Modello di organizzazione, gestione e controllo

ai sensi del D.Lgs. n. 231 del 8 giugno 2001

- PARTE SPECIALE -

04

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

art. 24*bis* d.lgs. n. 231/2001

SOMMARIO

1.0 - INTRODUZIONE AI REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI 3

2.0 - CRITERI PER LA DEFINIZIONE DEI REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. N. 231/01 - ART. 24*BIS* 3

2.1 - FALSITÀ IN DOCUMENTI INFORMATICI - ART. 491*BIS* C.P. 3
2.2 - ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO - ART. 615*TER* C.P. 4
2.3 - DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI - ART. 615 *QUATER* C.P. 5
2.4 - DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO - ART. 615*QUINQIES* C.P. 5
2.5 - INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE - ART. 617*QUATER* C.P. 6
2.6 - INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE - ART. 617*QUINQUIES* C.P. 6
2.7 - DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI - ART. 635*BIS* C.P. 7
2.8 - 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. 7
2.9 - DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI - ART. 635*QUATER* C.P. 7
2.10 - DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ - ART. 635*QUINQUIES* C.P. 8
2.11 - FRODE INFORMATICA - ART. 640*TER* C.P. 8
2.12 - FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA - ART. 640*QUINQUIES* C.P. 9
2.13 - DISPOSIZIONI URGENTI IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA 9

3.0 - LE ATTIVITÀ SENSIBILI RELATIVE AI REATI INFORMATICI 9

4.0 - ORGANI E FUNZIONI AZIENDALI COINVOLTE 10

5.0 - PRINCIPI E REGOLE DI COMPORTAMENTO 10

6.0 - PRINCIPI DI RIFERIMENTO SPECIFICI RELATIVI ALLA REGOLAMENTAZIONE DELLE ATTIVITÀ SENSIBILI 12

7.0 - I CONTROLLI DELL'ORGANISMO DI VIGILANZA 14

1.0 - Introduzione ai reati informatici e di trattamento illecito dei dati

Oggetto della presente sezione del MOGC 231 sono i **reati informatici**, ossia gli illeciti realizzati mediante l'utilizzo di sistemi informatici.

L'obiettivo della presente sezione di Parte Speciale (**04**) è che tutti i Dipendenti e gli altri soggetti eventualmente autorizzati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi degli illeciti in materia informatica.

Nello specifico, la presente Parte Speciale ha lo **scopo** di:

- indicare i **principi procedurali** e le regole di comportamento che i Dipendenti e gli altri soggetti eventualmente autorizzati sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza, nonché ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli **strumenti esecutivi** per esercitare le attività di controllo, monitoraggio e verifica.

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti.

2.0 - Criteri per la definizione dei reati informatici e di trattamento illecito dei dati. Le fattispecie di reato richiamate dal d.lgs. n. 231/01 - art. 24*bis*

Ad integrazione delle definizioni elencate nella Parte Generale del Modello, si consideri la seguente ulteriore definizione di "*Delitti Informatici*" come richiamati dall'art. 24*bis* del d.lgs. n. 231/2001 e disciplinati dal codice penale agli artt. **491-*bis*, 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*** e **640-*quinquies***.

La legge 18 marzo 2008, n. 48, ratificando la Convenzione di Budapest, ha ampliato le fattispecie di reato che possono generare la responsabilità delle società attraverso l'introduzione nel Decreto 231 dell'art. 24*bis* "*Delitti informatici e trattamento illecito di dati*".

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'Art. 24*bis* del D.Lgs. n. 231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi.

2.1 - Falsità in documenti informatici - art. 491*bis* c.p.

L'articolo 491*bis* c.p. (documenti informatici) sanziona tutte le ipotesi di **falso** previste dal Libro Secondo, Titolo VII, Capo III del codice penale.

Le indicate ipotesi delittuose, attraverso il richiamo operato dall'art. 491*bis* c.p., sono punibili nel caso in cui la condotta riguardi un **documento informatico pubblico avente efficacia probatoria** il quale, pertanto, è equiparato a tutti gli effetti ai documenti tradizionali.

Per documento informatico, secondo la definizione del Codice dell'amministrazione digitale (*ex* art. 1, lett. p del d.lgs. n.82/2005), deve intendersi *il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*

Il d.lgs. n. 7 del 15 gennaio 2016 ha, inoltre, aggiunto 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*".

Esempio pratico

Il dipendente autorizzato ad operare sugli archivi della società procede deliberatamente alla cancellazione o all'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente.

2.2 - Accesso abusivo ad un sistema informatico o telematico - art. 615*ter* c.p.

Il delitto in esame punisce la condotta di "***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 diritto ad escluderlo***".

Viene sanzionato "l'accesso virtuale" che, pertanto, non comporta condotte di aggressione fisica al sistema, cui si accede a distanza su reti informatiche.

È un reato che tutela l'inviolabilità del domicilio informatico. Si tende a configurarlo come reato a natura **plurioffensiva,** volto a garantire:

- la **protezione del domicilio informativo** quale estensione di quello materiale;
- il diritto alla **riservatezza**;
- i diritti di **carattere patrimoniale**, come il diritto all'uso del computer per fini economici e produttivi;
- il diritto all'integrità dei dati e dei programmi contenuti nel sistema informatico;

Il termine "*accesso abusivo*" si riferisce all'**introduzione indebita effettuata contro la volontà del titolare del sistema**, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema.

Risponde del delitto di accesso abusivo al sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, **vi si sia trattenuto contro la volontà del titolare** del sistema oppure il soggetto che abbia utilizzato il sistema per fini differenti da quelli per i quali era stato autorizzato.

Il delitto è punito con la **reclusione fino a tre anni** sebbene il codice penale preveda differenti ipotesi aggravate:

1. reclusione **da uno a cinque anni** nel caso in cui:
   a) 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;
   b) il colpevole per commettere il fatto usa **violenza sulle cose** o alle persone, ovvero se è palesemente armato;
   c) 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.
2. reclusione **da uno a cinque anni e da tre a otto anni**:
   a) qualora il delitto in oggetto riguardi 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.

Esempio pratico

Un dipendente accede abusivamente nei sistemi informatici dell'azienda, (ad esempio al fine di manipolare i dati relativi al bilancio falso, ovvero per attivare servizi non richiesti dalla clientela); oppure ai sistemi di terze parti, (c.d. *outsider hacking*), per prendere cognizione di dati riservati di un'impresa concorrente).

Il reato, infatti, si configura anche solo accedendo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

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

Il reato si realizza quando un soggetto, "***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 di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo***".

Il reato è punito con la **reclusione sino ad un anno** e con la **multa sino a euro 5.164,00.**

La pena è della reclusione **da uno a due anni** e della **multa da euro 5.164,00 a euro 10.329,00** se il danno è commesso:

a) 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;

b) 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;

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

La finalità di tutela è quella di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615*quater*, infatti, sono punite le **condotte preliminari** all'accesso abusivo, consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico, (*password*, o schede informatiche come *badge*, carte di credito, bancomat e *smart card).*

Il delitto si integra quando il soggetto, che legittimamente possiede uno dei dispositivi di cui sopra (operatore di sistema), li **comunica senza autorizzazione a terzi soggetti**, ovvero nel caso in cui tale soggetto si procura illecitamente uno di tali dispositivi.

L'art. 615*quater*, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Esempio pratico

Il dipendente dell'azienda autorizzato ad un certo livello di accesso al sistema informatico ottiene illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'azienda.

2.4 - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico - art. 615*quinqies* c.p.

Il reato si realizza qualora qualcuno, "***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***".

Tale reato è punito con la **reclusione fino a due anni** e con la **multa sino a euro 10.329,00**.

Questo delitto è integrato, ad esempio, nel caso in cui il soggetto si procuri un virus, idoneo a danneggiare un sistema informatico o qualora si producano o si utilizzino delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi elettronici.

Questi fatti sono punibili solo nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento.

Esempio pratico

Un dipendente della società inocula un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico di una società concorrente.

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

Il reato si integra qualora un soggetto "**fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni**", nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico.

Tale reato è punito con la **reclusione da un anno e sei mesi a cinque anni**.

Il trattamento sanzionatorio è aggravato con la reclusione **da tre a otto anni** nelle seguenti ipotesi:

a) 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;
b) 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;
c) da chi esercita anche abusivamente la professione di investigatore privato.

La fraudolenza consiste nella modalità occulta dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale, ossia diretta ad un numero di soggetti determinati o determinabili. Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Esempio pratico

Il dipendente della società si determina nel captare fraudolentemente delle comunicazioni di un'azienda rivale col proposito di effettuare una attività di sabotaggio industriale a vantaggio della società per cui lavora.

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

Questa fattispecie di reato si realizza quando qualcuno, "***fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi***".

Tale reato è punito con la **reclusione da uno a quattro anni**.

La condotta vietata dall'art. 617*quinquies* è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate.

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione.

Esempio pratico

Il dipendente, al fine di avvantaggiare la propria azienda, si introduce fraudolentemente presso la sede di una società concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

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

Tale fattispecie di reato si realizza quando un soggetto "***distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui***".

Tale reato è punito con la **reclusione da sei mesi a tre anni**.

Il d.lgs. n. 7 del 15 gennaio 2016 ha, da ultimo, aggiunto che "*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*".

Esempio pratico

Il reato si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove l'eliminazione o l'alterazione dei file o di un programma informatico siano poste per distruggere l'elenco clienti di una società concorrente.

2.8 - 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.

Tale reato si realizza quando un soggetto "***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***".

Tale reato è punito con la **reclusione da uno a quattro anni**.

La sanzione è da **tre a otto anni** se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

Il d.lgs. n. 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*".

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati, ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

2.9 - Danneggiamento di sistemi informatici o telematici - art. 635*quater* c.p.

Il reato si realizza quando un soggetto "***mediante le condotte di cui all'art. 635bis (danneggiamento di dati, informazioni e programmi informatici), 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***".

Tale reato è punito con la **reclusione da uno a cinque anni**.

Il d.lgs. n. 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*".

Qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile od ostacoli gravemente il funzionamento del sistema, si configura il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635*bis* c.p.

2.10 - Danneggiamento di sistemi informatici o telematici di pubblica utilità - art. 635*quinquies* c.p.

Il reato si configura quando "***il fatto di cui all'art. 635quater (Danneggiamento di sistemi informatici o telematici) 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***".

Tale reato è punito con la pena della **reclusione da uno a quattro anni**.

La sanzione è della **reclusione da tre a otto anni** se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile.

Il d.lgs. n. 7 del 15 gennaio 2016 ha aggiunto un'ipotesi aggravata: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*".

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi **di pubblica utilità**, (art. 635*ter* c.p.), quel che rileva è che il sistema informativo sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica del sistema stesso.

È bene ribadire, come già fatto in altre occasioni, che la punibilità della società è limitata alle condotte poste in essere nell'interesse o a vantaggio della stessa, secondo i criteri delineati dall'art. 5 d.lgs. n. 231/2001.

Il reato si può configurare nel caso in cui un dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

2.11 - Frode informatica - art. 640*ter* c.p.

Il delitto in esame si configura quando chiunque, "***alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno***".

La pena prevista è la **reclusione da sei mesi a tre anni** e la **multa da euro 51 a euro 1.032**.

Se, tuttavia, il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema, la pena è aumentata da **uno a cinque anni** e con la **multa da euro 309 a euro 1.549**.

Se, infine, il fatto è commesso con furto e indebito utilizzo in danno di qualcuno, la **reclusione va da due a sei anni** e la **multa da euro 600 a euro 3.000**.

Il delitto è punibile a querela della persona offesa, salvo che il fatto sia aggravato.

A differenza del reato di truffa di cui all'art. 640 c.p., nel reato in esame non si richiede la "induzione in errore" della vittima, in quanto l'attività fraudolenta investe il sistema informatico della stessa.

2.12 - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica - art. 640*quinquies* c.p.

Questo reato si configura quando "***il soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé 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***".

Tale reato è punito con la **reclusione fino a tre anni** e con la **multa da euro 51 a euro 1.032**.

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

2.13 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

L'articolo 1 del D.L. n. 105 del 21 settembre 2019, coordinato con legge di conversione n.133 del 18 novembre 2019, ha istituito in Italia il cd. ***perimetro di sicurezza nazionale cibernetica,*** finalizzato ad "*assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori, pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività' civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale".*

Al comma 11 dello stesso articolo 1, si dispone: "*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 attività 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 attività 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, è punito con la* ***reclusione da uno a tre anni***".

La normativa ha modificato l'articolo 24*bis*, comma 3, del d.lgs. n. 231/2001, che diventa "*In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all'ente la* ***sanzione pecuniaria sino a quattrocento quote***".

3.0 - Le attività sensibili relative ai reati informatici

L'analisi della struttura organizzativa aziendale di WEM-Waste Engineering Management s.r.l. ha consentito di individuare le seguenti **attività sensibili**, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24*bis* del d.lgs. n. 231/2001:

- **a.** gestione dei profili utente e del processo di autenticazione;
- **b.** gestione del sistema di firma digitale;
- **c.** gestione del processo di creazione, trattamento, archiviazione di documenti con valore probatorio;
- **d.** gestione e protezione della postazione di lavoro;
- **e.** gestione degli accessi da e verso l'esterno;
- **f.** gestione e protezione delle reti;
- **g.** gestione degli output di sistema e dei dispositivi di memorizzazione (es. usb, cd);
- **h.** sicurezza delle componenti informative fisiche (include sicurezza cablaggi, dispositivi di rete, etc.);
- **i.** gestione delle attività di manutenzione dei sistemi.

I delitti trovano come presupposto la sicurezza e l'utilizzo della **rete informatica** e precisamente:

- tutte le attività aziendali svolte dal personale tramite accesso alla rete aziendale, del servizio di posta elettronica e accesso ad internet;
- gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica;
- erogazione di servizi di installazione e servizi professionali di supporto al personale (assistenza, manutenzione, gestione della rete, manutenzione e security);
- la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati (sicurezza nazionale cibernetica). Allo stato il presupposto non è applicabile alla W.E.M.-Waste Engineering Management s.r.l.

4.0 - Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili - **tutte astrattamente ipotizzabili** - si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali:

- **Area amministrativa/ Uffici Segreteria Generale**
  - gestione account Posta Elettronica Certificata;
  - gestione account Società;
- **Responsabile Acquisti, Forniture e Contratti - Risorse Umane - Contabilità, Bilancio e Fisco - Sviluppo Commerciale - Direttore Tecnico**
  - gestione account Posta Elettronica / peo e pec;
  - gestione account Società;
  - potere di certificazione di firma digitale;
- **Amministratore Unico**
  - funzioni di controllo sulle Aree Sensibili;
- **Responsabile Formazione**
  - in merito alla formazione, informazione sull'utilizzo dei sistemi informatici;

5.0 - Principi e regole di comportamento

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del MOGC 231.

In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti, di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, l'Amministratore, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- **la normativa italiana applicabile alle attività svolte;**
- **il Codice Etico Aziendale;**
- **il presente Modello;**
- **gli standard generali di controllo;**
- **le procedure e le linee guida aziendali** nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della società.

Si individuano qui di seguito i principi che informano le specifiche procedure dell'azienda, relativi a qualsiasi operazione/attività che coinvolga l'ente nella famiglia dei delitti informatici e trattamento illecito di dati trattati nella presente Sezione, in aderenza alla previsione dettata dall'art. 24*bis* del d.lgs. n. 231/2001.

A tal fine, in via generale e astratta, è vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplato dal citato art. 24*bis*.

Princìpi

In generale, la prevenzione dei crimini informatici è svolta attraverso adeguate misure tecnologiche, organizzative e normative ed in particolare attraverso l'applicazione dei seguenti controlli di carattere generale:

- previsione nel **codice etico** di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno della società che tramite apparecchiature non soggette al controllo della stessa;
- previsione di un idoneo sistema di **sanzioni disciplinari** (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del modello) che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite;
- predisposizione di adeguati **strumenti tecnologici** atti a prevenire e/o impedire la realizzazione di reati informatici da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio;
- predisposizione di **programmi di formazione, informazione e sensibilizzazione** rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.

Conseguentemente, gli Organi Sociali, l'Amministratore, i dipendenti nonché gli stakeholder coinvolti nello svolgimento delle attività a rischio hanno l'espresso **obbligo** di perseguire i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

– **Segregazione dei ruoli e delle responsabilità**

Deve trovare attuazione il principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio; deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso.

– **Procedure**

Disposizioni aziendali e procedure idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività.

– **Poteri autorizzativi e di firma**

I poteri autorizzativi e di firma devono essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese e essere chiaramente definiti e conosciuti all'interno della società.

– **Tracciabilità**

Tracciabilità delle attività svolte nell'ambito dei processi esposti a rischio; ogni operazione relativa alle attività sensibili deve essere adeguatamente registrata per ciò che attiene agli accessi e alle attività svolte. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione distruzione delle registrazioni effettuate.

– **Gestione delle segnalazioni**

Raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati informatici rilevati da soggetti interni ed esterni alla società.

– **Riporto all'ODV**

È fatto obbligo di riferire all'ODV eventuali situazioni di irregolarità.

6.0 - Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel MOGC 231 e nei suoi protocolli, (sistema procuratorio, Codice Etico, in primo luogo), gli Organi Sociali, l'Amministratore, e tutti i Destinatari sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'Art. 24*bis* del d.lgs. n. 231/2001, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale attività a rischio.

Le seguenti regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici.

1. **Gestione degli accessi**:
   - attribuzione di **credenziali** di accesso e assegnazione dei **codici** identificativi personali;
   - disattivazione dei codici utente associati al personale che ha perso il diritto di accesso a tutti i sistemi informatici o che non accede più ai vari sistemi;
   - attività di controllo volta a verificare, prima della creazione di un'utenza, che la stessa non sia già stata precedentemente assegnata/disabilitata/rimossa e che uno stesso codice identificativo personale non venga assegnato, neppure in tempi diversi, a persone diverse;
2. **Modalità di utilizzo e di salvaguardia del PC:**
   - misure che l'utente deve adottare per garantire un'adeguata protezione delle apparecchiature incustodite;
3. **Installazione di software** sui sistemi operativi;
4. **Dismissione** dei supporti di memorizzazione su cui sono registrate informazioni aziendali.
5. Presenza di sistemi di protezione **antivirus** e **antispam;**
6. Esistenza di procedure, in materia di **"privacy"** e di **"security",** che disciplinano gli aspetti legati al corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
7. Attuazione del **progetto di formazione,** volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy;
8. Consegna a ciascun dipendente della società, contestualmente all'assegnazione del pc e/o dell'indirizzo di posta elettronica, di **norme per l'utilizzo dei Personal Computer aziendali** e sull'utilizzo della posta elettronico e, in generale, di documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico.
9. Denuncia tempestiva di eventuali **vulnerabilità dei sistemi;**
10. Attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni), attraverso **l'adozione di sistemi antincendio, antiallagamento, di condizionamento;**
11. Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici **(registrazione dei log on e log off);**
12. **Protezione del trasferimento dati** al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking attraverso, tra l'altro, una serie di provvedimenti volti a garantire che**:**

- l'informazione inserita ed elaborata dal sistema pubblico sia processata completamente ed in modo tempestivo;
- le informazioni sensibili siano protette durante i processi di raccolta e di conservazione;
- l'accesso al sistema pubblico non consenta ingressi fortuiti alle reti con cui è connesso.

Princìpi procedurali specifici

In particolare, si elencano qui di seguito le regole che sono adottate dalla società e rispettate dai dipendenti e dagli altri soggetti eventualmente autorizzati nell'ambito delle Attività Sensibili:

a) i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come **riservati**;

b) è **vietato introdurre in azienda computer, periferiche**, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato;

c) è vietato in qualunque modo modificare la **configurazione di postazioni** di lavoro fisse o mobili effettuata dal servizio infrastrutture;

d) è vietato acquisire, **possedere o utilizzare strumenti software e/o hardware** che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);

e) è vietato ottenere **credenziali di accesso a sistemi informatici** o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società;

f) è **vietato divulgare**, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

g) è vietato accedere ad un **sistema informatico altrui** (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;

h) è vietato **manomettere, sottrarre o distruggere** il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

i) è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;

j) è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;

k) è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

l) è vietato **comunicare a persone non autorizzate**, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

m) è proibito distorcere, oscurare o sostituire la propria **identità e inviare e-mail** riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati;

n) è vietato lo **spamming**;

o) è **obbligatorio segnalare all'Organismo di Vigilanza** qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

L'azienda, con il presente Modello, adotta e rispetta i seguenti adempimenti:

1. informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri **codici di accesso** (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi;

2. fare sottoscrivere ai dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali;

3. ai dipendenti e agli altri soggetti eventualmente autorizzati, viene comunicata la necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

4. i sistemi informatici sono impostati in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si **blocchino automaticamente**;

5. l'accesso da e verso l'esterno (connessione alla rete internet) è consentito esclusivamente ai sistemi informatici dei dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria;

6. gli accessi alla stanza server sono limitati unicamente al personale autorizzato;

7. per quanto possibile, ogni sistema informatico societario è protetto al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

8. ogni sistema informatico è fornito di adeguato software **firewall e antivirus**;

9. è vietata l'installazione e l'utilizzo di software non approvati dalla società e non correlati con l'attività espletata per la stessa;

10. è vietato l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file);

11. è vietata l'installazione e l'utilizzo, sui sistemi informatici della società, di software (c.d. **"p2p", di files sharing o di instant messaging**) mediante i quali è possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.);

12. per la connessione alla rete internet mediante collegamenti wireless, l'accesso è protetto impostando una chiave d'accesso;

13. è previsto un procedimento di autenticazione mediante **username e password al quale corrisponda un profilo** specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati;

14. si prevedono periodicamente, ove possibile, controlli sulle attività effettuate dal personale sulle reti.

7.0 - I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza può effettuare periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'art. 24*bis* del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 24*bis* del Decreto sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24*bis* del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio di delitti informatici, diretti a verificare la corretta

esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;

- proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti informatici di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale;
- monitorare il rispetto delle procedure e la documentazione interna per la prevenzione dei delitti informatici;
- consultarsi con il responsabile della Sicurezza Informatica e/o del Servizio Sistemi Informativi ed invitare periodicamente lo stesso a relazionare alle riunioni dell'ODV;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguite.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

FLUSSI INFORMATIVI VERSO ODV: nessun obbligo di flusso informativo (salvo verificazione di evento rilevante ai sensi del D.lgs. 231/2001).

VERIFICA DELL'ODV: non è prevista alcuna verifica, salvo i casi in cui venga comunicata l'insorgenza di un evento rilevante ex D.lgs. 231/2001 o altra rilevante/fondata comunicazione ovvero i casi di verifiche eccezionali dell'ODV.