MODELLO ORGANIZZATIVO

di proprietà di

T.I. LOG Srl

P.IVA 10620390962

Sede Legale:

Via Dante, 14 20121 Milano

Sede Operativa:

Via Marona, 33 26025 Pandino -CR-

PARTE SPECIALE 2

Delitti informatici e trattamento illecito di dati (ex Art. 24-bis, D.Lgs. n. 231/2001)

Gestione del documento

Il documento si trova in **Ed. 01 Rev. 00**

Redazione	Dott. G. De Rosa		
Verifica ed Emissione	OdV		
Approvazione	Legale Rappresentante		

Elenco delle Edizioni e Revisioni

Edizione	**Revisione**	**Data**	**Oggetto della Revisione**
01	00	31.05.2021	Prima Stesura

Sommario

1. Il reato posto a catalogo

Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019]

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

2. Le fattispecie di reato previste

Documenti informatici (art. 491-bis c.p.)

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.

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

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

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

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo , è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a due anni e della multa da cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater.

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

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329..

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

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617quater

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

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

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.)

Salvo che il fatto costituisca piu' grave reato, chiunque commette 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(2), è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

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

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

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

Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento(3), la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Il 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, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attivita' ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attivita' ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, e' punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote.

3. Funzione della parte speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, dai dipendenti, nonché dai consulenti e partner, in relazione alle fattispecie di attività sensibili in relazione al reato presupposto.

Obiettivo della presente Parte Speciale è che tali soggetti mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente.

I presidi principali per l'attuazione delle vigenti previsioni normative sono stati individuati in:

a) un modello organizzativo e di controllo;

b) codice etico;

c) sistema sanzionatorio;

d) sistema di comunicazione.

Allo stesso modo sono stati individuati gli elementi caratteristici di ciascun presidio principale, ed in particolare:

- l'istituzione di un Organismo di Vigilanza autonomo ed indipendente cui è affidato il compito di controllare il grado di effettività, adeguatezza, mantenimento ed aggiornamento del modello organizzativo, di razionalizzare le procedure decisionali (in un'ottica di documentabilità e verificabilità), di adottare un sistema chiaro di riparto dei compiti e delle responsabilità, di rendere operativo il flusso di informazioni tra le diverse funzioni aziendali e dalle stesse all'Organismo medesimo, di predisporre un sistema di reporting dell'Organismo di Vigilanza verso gli Organi sociali;

- l'adozione di un codice etico e/o di un codice di condotta che costituisce la carta dei valori aziendali, debitamente diffuso a tutti i componenti della struttura aziendale ed ai Partner contrattuali, costantemente aggiornato;

- l'adozione di un sistema disciplinare volto a garantire efficacia ed effettività alle prescrizioni interne;

- la predisposizione di un sistema di comunicazione dettagliato, completo e costantemente monitorato attraverso, ad esempio, manuali operativi, piani di formazione del personale, reti intranet.

4. Le attività sensibili individuate

L'art. 6, comma 2, lett. a) del d.lgs. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal d.lgs. 231/2001.

L'analisi dei processi aziendali di **TILOG Srl** ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dagli artt. 24 e 25 del d.lgs. 231/2001.

Qui di seguito sono elencate le fattispecie di attività sensibili in relazione al reato presupposto.

In particolare, con riferimento ai reati oggetto della Presente Parte Speciale, sono stati individuati i seguenti Processi Sensibili:

1. Gestione dei profili utente

2. Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio attraverso apposizione di firma elettronica e/o di marcatura temporale

3. Gestione e protezione dei device (laptop, mobile phone, tablet, ecc) concessi in uso ai lavoratori

4. Gestione e protezione delle reti aziendali e della rete web

6. Gestione dei dispositivi di memorizzazione dei dati

7. Sicurezza fisica dei luoghi;

5. Funzioni aziendali coinvolte

Information Tecnology / Amministratore di sistema

Commerciale

Amministrazione e Controllo

Finanza

Audit

6. Sistema di prevenzione

Le attività in tutti i Processi Sensibili sono svolte conformandosi alle leggi vigenti, alle norme del Codice etico, ai valori e alla politica aziendale e, alle regole contenute nel Modello e nei protocolli attuativi dello stesso.

La società è dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

a. conoscibilità all'interno della società (ed eventualmente anche nei confronti delle altre società);

b. chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri e responsabilità (organigramma e mansionario definito);

c. chiara descrizione delle linee di riporto.

Le procedure interne sono caratterizzate dai seguenti elementi:

a. separatezza, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni");

b. traccia scritta di ciascun passaggio rilevante del processo;

c. adeguato livello di formalizzazione.

6.1 Principi generali di comportamento

Nello svolgimento delle proprie attività, oltre alle regole di cui al Modello e, in particolare, a quelli indicate ai successivi paragrafi gli Organi sociali, i Dirigenti e i Dipendenti dell'azienda, nonché i Consulenti e i Partner nell'ambito delle attività da essi svolte conoscono e rispettano:

- in generale, la normativa applicabile;
- i principi di Corporate Governance approvati dall'amministrazione aziendale;

- il Codice Etico;
- il sistema di controllo interno, e quindi le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti la struttura organizzativa aziendale e il sistema di controllo della gestione.

I divieti di carattere generale appresso specificati si applicano in via diretta agli Organi sociali, ai Dirigenti e ai Dipendenti dell'azienda, nonché ai Consulenti e ai Partner, in forza di apposite clausole contrattuali.

E' fatto divieto 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; è fatto altresì divieto di porre in essere comportamenti in violazione dei principi procedurali previsti nella presente parte speciale.

In particolare, **è fatto divieto** a dipendenti, Organi Sociali, Consulenti e Partner, di:

- diffondere dati personali e aziendali all'esterno dell'organizzazione;
- Introdurre in azienda device non autorizzati;
- manomettere le impostazioni dei device poste in essere dal resp. IT;
- Scaricare software o programmi sui device non autorizzati dal resp. IT;
- divulgare o cedere le proprie credenziali di accesso ai device / sistemi aziendali a colleghi / terzi parti;
- sottrarre dati dagli archivi informatici aziendali;
- esercitare attività di spam;
- alterare il funzionamento di sistemi informatici e telematici o manipolare i dati in esso contenuti.

6.2 Principi procedurali

Sono stabilite le seguenti regole:

- ai Dipendenti e ai componenti degli Organi sociali viene erogato formazione specifica in ordine alla corretta gestione e custodia delle proprie credenziali e ai profili di rischiosità presenti nella navigazione internet;
- Gli autorizzati al trattamento dei dati personali sono tutti formati ed hanno sottoscritto idoneo mandato;
- I responsabili del trattamento dei dati, ovvero coloro i quali gestiscono i dati in nome e per conto dell'ente, sono qualificati previamente e, in caso positivo di qualifica, viene fatto firmare idoneo mandato;

- I device sono tutti protetti con idonei antivirus e antimalware;
- I dati presenti nei device sono tutti crittografati;
- I luoghi di lavoro sono presidiati da sistemi anti-intrusione;
- Vengono reimpostati blocchi di navigazione su siti specifici;
- Gli apparati wireless vengono tutti dotati di chiave di accesso;
- Viene effettuato un controllo periodico dei log file da parte dell'amministratore di sistema;

7. Il sistema delle deleghe e delle procure

Il sistema delle deleghe e procure è caratterizzato da elementi di "certezza", ai fini della prevenzione dei reati, e consentire la gestione efficiente dell'attività aziendale.

Si intende per delega l'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

Si intende per procura il negozio giuridico unilaterale con cui la società attribuisce ad un singolo soggetto il potere di agire in rappresentanza della stessa nei confronti dei terzi.

Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza nei confronti di terzi viene conferita una procura di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la delega.

I requisiti essenziali del sistema di deleghe e procure sono i seguenti:

a) tutti coloro che intrattengono per conto dell'azienda rapporti con parti terze devono essere dotati di delega formale in tal senso e, ove occorra, anche di procura (i Consulenti e Partner devono essere in tal senso incaricati nello specifico contratto di consulenza o partnership);

b) a ciascuna procura che comporti il potere di rappresentanza delle società nei confronti dei terzi deve corrispondere una delega interna che descriva il relativo potere di gestione;

c) le deleghe devono coniugare ciascun potere alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;

d) ciascuna delega deve definire in modo specifico e in equivoco:

- i poteri del delegato, precisandone i limiti;
- il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;

e) al delegato devono essere riconosciuti poteri di spesa adeguati alle funzioni conferite;

f) la procura deve prevedere esplicitamente i casi di decadenza dai poteri conferiti;

g) il sistema delle deleghe e procure deve essere tempestivamente aggiornato.

L'Organismo di Vigilanza verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso vi siano anomalie.

8. I Controlli dell'Organismo di vigilanza

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si veda la Parte Generale del presente Modello), l'Organismo effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato reporting verso gli organi deputati, ecc.).

A tal fine, si ribadisce, che all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Di detti controlli l'Organismo riferisce all'Amministratore Delegato e/o Amministratore Unico dell'Azienda.

9. Lista di distribuzione

Il presente documento viene distribuito alle funzioni aziendali coinvolte attraverso la repository interna.

10. Archiviazione

Il presente documento viene archiviato per il termine di 10 anni.