PARTE SPECIALE - B -

REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI
ex art. 24-bis D.lgs. 231/2001

Indice

1. CONTESTO, OBIETTIVI E FUNZIONE DELLA PARTE SPECIALE

Per effetto della Legge 18 marzo 2008, n. 48, è stato ampliato l'originario catalogo dei reati-presupposto della responsabilità dell'ente, introducendo i reati informatici a tutela dell'integrità dei sistemi informativi e dei servizi informatici delle Amministrazioni Pubbliche, degli enti e dei soggetti pubblici e privati da cui dipendono l'esercizio di funzioni e servizi fondamentali per lo Stato, per le attività sociali ed economiche.

Pertanto, si registrano successivi interventi legislativi volti ad assicurare un elevato livello di sicurezza delle reti e dei sistemi informatici, istituendo il c.d. perimetro di sicurezza nazionale cibernetica – cfr. D.L. 105 del 21 settembre 2019, convertito in L. 18 novembre 2019, n. 133. A ciò si aggiunga la più recente Legge n. 90/2024 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", con

modifiche integrative delle fattispecie di reato previste dall'art. 24-bis D.lgs 231/01 e finalizzate ad inasprire le sanzioni applicabili ai reati informatici commessi dall'ente.

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Destinatari del Modello (Organi Sociali, Dipendenti, Consulenti, Partner, etc.), come definiti nella Parte Generale, coinvolti nelle "aree/processi/attività sensibili", ossia di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui all'art. 24 bis del Decreto n. 231/2001.

Obiettivo del presente documento è che i Destinatari del Modello, nella misura in cui gli stessi possano essere coinvolti nelle Attività Sensibili di seguito indicate, si attengano a principi e regole di condotta, generali e specifiche, al fine di prevenire e impedire il verificarsi dei reati informatici.

A tale fine, verranno indicati nel proseguo:
a) le attività e/o i processi aziendali definiti "sensibili" ovvero esposti al rischio potenziale di commissione del reato presupposto oggetto della presente Parte Speciale;
b) le regole e i principi generali di condotta nonché i protocolli interni, quali controlli specifici, che dovranno essere seguiti per prevenire e limitare la possibile commissione delle fattispecie delittuose mappate e comunque per gestire eventuali criticità che dovessero verificarsi.

2. LE MACROCATEGORIE DEI REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI AI SENSI DEL D. LGS. n. 231/2001: CONTESTO

La presente Parte Speciale, tra i reati presupposto sanzionabili ai sensi del Decreto Legislativo n. 231/2001, si riferisce ai reati informatici e trattamento illecito di dati (art. 24-bis) [articolo aggiunto articolo aggiunto dalla L. n. 48/2008].

Per conoscere la definizione e gli elementi costitutivi delle fattispecie di reato, *ex* D.Lgs. 231/01, rientranti nella presente Parte Speciale, si veda l'allegato 3.

3. LE FATTISPECIE *ex* ART. 24-BIS D. LGS. N. 231/2001 ATTINENTI AL CONTESTO DI C.I.A.P.I.

Sulla base delle analisi documentali condotte nonché all'esito delle informazioni raccolte durante gli incontri con i referenti aziendali, C.I.A.P.I. ha ritenuto ipotizzabili per il proprio contesto le seguenti fattispecie di reato rientranti nella macrocategoria analizzata:

FATTISPECIE DI REATO *EX* D. LGS. N. 231/2001 ATTINENTI AL CONTESTO DI C.I.A.P.I.	ART. 24-bis
	Documenti informatici (art. 491-bis c.p.)
	Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
	Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.)
	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
	Estorsione informatica (art. 629 c.p.)

4. LE AREE SENSIBILI/ATTIVITA' ESPOSTE AL POTENZIALE RISCHIO DEI REATI INFORMATICI E LE FUNZIONI AZIENDALI POTENZIALMENTE COINVOLTE

Dall'approfondito processo di analisi delle attività concrete poste in essere da C.I.A.P.I., le principali Attività Sensibili che la Società ha individuato al proprio interno e le relative funzioni aziendali potenzialmente coinvolte sono le seguenti:

MACRO-PROCESSO	ATTIVITA' SENSIBILI	FUNZIONI AZIENDALI COINVOLTE
Direzione	- Gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa	- Servizio economico finanziario; - Ufficio Servizi alla formazione; - Risorse Umane e Affari Generali; - Ufficio Gestione Sistemi di Qualità
Segreteria di Direzione	- Supporto alle attività del CdA e della Direzione	- Direzione - CdA

MACRO-PROCESSO	ATTIVITA' SENSIBILI	FUNZIONI AZIENDALI COINVOLTE
	- Controllo e Gestione della corrispondenza in entrata e in uscita - Ricezione, screening candidature e contrattualizzazione consulenti esterni	- Assicurazione Qualità - Responsabili UOB - Ufficio del personale - Servizi alla formazione - Servizio economico-finanziario
Assicurazione Qualità	- Gestione, aggiornamento e controllo del Sistema Qualità - Gestione dei rapporti con i fornitori	- Direzione - Responsabili UOB - Servizi alla formazione - Ufficio servizi alla formazione - Servizio economico-finanziario - Responsabile acquisti
Manutenzione	- - Gestione dei rapporti con Assessorato regionale, Demanio e Protezione Civile per la gestione del patrimonio immobiliare	- RSPP - Direzione
Risorse Umane	- Gestione amministrativa del personale ed elaborazione cedolini - Gestione dei rapporti con i sindacati - Organizzazione e budgeting / pianificazione costi del personale	- Segreteria di direzione - Gestione dei sistemi di qualità - Ufficio Contabilità generale - Ufficio servizi alla formazione - - Ufficio Affari Generali
Servizi alla formazione	- Gestione del processo di erogazione dell'attività formativa	- Direzione - Responsabile Assicurazione Qualità - Ufficio del Personale - - Ufficio Progettazione
Servizio economico-finanziario	- Gestione del processo di approvvigionamento di beni e servizi - Predisposizione del bilancio annuale, del bilancio preventivo e del conto consuntivo - Gestione degli adempimenti fiscali - Gestione della contabilità	- Ufficio Contabilità generale - Ufficio contabilità corsi - Risorse Umane e Affari Generali - Segreteria di Direzione - Servizi alla formazione - Direzione

MACRO-PROCESSO	ATTIVITA' SENSIBILI	FUNZIONI AZIENDALI COINVOLTE
		- Responsabile ufficio Magazzino - Responsabile assicurazione qualità

5. REGOLE E PRINCIPI GENERALI DI CONDOTTA DI NATURA PREVENTIVA

Nell'espletamento delle attività aziendali e, in particolare, nello svolgimento delle Attività Sensibili elencate al precedente paragrafo n. 4, è richiesto il rispetto dei principi di comportamento di seguito indicati e al pari è espressamente vietato attuare, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle oggetto della presente Parte Speciale (art. 24-*bis* del Decreto).

In particolare, nell'espletamento delle attività sensibili è fatto obbligo seguire i seguenti principi:

- attenersi alle procedure aziendali di conservazione documentale e alle disposizioni del Codice di condotta in materia di utilizzo delle risorse informatiche;
- garantire il regolare funzionamento delle attività di competenza;
- mettere in atto e rendere operativo il principio di segregazione dei compiti e delle funzioni anche attraverso la formalizzazione e la predisposizione di specifiche procedure interne;
- garantire la tracciabilità documentale di tutte le operazioni e attività effettuate, rispettando gli obblighi di archiviazione come da procedure interne;
- adottare misure volte garantire la massima riservatezza sulle informazioni raccolte nei sistemi informativi;
- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dal C.I.A.P.I. e per le specifiche finalità assegnate;
- garantire la tracciabilità documentale di tutte le operazioni e attività effettuate, rispettando gli obblighi di archiviazione come da procedure interne;
- utilizzare e gestire correttamente i contenuti dei siti internet impiegati nello svolgimento delle attività di competenza;

- definire, mantenere nel continuo e diffondere a tutti gli stakeholders le modalità di comportamento da assumere per un corretto e lecito utilizzo dei software e delle banche dati in uso;
- controllare periodicamente la regolarità delle licenze dei prodotti in uso, procedendo, ove necessario, ai rinnovi;
- seguire le prescrizioni interne e presentare denuncia all'Autorità Giudiziaria preposta in caso di smarrimento o furto di apparecchiatura informatica fornita in dotazione da C.I.A.P.I. per motivi lavorativi;
- custodire gli strumenti tecnico/informatici, forniti in dotazione da C.I.A.P.I. per motivi lavorativi, in modo tale da impedire a chiunque l'accesso non autorizzato;
- conservare in forma riservata la propria password per l'accesso agli strumenti tecnico/informatici forniti in dotazione da C.I.A.P.I. per motivi lavorativi;
- segnalare senza ritardo alle funzioni competenti e nel rispetto delle procedure interne, eventuali utilizzi e/o funzionamenti anomali delle risorse tecnico/informatiche fornite in dotazione da C.I.A.P.I.

Al pari, nell'espletamento delle attività sensibili è fatto divieto di:

- alterare il contenuto di comunicazioni/documenti informatici anche aventi efficacia probatoria;
- introdursi in un sistema informatico o telematico in assenza di un'autorizzazione dal responsabile dell'UOB competente;
- danneggiare o rendere inservibili sistemi informatici o telematici di pubblico interesse;
- acquisire fraudolentemente informazioni riservate mediante intercettazione, impedimento o interruzione di comunicazioni trasmesse tramite un sistema informatico o telematico utilizzato da C.I.A.P.I. nell'espletamento delle proprie attività
- installare software sui dispositivi informatici assegnati da C.I.A.P.I., in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano la licenza d'uso;
- utilizzare o installare strumenti tecnico/informatici (software e/o hardware) per attività di intercettazione, falsificazione, danneggiamento, alternazione o soppressione del contenuto di comunicazioni e/o documenti informatici pubblici o privati;
- diffondere immagini, documenti o altro materiale tutelato dalla normativa in materia di diritto d'autore, tramite strumenti aziendali, tra cui, in particolare, il sito internet e la intranet aziendale;
- effettuare copie non specificamente autorizzate di dati e di software aziendali;

- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni di proprietà di C.I.A.P.I. o comunque attinenti al contesto lavorativo dell'azienda;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, e/o al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- visitare siti internet che contengono materiale recante offesa al pudore, alla pubblica decenza o istigazione alla realizzazione o rappresentazione di condotte criminali in genere;
- trasmettere o scaricare, dalla rete internet, materiale considerato osceno, pornografico, minaccioso o che possa molestare la razza o la sessualità o, comunque tale da arrecare offesa, di qualsiasi natura, alla persona;
- utilizzare strumenti di IA per fini lavorativi in violazione delle istruzioni impartite da C.I.A.P.I. e nel rispetto dei principi di etica digitale.

6. STRUMENTI DI CONTROLLO INTERNI IMPLEMENTATI DA C.I.A.P.I.

Al fine di presidiare le Attività Sensibili e prevenire il rischio di commissione dei reati oggetto della presente Parte Speciale, in C.I.A.P.I. vengono attuati i principi e i divieti elencati al precedente parag. 5 oltre che i protocolli previsti dalla Parte Generale del Modello di Organizzazione, Gestione e Controllo e nel Codice di Comportamento della Regione Siciliana e degli Enti di cui all'art. 1 della L. R. n.10/2000.

A tal fine, C.I.A.P.I. è dotata di strumenti organizzativi improntati a principi generali di:

- formale delimitazione dei ruoli e delle responsabilità, con una descrizione dei compiti di ciascuna funzione;
- precisa indicazione delle linee di riporto;
- conoscibilità, trasparenza e pubblicità dei poteri attribuiti sia verso l'interno che verso l'esterno.

I principi cui si ispirano tali Presidi Specifici vengono indicati nella tabella che segue:

PRESIDI GENERICI E TRASVERSALI	PRESIDI SPECIFICI
➢ Statuto Sociale ➢ Organigramma – Rappresentazione di più livelli di controllo delle attività svolte	Procedure, istruzioni operative e prassi consolidate che definiscono ruoli e responsabilità delineando chi

➢ Controllo analogo della Regione Siciliana - Il controllo analogo delle Società Partecipate consiste nel comando sulle iniziative e nel controllo delle azioni delle Società Partecipate, da parte degli Enti Pubblici titolari di quote sociali mediante il quale si perseguono obiettivi che impattano su: - Trasparenza e responsabilità; - Gestione delle risorse; - Prevenzione della corruzione ➢ Revisore Unico – che garantisce la verifica sulla regolarità contabile e la corretta rilevazione dei fatti di gestione delle scritture contabili ➢ Certificazione UNI EN ISO 9001 ➢ Piano Triennale Anticorruzione e Trasparenza ➢ Modello di Organizzazione Gestione e Controllo 231 ➢ Whistleblowing	e come debba svolgere l'attività di competenza, definendo i diversi livelli di controllo. In particolare, quali presidi di controllo specifici a valere sui reati informatici, C.I.A.P.I. ha adottato: - PQ 05 Procedura di Gestione della documentazione e della registrazione della Qualità
	Convenzioni stipulate con l'Assessorato Regionale della Famiglia, delle Politiche Sociali e del lavoro – Dipartimento del lavoro, dell'impiego, dell'orientamento, dei servizi e delle attività formative
	Albo di fornitori qualificati
	Software di archiviazione documentale
	Software PEC

7. LE FATTISPECIE DELLE MACROCATEGORIE EX ART. 24-BIS NON ATTINENTI AL CONTESTO DI C.I.A.P.I.

Il processo di analisi delle attività, per quanto insussistente il rischio "0" di potenziale commissione di un reato, ha condotto C.I.A.P.I., in considerazione della natura delle attività stesse e/o degli elementi costitutivi dei reati medesimi (ritenuti, in ogni caso, ragionevolmente gestiti dal rispetto dei principi e regole enunciati nel Codice di comportamento dei dipendenti della Regione Siciliana e degli Enti di cui all'art. 1 della Legge Regionale 15 maggio 2000, n.10) e/o della mancanza di interesse e vantaggio, a ritenere remota o non ipotizzabile, all'interno della macrocategoria *ex* art. 24-bis, la commissione delle seguenti singole fattispecie di reato:

FATTISPECIE DI REATO *EX* D. LGS. N. 231/2001 NON ATTINENTI AL	ART. 24-bis
	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)
	Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere

CONTESTO DI C.I.A.P.I.	comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
	Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
	Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
	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.)
	Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
	Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

8. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Al fine di consentire all'Organismo di Vigilanza, di svolgere in modo effettivo la propria attività di sorveglianza e di prevenzione dei reati, preme evidenziare e ribadire che nell'espletamento delle Attività Sensibili diviene importante il rispetto delle regole dettate nella Parte Generale del Modello di Organizzazione, Gestione e Controllo, prestando particolare attenzione a quelle relative ai flussi informativi verso l'Organismo di Vigilanza.

Sul punto, le Funzioni aziendali coinvolte nello svolgimento delle Attività Sensibili mappate sono tenute ad inoltrare all'Organismo di Vigilanza, secondo le modalità indicate nella suddetta Parte Generale, e in ogni caso tempestivamente, ogni informazione utile che descriva:

- una possibile violazione del Modello conseguente alla commissione di un reato presupposto;
- un potenziale rischio di commissione di un reato presupposto informatico;
- la commissione di un reato presupposto informatico;
- eventuale svolgimento di attività non allineate alle procedure/istruzioni aziendali e relativa motivazione;

L'importanza dei flussi informativi verso l'Organismo di Vigilanza assume, peraltro, particolare rilievo laddove C.I.A.P.I. intraprenda o attui attività di business o strategie

aziendali eccezionali o straordinarie che possono esporre astrattamente la Società al rischio reato.

I Responsabili delle attività sensibili trasmettono all'OdV le informazioni indicate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili.

Inoltre, i responsabili coinvolti sono tenuti a segnalare prontamente/tempestivamente all'OdV tutti quei comportamenti e quei fatti che, quand'anche non determinino la produzione di un illecito, comportano uno scostamento rispetto a quanto previsto dai protocolli di controllo.