PARTE SPECIALE H

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

1. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

1.1 TIPOLOGIE DI REATI

La presente Parte Speciale è dedicata ai principi di comportamento e di controllo relativi ai delitti informatici e trattamento illecito di dati, così come individuati nell'articolo 24-*bis* del Decreto.

Le fattispecie prese in considerazione dal Decreto Legislativo sono le seguenti:

- Art. 491-*bis* c.p.	Documenti informatici;
- Art. 615-*ter* c.p.	Accesso abusivo ad un sistema informatico o telematico;
- Art. 615-*quater* c.p.	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici;
- Art. 615-*quinquies* c.p.	Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- Art. 617-*quater* c.p.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- Art. 617-*quinquies* c.p.	Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- Art. 635-*bis* c.p.	Danneggiamento di informazioni, dati e programmi informatici;
- Art. 635-*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-*quater* c.p.	Danneggiamento di sistemi informatici o telematici;

- Art. 635-*quinquies* c.p.	Danneggiamento di sistemi informatici o telematici di pubblica utilità;
- Art. 640 quinquies c.p.	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica;
- Art. 1, co. 11, D. L. n. 105/2019	Ostacolo o condizionamento dei procedimenti per la Sicurezza Cibernetica e delle relative attività ispettive e di vigilanza.

1.2 AREE DI RISCHIO

In relazione ai reati sopra elencati, le aree di attività di rischio che, potenzialmente, potrebbero presentare profili di maggiore criticità con riferimento ai delitti informatici e al trattamento illecito di dati riguardano la gestione e il monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito dei quali sono ricomprese le seguenti attività:

- gestione del profilo utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi verso l'esterno e/o verso l'interno tramite la rete internet;
- protezione delle reti (sicurezza cablaggi, dispositivi di rete, ecc.);
- gestione degli *output* di sistema e dei dispositivi di memorizzazione;
- installazione di programmi e dispositivi;
- gestione del processo di conservazione sostitutiva documentale.

I soggetti e/o le funzioni potenzialmente coinvolti sono tutti i Destinatari.

1.3. PRINCIPI DI COMPORTAMENTO

In via generale, nell'esercizio delle attività e delle mansioni ad essi affidate, i Destinatari devono astenersi dal realizzare, collaborare o dare causa alla realizzazione di comportamenti che possano integrare o comunque agevolare la commissione delle fattispecie di reato di cui alla presente Parte Speciale.

I Destinatari, nell'ambito delle rispettive competenze e funzioni, devono astenersi dal:

- porre in essere o collaborare alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato qui contemplate;
- divulgare informazioni relative ai sistemi informatici aziendali;

- utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta.

In particolare, è fatto espresso divieto di:

a. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
c. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
d. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
e. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o *software* allo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
f. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
g. installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
h. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
i. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
j. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i Destinatari devono:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- assicurare la protezione dei sistemi e delle informazioni da potenziali attacchi informatici;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi, evitando che terzi soggetti possano venirne a conoscenza;

- non prestare o cedere a terzi qualsiasi apparecchiatura informatica;
- evitare di trasferire all'esterno della Società e/o trasmettere *files*, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio *computer* oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc.…);
- evitare l'utilizzo di *password* di altri utenti aziendali, anche per l'accesso ad aree protette in nome e per conto degli stessi;
- evitare l'utilizzo di strumenti *software* e/o *hardware* atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di *software*;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione di dati della Società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

1.4 FLUSSI INFORMATIVI VERSO L'ODV

Tutti i Destinatari coinvolti nella gestione dei sistemi informativi devono segnalare all'Organismo di Vigilanza qualsiasi eccezione comportamentale rispetto alle regole sopra indicate, nonché a quelle riportate nel Codice Etico e inoltre:

- eventuali tentativi di atti di "pirateria" accertati sui sistemi informativi;
- utilizzo di password non autorizzate, nonché scambi delle stesse tra soggetti diversi;
- intercettazione di modifiche non autorizzate da parte degli utenti.