

PARTE SPECIALE D

Delitti informatici, trattamento illecito di dati e delitti in violazione del diritto d'autore

Frode informatica ai danni dello Stato (art. 24 D. Lgs. 231/2001)
Reati informatici e trattamento illecito di dati (art. 24-bis D. Lgs. 231/2001)
Art. 171 bis legge 633/1941 (art. 25-novies D. Lgs. 231/2001)

1 ^a edizione:	Consiglio di Amministrazione del 27 marzo 2020
2 ^a edizione:	

Art. 24

Art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico.

1. In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 640, comma 2, n. 1, 640-bis e 640-ter se commesso in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.
2. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità; si applica la sanzione pecuniaria da duecento a seicento quote.
3. Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

Art. 24-bis.

Delitti informatici e trattamento illecito di dati

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
3. 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 (2).
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

(1) Articolo aggiunto dall'articolo 7 della legge 18 marzo 2008, n. 48.

(2) Comma modificato dall'articolo 1, comma 11-bis, del D.L. 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133.

Art. 25-novies.

Delitti in materia di violazione del diritto d'autore

1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174- quinquies della citata legge n. 633 del 1941.

(1) Articolo inserito dall'articolo 15, comma 7, lettera c), della legge 23 luglio 2009, n. 99

INDICE

- 1. Le fattispecie di criminalità informatica previste nel D.lgs 231/01**
- 2. Individuazione dei reati non rilevanti**
- 3. Destinatari e obiettivi della “Parte Speciale D”**
- 4. Processi sensibili**
- 5. Principi generali di comportamento**
- 6. Procedure specifiche**
- 7. Il sistema di controllo: compiti e poteri dell'OdV**

1. Le fattispecie di criminalità informatica previste nel D.lgs 231/2001

Il D.lgs. 231/01 prevede alcune fattispecie criminose che possono essere realizzate attraverso l'ausilio di sistemi informatici o telematici.

La Società ha ritenuto opportuno indicare le misure adottate al fine di scongiurare il verificarsi di comportamenti illeciti connessi alla disponibilità di mezzi informatici, in quanto la sicurezza dei sistemi informatici è ritenuta elemento essenziale del sistema di controllo aziendale.

Oltre al reato di frode informatica di cui all'art. 640 *ter* c.p., già considerato nella Parte Speciale A, il legislatore ha inserito successivamente ulteriori ipotesi delittuose che rilevano ai fini della presente Parte Speciale nei limiti in cui siano commesse nell'interesse o a vantaggio della Società.

L'ipotesi che la commissione di talune fattispecie integri il suddetto requisito è un rischio alquanto marginale, ma si è ritenuto opportuno inserire una Parte Speciale specifica in ragione del fatto che il sistema informatico implica la gestione di tutti i dati aziendali ed occorre pertanto un corretto utilizzo dello stesso.

L'art. 24-*bis* che prevede i "Delitti informatici e trattamento illecito di dati" è stato introdotto dalla Legge n. 48/08, legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, convenzione redatta a Budapest il 23 novembre 2001.

Fondamentale per il corretto inquadramento delle fattispecie di reato contemplate dall'art. 24-*bis* è la definizione di sistema informatico, ovvero ogni sistema di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione di dati su supporti adeguati, per mezzo di impulsi elettronici.

Nella presente Parte Speciale si richiama inoltre il reato di cui all'art. 171 bis della legge 22 aprile 1941 n. 633 che, unitamente ad altre fattispecie criminose, è stato inserito nel D. Lgs. 231/01 all'art. 25 *nonies* che prevede i "Delitti in materia di violazione del diritto d'autore".

Infatti, nonostante le fattispecie richiamate dagli artt. 24-*bis* e 25 *nonies* D. Lgs. 231/2001 tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Parte Speciale in quanto:

- tali fattispecie presuppongono comunque un corretto utilizzo delle risorse informatiche;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali adottati dalla Società sono plurivalenti e mirano a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

Si riporta per maggiore chiarezza una breve descrizione delle fattispecie delittuose interessate:

A. Delitti informatici e trattamento illecito di dati

❑ *Frode informatica (art. 640-ter c.p.)*

Tale ipotesi di reato, come già specificato nella Parte Speciale A, si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico.

Il reato è configurabile ad esempio, quando, un soggetto operante nell'ambito della realtà aziendale, violando il sistema informatico di un ente pubblico, riduca il debito fiscale o contributivo della Società nei confronti di enti pubblici.

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

Questo reato si configura quando un 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, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato cd. proprio in quanto può essere commesso solo da parte dei certificatori qualificati, o meglio, da parte dei soggetti che prestano servizi di certificazione di firma elettronica qualificata.

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

Il reato consiste nell'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza ovvero nella permanenza contro la volontà espressa o tacita di chi ha il diritto di escludere i terzi.

Pare opportuno evidenziare che il delitto è procedibile d'ufficio solo qualora esso sia stato commesso nella sua forma aggravata, ovvero quando 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 ancora da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; così come se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; ovvero 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.

I fatti sono procedibili d'ufficio anche qualora 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.

Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto operante in CRM Microport, nell'interesse o a vantaggio della Società, acceda abusivamente a sistemi informatici di proprietà di terzi, protetti da misure di sicurezza, per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale.

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

Tale fattispecie di reato si perfeziona qualora 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 ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

L'art. 615-quater cod. pen. pertanto, punisce condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (quali badge o smart card). Tale fattispecie si configura sia nel caso in cui il soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), li comunichi

senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

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

Tali condotte, in ogni caso, assumono rilevanza penale a norma dell'articolo in esame solo nel caso in cui risultino finalizzate a procurare a sé o ad altri un profitto ovvero ad arrecare ad altri un danno.

- ❑ *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen.)*

Tale reato si realizza qualora un soggetto, 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 procuri, produca, riproduca, importi, diffonda, comunichi, consegna o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Tale delitto potrebbe, ad esempio, configurarsi qualora un soggetto operante nell'ambito della Società si procuri un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale, per distruggere, in ipotesi, documenti "sensibili" in relazione ad un procedimento penale a carico della Società.

- ❑ *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater cod. pen.)*

Tale ipotesi di reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, mediante qualsiasi mezzo di informazione al pubblico, il contenuto di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato potrebbe configurarsi, ad esempio, con il vantaggio concreto della Società, nel caso in cui un soggetto operante nell'ambito della Società, impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati o l'offerta per la partecipazione ad una gara.

- ❑ *Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies cod. pen.)*

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

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

La condotta criminosa si realizza attraverso la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o software altrui.

Si precisa che il reato è procedibile a querela della persona offesa, mentre è procedibile d'ufficio se il fatto viene commesso con violenza alla persona o con minaccia, ovvero con abuso della qualità di operatore del sistema.

- ❑ *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.)*

La norma anticipa la tutela per i soggetti pubblici considerando integrato il reato da fatti diretti 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, anche qualora dalla condotta posta in essere non derivino effettivamente la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici; peraltro, qualora si verifichino tali eventi, si inasprisce la pena applicabile.

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

Tale ipotesi di reato si configura attraverso la distruzione, il danneggiamento, il fatto di rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o di ostacolarne gravemente il funzionamento attraverso la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi informatici altrui, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi.

- ❑ *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen.)*

Questo reato si configura quando la condotta di cui al precedente art. 635-quater cod. pen. è diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Analogamente a quanto osservato per il reato di cui all'art. 635 *ter* c.p., la condotta assume rilevanza penale anche se non ne derivino concretamente la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità o non ne sia ostacolato gravemente il funzionamento; peraltro, qualora si verifichino la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero questo sia reso, in tutto o in parte, inservibile, si inasprisce la pena applicabile.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità la condotta deve avere ad oggetto un intero sistema – e non solo informazioni, dati o programmi informatici, come nel delitto di cui all'art. 635 *ter* c.p.; inoltre, deve riguardare un sistema utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

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

La norma, richiamata dall'art. 24-*bis* del D. Lgs. 231/01, sostituita dall'art. 2 del D. Lgs. 15 gennaio 2016, n. 7, precisa che se alcuna delle falsità previste dal capo terzo, del titolo settimo, del libro secondo del Codice Penale relativo alla falsità in atti, riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici. In particolare, si precisa che si ha "falsità materiale" quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente o sottoscrittore, con divergenza tra autore apparente e autore reale del documento (contraffazione) ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione. Si ha, invece, "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere.

Nel falso ideologico, dunque, è lo stesso autore del documento che attesta fatti non rispondenti al vero.

A titolo esemplificativo, integra il delitto di falsità in Documenti Informatici la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati “sensibili” in vista di una possibile attività ispettiva.

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- *Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.):*

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni”;

- *Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.):*

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni”;

- *Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.):*

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni”;

- *Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.):*

“Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476”;

- *Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.):*

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni”;

- *Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.):*

“Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro”;

- *Falsità materiale commessa da privato (art. 482 c.p.):*

“Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo”;

- *Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.):*

“Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi”;

- *Falsità in registri e notificazioni (art. 484 c.p.):*

“Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00”;

- *Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.):*

“Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480”;

- *Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.):*

“Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dall'art. 487, si applicano le disposizioni sulle falsità materiali in atti pubblici”;

- *Uso di atto falso (art. 489 c.p.):*

“Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.”

- *Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.):*

“Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute.”

- *Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.):*

“Agli effetti delle disposizioni precedenti, nella denominazione di “atti pubblici” e di “scritture private” sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti”;

- *Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.):*

“Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni”.

- ❑ *Decreto-Legge 21 settembre 2019 n.105 convertito con modificazioni, dalla Legge 18 novembre 2019, n. 133. - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica (SICUREZZA CIBERNETICA)*

Art. 1 - Perimetro di sicurezza nazionale cibernetica

In sintesi il Decreto istituisce il c.d. **perimetro di sicurezza nazionale cibernetica**, “al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, 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” (**art. 1 D.L. 105/2019**).

La norma sanziona la condotta di chi, allo scopo di ostacolare o condizionare l'espletamento degli obblighi informativi degli enti individuati dal decreto o delle attività ispettive e di vigilanza previste, 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) dello stesso articolo di legge, o ai fini delle comunicazioni, o per lo svolgimento delle attività ispettive e di vigilanza od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

Si tratta, all’atto pratico, della violazione dolosa degli obblighi di cui sono destinatari i soggetti pubblici o privati che, in ragione del loro ruolo strategico e del loro ricorso a beni, strumenti o servizi ICT (**Information and Communication Technology**), rientrano nel perimetro di sicurezza nazionale: obblighi (perlopiù, ma non solo) di informazione nei confronti di autorità preposte, che se ottemperati permettono allo Stato di esplicare efficacemente i propri poteri di controllo e intervento laddove sopraggiungano ragioni di sicurezza nazionale.

B. Delitti in materia di violazione del diritto d'autore

Tra i reati richiamati dall’articolo 25 *novies* D. Lgs. 231/01 si riportano le seguenti fattispecie, in quanto come si vedrà nel paragrafo successivo sono le uniche rilevanti per la Società.

- ❑ *Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis l.633/1941 comma 1);*

La norma sanziona la condotta di chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE). La norma sanziona altresì l’ipotesi in cui il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l’elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Tale reato potrebbe ad esempio essere commesso nell'interesse della Società qualora venissero utilizzati, per scopi lavorativi, programmi contenuti in supporti non contrassegnati dalla SIAE al fine di risparmiare il costo della licenza per l'utilizzo di un software originale.

- ❑ *Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171 bis l. 633/1941 comma 2).*

È punito chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-*quinqüies* e 64-*sexies*, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter*, ovvero distribuisce, vende o concede in locazione una banca di dati.

2. Individuazione dei Reati non rilevanti per la Società

In relazione a talune delle fattispecie illustrate nel paragrafo precedente non è neppure ravvisabile un rischio residuale di commissione per la difficoltà di ipotizzare un interesse aziendale esclusivo o concorrente correlato con quello del soggetto agente.

Si tratta dei seguenti delitti di sabotaggio informatico:

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

È inoltre da escludere la fattispecie di “Frode informatica del soggetto che presta servizi di certificazione di firma elettronica” (art. 640-quinquies c.p.) in quanto reato che può essere commesso solamente da soggetto qualificato.

Al momento dell'adozione della presente parte speciale, ed in attesa dei Decreti attuativi che verranno adottati per l'esatta individuazione dei soggetti destinatari, del contenuto degli obblighi e delle precise modalità procedurali da adottare, rimane in sospeso la valutazione della rilevanza dei reati previsti dall'art. 1 comma 11 del Decreto-Legge n.105/2019 (convertito con modificazioni, dalla Legge n. 133/ 2019).

Allo stato non pare, in ogni caso, che la normativa sia alla stessa applicabile. Non è infatti astrattamente ipotizzabile che dal malfunzionamento, interruzione - anche parziali - ovvero utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici di cui CRM Microport si serve, possa derivare un pregiudizio per la sicurezza nazionale.

La Società non ha infine valutato i seguenti reati in materia di violazione del diritto d'autore, richiamati dall'art. 25-novies D. Lgs. 231/2001, in quanto non rilevanti rispetto all'attività ed alla realtà aziendale di CRM Microport:

- art. 171, primo comma, lettera a bis) legge n. 633/1941 (*Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa*);
- art. 171, terzo comma legge n. 633/1941 (*Reato di cui al primo comma commesso su opere altrui non destinate alla pubblicazione ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offeso l'onore o la reputazione*);
- art. 171-ter legge n. 633/1941 (*Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; abusiva riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa*);
- art. 171-septies legge n.633/1941 (*Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione*);
- art. 171-octies legge n.633/1941 (*Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale*).

3. Destinatari e obiettivi della “Parte Speciale D”

La Parte Speciale D disciplina i comportamenti posti in essere dalle funzioni di CRM Microport nell'utilizzo dei sistemi informatici o telematici dell'Azienda.

Finalità della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei Reati oggetto della presente Parte Speciale.

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

- a) fornire le «regole di comportamento» e le procedure che tutte le funzioni della Società sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- b) fornire all'Organismo di Vigilanza, e ai responsabili delle altre funzioni aziendali che cooperano con il medesimo, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

4. Processi sensibili

Le attività nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione (a titolo esemplificativo si considerino l'area amministrativa, l'area commerciale, l'area personale, ecc.).

I reati sopra considerati hanno come presupposto la disponibilità di un terminale e la concreta disponibilità di accesso alle postazioni di lavoro; per tale ragione le aree di attività ritenute più specificamente a rischio ("Aree di Attività a Rischio") sono quelle che comportano l'utilizzo di un personal computer, l'accesso alla posta elettronica, l'utilizzo di programmi informatici e l'accesso a internet.

Le attività sensibili individuate, in riferimento ai reati informatici richiamati nella presente Parte Speciale, sono le seguenti:

A) Gestione e utilizzo dei sistemi informatici e delle informazioni aziendali (c.d. "patrimonio informativo"), nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi verso l'esterno (in particolare gli adempimenti telematici tributari, previdenziali, le comunicazioni obbligatorie ad enti pubblici quali INAIL, INPS, ecc) ;
- gestione e protezione delle reti;
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.) dei sistemi informatici;

B) Gestione delle autorizzazioni e delle licenze di programmi software e banche dati, monitoraggio e controllo dei software installati.

C) Operatività amministratori di sistema

D) Utilizzo della posta elettronica e delle reti telematiche/Internet;

E) Gestione degli accessi ad opera di terzi.

5. Principi generali di comportamento

Ai fini della prevenzione dei reati sopra indicati, il Modello prevede l'espresso divieto a carico dei destinatari di porre in essere, o concorrere in qualsiasi forma nella realizzazione di comportamenti tali da integrare le fattispecie considerate nella presente Parte Speciale;

A tal fine, più specificamente, la Società pone, a carico del destinatari, l'espresso divieto di:

- a) alterare documenti informatici 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 o cancellare dati o informazioni;
- d) accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;

- e) 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, al fine di acquisire informazioni riservate;
- f) 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;
- g) svolgere attività di approvvigionamento o produzione o diffusione di apparecchiature o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti pubblici o privati, danneggiare le informazioni, i dati o i programmi in esso contenuti, ovvero favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- h) 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;
- i) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- l) utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio *virus*, *worm*, *troian*, *spyware*, *dialer*, *keylogger*, *rootkit*) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- m) svolgere attività di modifica o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- n) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- o) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.
- p) produrre e trasmettere documenti in formato elettronico con dati falsi o alterati;

Nell'ambito delle suddette regole, è previsto, in particolare, l'obbligo di:

- a) comportarsi in conformità alle norme di legge, di regolamento, alle procedure aziendali esistenti in ogni attività che comportino l'utilizzo di un terminale e l'accesso a sistemi informatici. Ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (ad esempio *personal computer* fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività e non possono essere cedute a terzi. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- b) ogni dipendente/amministratore del sistema è tenuto alla segnalazione alla Direzione aziendale di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di *hacker* esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente;
- c) osservare altresì rigorosamente tutte le norme poste dalla legge a tutela della Privacy e di agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano;
- d) garantire ed agevolare ogni forma di controllo, svolta nel rispetto dell'art. 4 dello Statuto dei Lavoratori, diretta a impedire la commissione di fattispecie delittuose;
- e) evitare di introdurre o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente autorizzate;

- f) evitare di trasferire all'esterno dell'Azienda o trasmettere *files*, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- g) evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Direttore di riferimento;
- h) evitare l'utilizzo di strumenti *software* o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni o documenti informatici;
- i) utilizzare la connessione a internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento. Non è consentito accedere da terminali in qualsiasi modo legati all'attività lavorativa svolta per la Società a siti e pagine web contenenti materiale vietato dalla legge (ad es. di carattere pedopornografico) o che possano costituire pericolo per la sicurezza della rete informatica. A tal fine l'Azienda provvede a monte a rendere operativo un blocco totale verso i siti internet di cui sopra, blocco che non dovrà in alcun modo subire tentativi di aggiramento da parte di soggetti facenti parte della realtà aziendale;
- j) rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi o funzionamenti anomali delle risorse informatiche;
- k) impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
- l) astenersi dall'effettuare copie non specificamente autorizzate di dati e di *software*;
- m) astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- n) osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
- o) osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

I responsabili delle funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nella presente Parte Speciale.

6. Procedure specifiche

La Società ha predisposto appositi presidi organizzativi di controllo e si è dotata di adeguate soluzioni di sicurezza, nel rispetto della normativa sulla privacy, per prevenire e controllare i rischi in tema di tecnologia dell'informazione, a tutela del proprio patrimonio informativo e dei dati personali dei soggetti interessati.

Le misure di sicurezza adottate ricomprendono, in particolare, la previsione di *password*, ovvero codici di accesso nominativi o numerici, la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico.

È altresì regolamentata la rigorosa custodia delle credenziali di accesso alle postazioni di lavoro, un sistema di controllo degli accessi alle banche dati, l'individuazione di un responsabile per settore, la sensibilizzazione del personale e una protezione *antivirus*.

Ulteriori misure adottate per ridurre le minacce all'integrità e alla riservatezza dei sistemi informatici sono:

- limitazioni dell'accesso al computer o ai dati che vengono comunicati, elaborati o stampati;
- misure per valutare l'affidabilità delle persone impiegate nello sviluppo e nella gestione dei sistemi computerizzati;
- controlli che mirano a segnalare tentativi di uso non autorizzato del sistema;
- interventi finalizzati ad assicurare la ripartizione delle responsabilità in maniera da ridurre al massimo le minacce derivanti da un esercizio dei poteri non autorizzato.

A) Gestione e utilizzo dei sistemi informatici e delle informazioni aziendali (c.d. "patrimonio informativo")

Le misure di sicurezza adottate ricomprendono, anche con particolare attenzione all'accesso a programmi riservati:

- la previsione di *firewall* e di *password*, ovvero codici di accesso riservati nominativi o numerici, la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico;
- la rigorosa custodia delle credenziali di accesso alle postazioni di lavoro;
- la previsione di screensaver che consentano il blocco automatico delle postazioni qualora non vengano utilizzate per un determinato periodo;
- un sistema di controllo degli accessi alle banche dati;
- la sensibilizzazione delle funzioni coinvolte segnalando la necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- la previsione di un'attività di formazione e addestramento volta a diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
- una protezione antivirus

B) Gestione delle autorizzazioni e delle licenze di programmi software e banche dati, monitoraggio e controllo dei software installati

La Società si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, l'Azienda si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che hanno causato danno all'Azienda, che ledono diritti di terzi o che, comunque, sono illecite.

Inoltre, si rammenta che, in osservanza della vigente normativa, i dati relativi all'utilizzo della posta elettronica e di internet sono conservati per periodi di tempo strettamente limitati.

I software utilizzati devono avere regolare licenza. È consentito l'uso di applicativi specifici sviluppati da personale CRM, l'uso di software freeware o di versioni Demo nel rispetto dei termini imposti dal produttore.

La documentazione e i codici di attivazione relativi alle licenze sono conservati:

☐ Dal servizio ICT per quel che riguarda software di uso comune (Office, Adobe Writer...) e per quel che riguarda contratti di utilizzo. Le licenze Windows sono conservate a bordo macchina.

☐ A cura dell'ente interessato per le licenze specifiche riguardanti macchinari (produzione, ricerca...)

La distribuzione o rivendita a terzi di copie di Software acquistati e della licenza d'uso associata a ciascuna copia del Software deve essere concessa solo a fronte di specifica autorizzazione da parte del venditore/sviluppatore.

C) Operatività amministratori di sistema

L'abilitazione per la connessione ad Internet e il servizio di posta elettronica vengono gestiti dall'Amministratore di Sistema o da altra figura tecnicamente competente a cui sono assegnate la responsabilità del corretto funzionamento degli strumenti elettronici, del monitoraggio costante dei livelli dei sistemi al fine di garantire la massima efficienza, della storicizzazione dei processi, della realizzazione e conservazione delle copie di backup, nonché di assicurare l'assistenza tecnica e formativa degli utenti.

D) Utilizzo della posta elettronica e delle reti telematiche

La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa.

Si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati dalla Società per le comunicazioni personali.

Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.

Nel caso in cui il dipendente non presti più la sua attività lavorativa presso la Società, la casella di posta elettronica sarà prontamente disattivata.

Qualora si verificano anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'amministratore di sistema.

La rete internet può e deve essere utilizzata dal dipendente a supporto all'attività lavorativa.

Al fine di ridurre il rischio di un utilizzo improprio di internet, quale ad esempio il caricamento o lo scaricamento di documenti non attinenti con l'attività lavorativa, la visione di siti internet non pertinenti con l'attività svolta, il collegamento a reti o forum comunque estranei alle mansioni del dipendente, e allo stesso tempo al fine di evitare per quanto possibile controlli che potrebbero comportare il trattamento di dati personali, anche non pertinenti, sensibili e giudiziari, sono di seguito evidenziati i principi che devono essere rispettati e le misure che la Società si riserva di adottare:

- rispetto della normativa vigente in materia di protezione di diritti di proprietà intellettuale nell'acquisizione, riproduzione, condivisione di immagini, di musica, filmati, software;
- utilizzo di sistemi e filtri che possono prevenire determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti o il download di file o software aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui è concesso l'accesso e categorie di siti cui non è concesso l'accesso ("black lists"), in quanto non correlati con la prestazione lavorativa;
- conservazione dei log di connessione dei dipendenti per finalità di accertamento e repressione dei reati nel rispetto di quanto previsto dalla normativa vigente.

Si invita comunque il dipendente a utilizzare internet nel rispetto delle leggi vigenti e prestando particolare cautela al fine di non importare virus, spam o altri programmi informatici dannosi.

E) Gestione degli accessi ad opera di terzi

In relazione alle eventuali attività di manutenzione da remoto ai PC delle segreterie connessi ad internet, il personale tecnico autorizzato dalla Società potrà utilizzare specifici software.

Tali programmi verranno utilizzati per assistere l'utente durante la normale attività informatica ovvero di svolgere manutenzione su applicazioni e su hardware. L'attività di assistenza e manutenzione avverrà previa autorizzazione telefonica da parte dell'utente interessato. La configurazione del software da utilizzare per gli interventi da remoto, prevedranno un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al PC.

7. Il sistema di controllo: compiti e poteri dell'OdV

Il sistema di controllo predisposto dalla Società prevede la supervisione ad opera dell'Organismo di Vigilanza, soggetto istituzionalmente preposto alla verifica dell'idoneità ed efficacia del Modello.

L'OdV, pertanto, effettua periodicamente specifici controlli sulle attività connesse ai "processi sensibili" al fine di verificare il rispetto dei Principi Generali di comportamento e delle procedure e delle istruzioni operative come sopra indicate

È stata all'uopo redatta specifica procedura che regola i flussi informativi nei confronti dell'OdV, al fine di fornire allo stesso le informazioni necessarie per l'espletamento dell'attività di verifica e controllo (Procedura "Flussi informativi nei confronti dell'OdV").

In ogni caso all'OdV vengono garantiti autonomi poteri di iniziativa e controllo e potrà avere accesso in qualunque momento a tutta la documentazione aziendale ritenuta rilevante.

Nell'ambito dei propri poteri potrà indire, a sua discrezione, riunioni specifiche con i soggetti deputati alla gestione dei "processi sensibili" e potrà attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello.

L'inosservanza dei principi e delle procedure previste nella presente Parte Speciale è passibile di sanzione disciplinare secondo quanto indicato nella parte generale alla sezione "Sistema disciplinare".