TORINO NUOVA ECONOMIA S.p.A.

Via Livorno n. 60

10144 Torino

MODELLO DI ORGANIZZAZIONE E GESTIONE EX ART. 6 D. LGS. 231/01

PARTE SPECIALE

SEZIONE IV

REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI; REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE DI CUI AGLI ARTT. 24 BIS E 25 NOVIES DEL D.LGS. 231/2001

Revisione 2 - 2016_Approvata dal Consiglio di Amministrazione nella seduta del 2 maggio 2016

INDICE

1. Premessa

La presente Parte Speciale del Modello è finalizzata a prevenire la commissione dei reati previsti dagli articoli 24 *bis* e 25 *novies* del D.Lgs. n. 231/01, che possono essere commessi nell'ambito della gestione dei sistemi informatici.

A seguito dei risultati delle periodiche attività di monitoraggio effettuate dagli organi competenti e dall'OdV si potrà procedere, qualora si rendesse necessario, all'implementazione della presente Sezione della Parte Speciale.

2. Funzione della Sezione IV della Parte Speciale

L'obiettivo della presente Parte Speciale è di far sì che tutti i destinatari del Modello, nell'ambito delle attività e/o dei processi sensibili come meglio successivamente individuati, adottino regole di condotta conformi ai principi contenuti, in primo luogo, nel Codice Etico, nel Modello (sia nella Parte Generale che nella presente Sezione della Parte Speciale), al fine di prevenire la commissione dei reati considerati rilevanti ai sensi degli articoli 24 *bis* e 25 *novies* del Decreto.

In particolare, la presente Parte Speciale ha lo scopo di:

1. indicare le regole di comportamento e le procedure che tutti i destinatari del Modello (amministratori, dirigenti, dipendenti, organi sociali, consulenti e collaboratori esterni) sono tenuti ad osservare al fine di una corretta ed efficace applicazione del Modello stesso;

2. fornire all'OdV ed ai responsabili delle altre funzioni aziendali che con lo stesso collaborano, gli strumenti effettivi per lo svolgimento delle attività di vigilanza, controllo e monitoraggio sull'applicazione del Modello.

3. Le ipotesi di reato rilevanti

3.1 Reati ex art. 24 *bis* D.Lgs. 231/2001.

L'art. 24 *bis* del Decreto, rubricato "Delitti informatici e trattamento illecito di

dati", così dispone:

"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, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
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).

Vengono di seguito riportati gli articoli del Codice penale richiamati dall'art. 24 *bis* del Decreto.

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

" *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla

funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Il reato si configura nel caso in cui un soggetto si introduca abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza, o vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Tale condotta assume rilievo penale sia se l'intrusione viene effettuata nel sistema informatico o telematico della Società (es. maggiorazione del costo dei servizi erogati, fatturazione servizi non richiesti) sia nel sistema di un Ente esterno, pubblico o privato, al fine di procurare un interesse o vantaggio alla Società (es. accesso abusivo nel sistema informatico di un concorrente al fine di conoscere l'offerta economica presentata per la partecipazione alla gara di appalto).

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

"*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.*

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

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

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

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

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

Il reato sussiste sia qualora un soggetto fraudolentemente intercetti o impedisca o interrompa comunicazioni relative ad un sistema informatico o telematico intercorrenti tra più sistemi e sia qualora riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

Il reato in esame, procedibile a querela della persona offesa, diviene perseguibile d'ufficio qualora venga commesso:

1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico da impresa esercente servizi pubblici o di pubblica necessità;
2. da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero

con abuso della qualità di operatore del sistema;
3. da chi esercita anche abusivamente la professione di investigatore privato.

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

"*Chiunque, 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, è punito con la reclusione da uno a quattro anni.*
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617quater".

Integra la fattispecie in esame l'installazione, fuori dai casi consentiti dalla legge, di 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.)

"*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
*Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni" (*articolo modificato dalla Legge 15 gennaio 2016 n. 7).

Il reato si configura quando un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635*ter* c.p.)

"*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

*Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata" (*articolo modificato dalla Legge 15 gennaio 2016 n. 7).

L'articolo in esame punisce chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Danneggiamento di sistemi informatici e telematici (art. 635 *quater* c.p.)

"*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.*

*Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata" (*articolo modificato dalla Legge 15 gennaio 2016 n. 7).

Il reato si configura quando un soggetto attraverso le condotte di cui all'art. 635*bis* o 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, salvo che non possa essere configurato un differente reato.

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

"*Se il fatto di cui all'articolo 635quater 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, la pena è della reclusione da uno a quattro anni.*
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata" (articolo modificato dalla Legge 15 gennaio 2016 n. 7).

Il reato si configura qualora il fatto previsto dall'art. 635*quater* sia diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

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

"*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri*

un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.
La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater".

Viene commesso il reato in esame quando un soggetto 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, al fine di procurare a sé o ad altri un profitto, o di 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* c.p.)

"*Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329*".

Il reato punisce chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici 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 allo scopo di favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento del suddetto sistema.

Falsità in un Documenti informatici pubblici o aventi efficacia probatoria (art. 491*bis* c.p.).

"*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici*" *(*articolo modificato dalla Legge 15 gennaio 2016 n. 7).

L'articolo in esame sanziona il comportamento di chi pone in essere condotte riconducibili ai reati di cui al Capo III, Titolo VII, Libro II del Codice Penale (*Della falsità in atti*), aventi ad oggetto *un documento informatico pubblico avente efficacia probatoria.*
In particolare i reati di falso richiamati sono i seguenti:

- *Falsità materiale commessa dal pubblico ufficiale in atti pubblici* (art. 476 c.p.);
- *Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative* (art. 477 c.p.);
- *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.);
- *Falsità ideologica commessa dal pubblico ufficiale in atti pubblici* (art. 479 c.p.);
- *Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative* (art. 480 c.p.);
- *Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità* (art. 481 c.p.);
- *Falsità materiale commessa da privato* (art. 482 c.p.);

- *Falsità ideologica commessa dal privato in atto pubblico* (art. 483 c.p.);
- *Falsità in registri e notificazioni* (art. 484 c.p.);
- *Falsità in foglio firmato in bianco. Atto pubblico* (art. 487 c.p.);
- *Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali* (art. 488 c.p.);
- *Uso di atto falso* (art. 489 c.p.) *(*articolo modificato dalla Legge 15 gennaio 2016 n. 7);
- *Soppressione, distruzione e occultamento di atti veri* (art. 490 c.p.) *(*articolo modificato dalla Legge 15 gennaio 2016 n. 7);
- *Copie autentiche che tengono luogo degli originali mancanti* (art. 492 c.p.);
- *Falsità commesse da pubblici impiegati incaricati di un pubblico servizio* (art.493 c.p.).

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

"*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a 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, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro*".

Il reato si configura nel caso n cui il soggetto che presta servizi di certificazione di firma elettronica violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

3.2 Reati ex art. 25 *novies* d.lgs. 231/2001.

L'art. 25 *novies* del d.lgs. 231/2001, rubricato "Delitti in materia di violazione del diritto d'autore", così dispone:
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.
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.

Delle numerose norme contenute nell'art 171, il Decreto Legislativo 231/01 inserisce come reati-presupposto solo la lettera a *bis*) del primo comma e il terzo comma.
La lett. a *bis*) del primo comma, introdotta dalla legge n. 7 del 2005, punisce la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell' ingegno protetta o di parte di essa.
Il Legislatore intende, dunque, tutelare l'interesse patrimoniale dell'autore dell'opera, che vedrebbe lesi i suoi diritti in caso di libera circolazione del proprio lavoro in rete.

Il terzo comma punisce, invece, le condotte sopra illustrate nel caso in cui si riferiscano ad un'opera altrui non destinata alla pubblicazione ovvero con usurpazione della paternità dell'opera ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.
Quest'ultima fattispecie, pertanto, è rivolta in particolare alla tutela dell'onore e della reputazione dell'autore dell'opera.

Venendo invece all'art. 171*bis,* occorre rilevare come la funzione di tale norma sia volta a fornire un'adeguata tutela penale del *software*.
Il primo comma dell'art. 171 *bis* punisce la condotta di abusiva duplicazione di *software* che avvenga al fine di trarne profitto; in particolare, viene sanzionato

chiunque 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.
Si precisa che il termine “profitto” invece può implicare sia il lucro e, quindi, l’accrescimento effettivo della sfera patrimoniale, sia il mancato depauperamento del patrimonio e, pertanto, il risparmio dei costi.
La stessa pena si applica, inoltre, se 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
Infine, il secondo comma dell’art. 171 *bis* mira a tutelare le banche dati, punendo le condotte di riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca dati, ovvero ancora l'estrazione o il reimpiego abusivi della banca di dati, la distribuzione, vendita o concessione in locazione una banca di dati.
Ai sensi dell’art. 2 della Legge sul diritto d’autore si intendono per banche dati: *“le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo” .*

Infine, l’art. 171 *ter* sanziona analoghe condotte aventi ad oggetto altre opere dell’ingegno quali le opere cinematografiche, televisive, discografiche in violazione del diritto d’autore, mentre l’art. 171 *octies* sanziona chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato 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.

4. Aree aziendali di TNE potenzialmente esposte al rischio di commissione dei reati di cui agli artt. 24*bis* e 25 *novies* del Decreto

All'esito del processo di individuazione e analisi delle aree a rischio (*as is analysis*) vengono indicate di seguito le attività ed i processi aziendali di T.N.E. che sono considerati maggiormente esposti al rischio di commissione degli illeciti sopra indicati:

1) Accesso a sistemi informatici interni ed esterni da parte dei destinatari della presente sezione della Parte Speciale del Modello;

2) Utilizzo delle *password* e/o di ogni altro codice identificativo che consenta l'accesso ad un sistema telematico o informatico;

3) Utilizzo della Posta elettronica;

4) Accesso, utilizzo e salvataggio di informazioni aziendali rilevanti;

5) Acquisto e conservazione di programmi informatici e/o di qualsiasi altro bene, materiale ed immateriale, nel pieno rispetto della disciplina posta a tutela del diritto d'autore;

6) Accesso a sistemi informatici e banche dati di proprietà di soggetti terzi, con particolare riferimento alle banche degli Enti Pubblici.

Si deve ritenere, altresì, attività sensibile la predisposizione del Documento Programmatico sulla Sicurezza previsto dal D.Lgs 196/03.

Con riferimento alle operazioni sensibili sopra individuate, si indicano di seguito, le funzioni/figure aziendali di T.N.E. potenzialmente connesse con lo svolgimento delle attività considerate a rischio di commissione dei reati di cui agli artt. 24 *bis* e 25 *novies* del Decreto:

- Presidente Consiglio di Amministrazione;
- Amministratore Delegato;
- Consiglio di Amministrazione;
- Collegio Sindacale;

- Ufficio Tecnico;
- Soggetti terzi incaricati dalla società per il compimento di specifiche attività nell'interesse della medesima;
- Consulenti esterni;
- Soggetti che, in base alla disciplina contenuta nel Titolo IV del D.Lgs. n. 81/08 e/o in virtù della specifica disciplina degli appalti pubblici, hanno specifici poteri decisionali e/o di controllo nei cantieri.

5. Principi generali di Comportamento

La gestione di tutte le attività a rischio di commissione dei Reati di cui agli articoli 24 *bis* e 25 *novies* del Decreto, nonché di tutti i processi strumentali alle attività a rischio, avviene in conformità ai principi di comportamento previsti nel Codice Etico, nella Parte Generale del Modello e, più nello specifico, nella presente Parte Speciale.

Conformemente a quanto previsto nel Codice Etico, nelle procedure, nei protocolli e nelle norme aziendali, ai soggetti sopra individuati è fatto divieto di:

- alterare e/o utilizzare abusivamente e in modo improprio i sistemi informatici aziendali;
- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- 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, onde acquisire informazioni riservate;
- 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;

- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- 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;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- utilizzare programmi e/o beni nel mancato rispetto della normativa posta a tutela del diritto d'autore e delle opere dell'ingegno.

I soggetti destinatari della presente sezione dovranno altresì:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione;
3. in caso di smarrimento o furto, informare tempestivamente il Titolare del Trattamento, e per conoscenza l'OdV, per gli opportuni provvedimenti;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea,

informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi;

5. evitare di trasferire all'esterno dell'Azienda e/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 e, comunque, previa autorizzazione del Titolare del Trattamento;

6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone;

7. evitare l'utilizzo di *passwords* di altri utenti aziendali, salvo espressa autorizzazione del Titolare del Trattamento;

8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;

10. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente e regolarmente acquisiti dall'Azienda;

12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

E' fatto altresì obbligo, per i soggetti destinatari, di osservare puntualmente le disposizioni previste dal Documento programmatico per la sicurezza (DPS) e dal "Regolamento Informatico per il trattamento e la sicurezza dei dati personali".

6. Le procedure adottate da TNE

T.N.E., al fine di garantire la corretta e costante attuazione dei principi e delle regole enunciate nel Codice Etico e nel Modello si richiama ai principi già attuati e specificamente richiamati dalla presente Sezione della Parte Speciale, nonché dalle procedure già esistenti e conformi alla disciplina normativa ed alle regole tecniche di settore.

A seguito dell'attività di monitoraggio sullo stato di attuazione del presente Modello e/o a seguito di specifiche segnalazioni che dovessero essere formulate al Consiglio di Amministrazione dalle competenti funzioni (ad es. OdV, Collegio Sindacale, Responsabile Tecnico) o dallo stesso direttamente verificate, potrà valutarsi l'opportunità di adottare specifiche procedure nella materia oggetto della presente sezione.

Nell'ambito della gestione dei sistemi informatici, l'attività di T.N.E. deve essere finalizzata a garantire:

- Riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione;
- Integrità: garanzia che ogni dato aziendale sia quello originariamente immesso nel sistema informatico e possa venire modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- Disponibilità: garanzia di reperibilità di dati aziendali in funzione delle esigenze connesse allo svolgimento dell'attività aziendale e nel rispetto delle norme che ne impongono la conservazione.

T.N.E., mediante il ricorso a soggeti esterni esperti in materia, si è dotata di un sistema di gestione informatica volto a prevenire i reati previsti dalla presente sezione.

E’ previsto un sistema di accesso alle postazioni informatiche mediante l’utilizzo di password, in dotazione ai singoli destinatari, che vengono periodicamente modificate.

Il sistema informatico di T.N.E. è protetto da un adeguato antivirus che viene regolarmente aggiornato; sono altresì stati installati filtri antispam onde garantire una corretta ed efficace gestione della posta elettronica.

I programmi informatici che sono scaricati sui computers (quali ad es. Microsoft Word, Excel, Autocad) sono versioni ufficiali debitamente licenziate; le relative licenze sono correttamente archiviate e tenute a disposizione.

Qualora dovessero emergere situazioni rilevanti che compromettano l’applicazione ed attuazione del sistema, sarà cura dell’OdV, anche su segnalazione delle funzioni competenti, darne tempestiva comunicazione all’organo dirigente proponendo le soluzioni opportune per una eventuale adeguata revisione del Modello.

Con riferimento al sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello, saranno passibili di sanzione coloro che, individuati quali destinatari della presente parte speciale, delle procedure gestionali ed istruzioni operative previste, si dovessero rendere alle stesse inosservanti.

Per quanto concerne invece i criteri di accertamento, contestazione, ed irrogazione della sanzione si rimanda integralmente alle disposizioni previste dalla Sezione “Sistema disciplinare” di cui alla Parte Generale del Modello.

7. Flussi di comunicazione

I destinatari ed i responsabili delle singole funzioni aziendali comunicano all'OdV ed al Consiglio di Amministrazione eventuali anomalie riscontrate ed afferenti l'oggetto della presente Sezione della Parte Speciale, onde consentire l'adozione degli opportuni provvedimenti.

Le figure che, in virtù di un rapporto interno e/o esterno a TNE, sono tenute ad effettuare la gestione e/o manutenzione delle apparecchiature e dei sistemi informatici, devono redigere sintetico report semestrale sull'attività svolta: tali reports sono inviati al Titolare del Trattamento che, con periodicità semestrale, provvede ad informarne l'OdV.

L'Amministratore di Sistema fornisce una relazione sullo stato di attuazione del sistema che con cadenza trimestrale viene comunicata all'OdV; il Responsabile tecnico comunica con cadenza trimestrale all'OdV sintentica relazione relative alle attività svolte che riguardano la presente sezione.

8. Le funzioni e le attività di controllo dell'Organismo di Vigilanza

Con riferimento alle funzioni di verifica e controllo dell'OdV, si rimanda integralmente a quanto già enunciato nella Parte Generale del Modello.

È in ogni caso compito dell'OdV:

1) verificare periodicamente, con il supporto delle funzioni aziendali competenti, il funzionamento del Modello di Organizzazione e Gestione e delle procedure esistenti e/o adottate;

2) verificare periodicamente, con il supporto delle funzioni aziendali competenti, la validità delle clausole standard eventualmente inserite nei contratti con consulenti, fornitori e/o partners esterni finalizzate all'osservanza, da parte dei medesimi, delle disposizioni di cui al Decreto ed

all’attuazione delle eventuali sanzioni in caso di violazione dei principi contenuti nel Codice Etico;

3) indicare all’organo dirigente le opportune integrazioni ai sistemi gestionali relativi ai flussi finanziari, con la proposizioni di modifiche o integrazioni utili a rilevare eventuali flussi finanziari atipici;

Devono essere tempestivamente comunicati all’OdV gli esiti di eventuali ispezioni e/o accertamenti da parte degli organismi di vigilanza nonché l’instaurazione di procedimenti, di natura amministrativa e/o penale, per violazione delle norme direttamente e/o indirettamente richiamate dagli articoli 24 *bis* e 25 *novies* del Decreto.

I risultati dell’attività dell’Organismo di Vigilanza devono essere riportati al Consiglio di Amministrazione ed al Collegio Sindacale, nonché al responsabile della funzione aziendale interessata; in particolare, il flusso informativo nei confronti del Consiglio di Amministrazione e del Collegio Sindacale deve consentire a tali organi di poter tempestivamente intervenire.