzi, non rispetta le normative sulla certificazione della firma elettronica.

DISPOSIZIONI URGENTI IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA - DECRETO-LEGGE 21 SETTEMBRE 2019, N.105 COORDINATO CON LEGGE DI CONVERSIONE N.133 DEL 18 NOVEMBRE 2019 (art. 1, comma 11, del D. Lgs. n. 105 del 21 settembre 2019)

L'art. 1, comma 11, del D.Lgs. n. 105 del 21 settembre 2019 (attuativo della Direttiva UE 2016/1148 sulla sicurezza delle reti e dei sistemi informativi) stabilisce che i fornitori di servizi essenziali e i gestori di infrastrutture critiche sono obbligati ad adottare misure di sicurezza adeguate per proteggere i propri sistemi informatici e le reti contro i rischi di attacchi cibernetici. La disposizione si inserisce nel quadro della cybersecurity, prevedendo che tali misure di sicurezza siano proporzionate ai rischi connessi ai servizi e alle infrastrutture trattati.

In particolare, il comma stabilisce l'obbligo di implementare, senza indugi, meccanismi di protezione e di gestione delle vulnerabilità per prevenire potenziali attacchi. L'inosservanza di tale obbligo da parte dei soggetti coinvolti comporta la possibilità di sanzioni amministrative, comprese sanzioni pecuniarie.

Il reato o la responsabilità derivante dalla violazione di questa disposizione non è necessariamente collegato a un danno diretto, ma riguarda piuttosto il mancato rispetto degli standard di sicurezza, che può esporre a rischi anche indiretti, in particolare in relazione al trattamento di dati sensibili e alla protezione delle infrastrutture critiche.

Il legislatore, quindi, pone particolare enfasi sulla responsabilità preventiva e sull'adozione di misure adeguate da parte delle organizzazioni che gestiscono servizi essenziali e infrastrutture critiche, in linea con la crescente attenzione verso la protezione delle reti informatiche e dei dati.

2. Aree di rischio

Di seguito sono elencate le attività sensibili individuate nel corso della fase di diagnosi dei rischi connessi all'attività d'impresa posta in essere da Assindustria:

- **Gestione dei profili utente e del processo di autenticazione**
- **Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio**
- **Gestione e protezione della postazione di lavoro**
- **Gestione degli accessi da e verso l'esterno**
- **Gestione e protezione delle reti**
- **Gestione degli output di sistema e dei dispositivi di memorizzazione** (es. USB, CD)

3. Destinatari

La presente Sezione riguarda i comportamenti adottati dall'Amministratore, soggetti apicali, dipendenti, partner di Assindustria S.r.l., nonché da collaboratori esterni e

fornitori di servizi informatici in *outsourcing* (di seguito collettivamente indicati come "Destinatari"). L'obiettivo della presente Parte Speciale è garantire che tutti i Destinatari, come sopra individuati, adottino comportamenti conformi alle disposizioni stabilite, al fine di prevenire il verificarsi di reati informatici e il trattamento illecito di dati.

4. Principi generali di comportamento

Tutte le attività sensibili devono essere svolte nel rigoroso rispetto della normativa vigente, dei valori e delle politiche aziendali, delle procedure operative interne, nonché delle disposizioni contenute nel Modello di Organizzazione, Gestione e Controllo e nella presente Parte Speciale. L'intero sistema di organizzazione e controllo di Assindustria si fonda su principi essenziali quali l'attribuzione chiara delle responsabilità, la corretta rappresentanza, la separazione delle funzioni operative e di controllo, nonché sui valori di lealtà, trasparenza, correttezza e tracciabilità dei processi decisionali e operativi.

Nel contesto delle attività esposte al rischio di commissione di reati informatici e, più in generale, nello svolgimento delle proprie funzioni, l'Amministratore, i dipendenti, i collaboratori e le controparti contrattuali operanti per conto della Società sono tenuti a conformarsi agli standard generali di controllo, ai principi comportamentali contenuti nel Codice Etico, alla normativa interna e alle disposizioni di legge applicabili.

La presente Parte Speciale si riferisce espressamente alle condotte rilevanti poste in essere dai destinatari del Modello nell'ambito delle aree aziendali individuate come a rischio di reati informatici, e ha lo scopo di rafforzare la prevenzione mediante l'adozione di comportamenti improntati alla diligenza, correttezza e conformità normativa.

A tal fine, è fatto espresso divieto ai soggetti coinvolti di porre in essere, anche indirettamente, condotte che possano costituire o agevolare la realizzazione delle fattispecie di reato richiamate all'art. 24-bis del D.Lgs. n. 231/2001, nonché di agire in contrasto con le procedure aziendali o con i principi espressi nella presente Parte Speciale.

La prevenzione dei reati informatici è garantita da un insieme coordinato di misure tecniche, organizzative e regolamentari. Tra queste si annoverano:

- la **previsione**, all'interno del Codice Etico, di **specifiche indicazioni volte a prevenire l'uso illecito degli strumenti informatici;**

- l'**adozione di un sistema sanzionatorio** (o di vincoli contrattuali, in caso di soggetti terzi) **efficace e dissuasivo**;
- l'**utilizzo di tecnologie idonee a ridurre il rischio di commissione di reati**, in particolare nelle aree operative più esposte;
- la **realizzazione di attività formative e informative** mirate ad accrescere la consapevolezza del personale sui rischi legati all'utilizzo improprio delle risorse digitali aziendali.

Conseguentemente, tutti i soggetti coinvolti nello svolgimento delle attività a rischio sono tenuti a rispettare i principi generali di controllo su cui si fondano gli strumenti e le metodologie adottate per la costruzione dei presidi specifici. Tali principi, di seguito elencati, costituiscono presupposto imprescindibile per una gestione conforme alle normative e finalizzata alla prevenzione dei reati informatici:

- *Segregazione delle attività*
  Deve essere garantita la separazione funzionale tra le diverse fasi operative dei processi esposti a rischio, in modo che le attività di autorizzazione, esecuzione e controllo siano attribuite a soggetti differenti. È necessario, ad esempio, che siano separati i compiti di progettazione ed esercizio, oppure quelli relativi all'acquisto di beni e alla loro contabilizzazione.
- *Esistenza di procedure*
  Devono essere presenti e correttamente adottate disposizioni aziendali e procedure formalizzate, in grado di definire principi comportamentali e modalità operative per la corretta esecuzione delle attività sensibili. Tali procedure devono stabilire in maniera chiara responsabilità, ruoli e controlli specifici.
- *Poteri autorizzativi e di firma*
  I poteri di autorizzazione e di firma devono essere definiti in modo coerente rispetto alla criticità delle attività e conformi alla struttura organizzativa, assicurando una proporzionalità tra livello di responsabilità e potere attribuito.
- *Tracciabilità*
  Tutte le attività svolte sui sistemi informatici connessi a processi sensibili devono essere tracciabili. Ogni operazione rilevante deve essere registrata in modo da consentire la verifica ex post dei processi decisionali e operativi. Devono inoltre essere regolamentate le condizioni per l'eventuale cancellazione o distruzione delle registrazioni.
- *Gestione delle segnalazioni*

Deve essere attivato un sistema efficace di raccolta, analisi e gestione delle segnalazioni relative a comportamenti a rischio o sospetti, provenienti sia da soggetti interni che esterni all'organizzazione.

- *Riporto all'OdV*
  Ogni irregolarità o anomalia riscontrata nello svolgimento delle attività a rischio deve essere prontamente comunicata all'Organismo di Vigilanza, affinché siano attivati i controlli e le verifiche del caso.

5. Procedure di attuazione dei comportamenti prescritti

I Destinatari del presente Modello, in ragione delle rispettive funzioni e responsabilità e in conformità alle disposizioni del Regolamento (UE) 2016/679 nonché alla normativa nazionale in materia di protezione dei dati personali, sono tenuti a osservare specifici principi di condotta. In tale ambito, è fatto obbligo:

- al Responsabile di settore di segnalare tempestivamente ogni accesso non autorizzato al sistema informatico aziendale;
- ai dipendenti, dirigenti e amministratori di attenersi scrupolosamente alle istruzioni operative impartite in relazione al trattamento dei dati e alla sicurezza informatica, con particolare riferimento a:
  - l'uso corretto dei personal computer aziendali;
  - l'accesso e l'utilizzo della rete aziendale;
  - la gestione e l'assegnazione delle credenziali di autenticazione;
  - l'utilizzo e la conservazione di dispositivi rimovibili;
  - l'impiego dei computer portatili aziendali;
  - le misure di protezione antivirus;
  - le policy aziendali in materia di software;
  - l'utilizzo appropriato della posta elettronica;
  - l'accesso alla rete Internet e l'utilizzo dei relativi servizi;
  - il rispetto delle policy in materia di riservatezza, privacy e tutela del know-how aziendale.

È, altresì, fatto espresso divieto ai Destinatari di porre in essere, direttamente o indirettamente, le seguenti condotte:

- alterare, manipolare o falsificare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere in modo abusivo a sistemi informatici o telematici di soggetti pubblici o privati;
- accedere indebitamente al proprio sistema informatico con l'intento di modificare, cancellare o manipolare dati o informazioni;

- detenere o utilizzare senza autorizzazione codici di accesso, parole chiave o altri strumenti idonei all'intrusione in sistemi informatici di terzi, pubblici o privati, al fine di acquisire dati riservati;
- intercettare, impedire o interrompere fraudolentemente comunicazioni relative a sistemi informatici o telematici di soggetti pubblici o privati, con lo scopo di ottenere informazioni riservate;
- alterare, cancellare o danneggiare dati, informazioni o programmi informatici aziendali, con o senza accesso abusivo ai sistemi.

6. Protocolli di prevenzione

La Società ha adottato un sistema di controlli interni finalizzato alla prevenzione dei reati informatici, fondato su un insieme coordinato di strumenti organizzativi, tecnici e procedurali.

L'Organismo di Vigilanza è incaricato di verificare che le procedure aziendali siano effettivamente conformi ai principi e alle prescrizioni contenute nella presente Sezione del Modello.

È fatto obbligo a chiunque venga a conoscenza di violazioni del Modello, del Codice Etico o delle procedure adottate in tema di prevenzione dei reati informatici, di segnalarle tempestivamente all'Organismo di Vigilanza mediante i canali di comunicazione dedicati.