TORINO NUOVA ECONOMIA S.p.A.

Corso Marche n. 79

10146 Torino

MODELLO DI ORGANIZZAZIONE E GESTIONE EX ART. 6 D.LGS. N. 231/2001

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. N. 231/2001

Revisione 4 - 2025 Approvata con Determina Amministratore Unico n. 01./2025

INDICE

1. Premessa

La presente Parte Speciale del Modello è finalizzata a prevenire la commissione di reati previsti dagli articoli 24*bis* e 25*novies* del D.Lgs. n. 231/2001 nell'ambito della gestione dei sistemi informatici.

In seguito ai 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 di 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 di 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 a osservare al fine di una corretta ed efficace applicazione del Modello stesso;

2. fornire all'OdV e 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, tenuto conto di quanto specificamente disciplinato nel documento *22D00024*

"Regolamento interno - Utilizzo dei sistemi informatici" Revisione 01-Febbraio 2022 trasmesso ai Dipendenti con lettera prot. FT/alm/22/035 del 10 febbraio 2022.

3. Le ipotesi di reato rilevanti

3.1 Reati ex art. 24bis D.Lgs. n. 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 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 (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).

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, ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Tale condotta assume rilievo penale sia ove l'intrusione sia effettuata nel sistema informatico o telematico della Società (es. maggiorazione del costo dei servizi erogati, fatturazione servizi non richiesti) sia ove sia effettuata 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 un anno e sei mesi a cinque anni* (le parole "da un anno e sei mesi a cinque anni" sono state sostituite alle parole "da sei mesi a quattro anni" dall'art. 19, comma 5, lett. a), L. 23 dicembre 2021, n. 238).

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 tre *a otto anni se il fatto è commesso* (le parole "da tre a otto anni" sono state sostituite alle parole "da uno a cinque anni" dall'art. 19, comma 5, lett. b), L. 23 dicembre 2021, n. 238)*:*

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 a un sistema informatico o telematico intercorrenti tra più sistemi, 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.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617*quinquies* c.p.) (Rubrica sostituita dall'art. 19, comma 6, lett. b), L. 23 dicembre 2021, n. 238, il testo precedente era il seguente: "Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche").

"Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti 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 (le parole "al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra

più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti" sono state sostituite alle parole "installa apparecchiature atte" dall'art. 19, comma 6, lett. a), L. 23 dicembre 2021, n. 238).
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 a intercettare, impedire o interrompere comunicazioni relative a 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 (comma sostituito dall'art. 2 D.lgs. 15 gennaio 2016, n. 7. Il testo recitava: "Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata").

L'articolo in esame punisce chiunque commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o a 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 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.*
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata" (*comma sostituito dall'*art. 2 D.lgs. 15 gennaio 2016, n. 7*. Il testo recitava: "Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata*").

Il reato si configura quando un soggetto attraverso le condotte di cui all'art. 635*bis* ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento, 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". (*comma sostituito dall'*art. 2 D.lgs. 15 gennaio 2016, n. 7*. Il testo recitava: "Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata"*).

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 ovvero a ostacolarne gravemente il funzionamento.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (Rubrica così sostituita dall'art. 19, comma 1, lett. c), L. 23 dicembre 2021, n. 238. Il testo

precedente era il seguente: “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, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti (le parole “si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti” sono state sostituite alle parole “si procura, riproduce, diffonde, comunica o consegna” dall’art. 19, comma 1, lett. a), L. n. 238/2021) codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni (le parole “sino a due anni” sono state sostituite alle parole “sino ad un anno” dall'art. 19, comma 1, lett. a), L. n. 238/2021) e con la multa sino a 5.164 euro. *La pena è della reclusione da uno a tre* (la parola “tre” è stata sostituita alla parola “due” dall'art. 19, comma 1, lett. b), L. n. 238/2021) *anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui al* (la parola “al” è stata sostituita alle parole “ai numeri 1) e 2) del” dall'art. 19, comma 1, lett. b), L. n. 238/2021) *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 a un sistema informatico o telematico protetto da misure di sicurezza ovvero 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.

Detenzione, diffusione e installazione abusiva (le parole “Detenzione, diffusione e installazione abusiva” sono state sostituite alla parola “Diffusione” dall’art. 19,

comma 2, lett. b), L. 23 dicembre 2021, n. 238.) 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, abusivamente si procura, detiene, (le parole "abusivamente si procura, detiene" sono state sostituite alle parole "si procura" dall'art. 19, comma 2, lett. a), L. n. 238/2021) produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa (Le parole "abusivamente si procura, detiene" sono state sostituite alle parole "mette a disposizione di altri" dall'art. 19, comma 2, lett. a), L. n. 238/2021) 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 procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta 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 a 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.) (articolo sostituito dall'art. 2 D.lgs. 15 gennaio 2016, n. 7)

"*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 sostituito dall'art. 2 del D.lgs. 15 gennaio 2016 n. 7).

L'articolo in esame sanziona il comportamento di chi ponga in essere condotte riconducibili ai reati di cui al Capo III, Titolo VII, Libro II del Codice Penale (*Della falsità in atti*), aventi a 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);
- Falsità in testamento olografo, cambiale o titolo di credito (art. 491 c.p.) (articolo sostituito dall'art. 2 del D.lgs. 15 gennaio 2016 n. 7);
- Documenti informatici (art. 491*bis* c.p.) (articolo sostituito dall'art. 2 D.lgs. 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.):
- Casi di perseguibilità a querela (art. 493*bis* c.p.);
- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493*ter* c.p.) (articolo inserito dall'art. 4, comma 1 lett. a) del D.lgs. 1° marzo 2018, n. 21; rubrica così sostituita dal'art. 2, comma 1, lett. a), n. 1, D.lgs. 8 novembre 2021, n. 184);
- Detenzione e diffusione di apparecchiature, dispositivo o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (articolo inserito dall'art. 2, comma 1, lett. b), D.lgs. 8 novembre 2021, n. 184) (art. 493*quater* 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. 25octies 1 D.lgs. n. 231/2001

L'art. 25*octies* 1 del D.lgs. 231/2001, rubricato "Delitti in materia di strumenti di pagamento diversi dai contanti" e inserito dall'articolo 3, comma 1, del D.Lgs. 8 novembre 2021, n. 184, così dispone:

1. In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di cui all'articolo 493-ter, la sanzione pecuniaria da 300 a 800 quote;

b) per il delitto di cui all'articolo 493-quater e per il delitto di cui all'articolo 640-ter, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria sino a 500 quote.

2. Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) se il delitto è punito con la pena della reclusione inferiore ai dieci anni, la sanzione pecuniaria sino a 500 quote;

b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote.

3. Nei casi di condanna per uno dei delitti di cui ai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.

Vengono di seguito riportati gli articoli del Codice penale richiamati dall'art. 25 *octies* 1 del Decreto.

Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493ter c.p.)

Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti (Le parole "o comunque ogni altro strumento di pagamento diverso dai contanti" sono state inserite dall'art. 2, comma 1, lett. a), n. 2, D.lgs. 8 novembre 2021, n. 184.) è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo (Le parole "gli strumenti o i documenti di cui al primo periodo" sono state sostituite alle parole "carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi" dall'art. 2, comma 1, lett. a), n. 3, D.lgs. 8 novembre 2021, n. 184.), ovvero possiede, cede o acquisisce tali strumenti (Le parole "tali strumenti" sono state sostituite alle parole "tali carte" dall'art. 2, comma 1, lett. a), n. 3, D.lgs. 8 novembre 2021, n. 184) o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta.

Il delitti di cui all'art. 493*ter* consistono: 1) nell'indebita utilizzazione, da parte di chi non ne è titolare, di carte di credito o pagamento o di qualsiasi altro documento analogo che abiliti al prelievo di contante, all'acquisto di beni o alla prestazione di servizi, o comunque di ogni altro strumento di pagamento diverso dai contanti; 2) nella falsificazione o nell'alterazione dei medesimi documenti o strumenti; 3) nel possesso, nella cessione o nell'acquisizione degli strumenti e dei documenti descritti, ove di provenienza illecita, o di ordini di pagamento prodotti con essi.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.
In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

L'*art.* 493*quater* contempla una norma a più fattispecie.

Di conseguenza il delitto *de quo* si configura anche se il soggetto attivo ha realizzato una sola delle condotte descritte dalla norma. L'integrazione contestuale ovvero senza un'apprezzabile soluzione di continuità di più condotte tipiche da parte dello stesso agente non comporta una pluralità di reati, e, quindi, un concorso formale fra gli stessi, ma rileva unicamente sul piano della dosimetria della pena ai sensi dell'art. 133.

La condotta consiste nel produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri l'oggetto materiale del reato e si caratterizza per essere finalizzata a consentire l'uso o a permettere l'utilizzo da parte di altri delle apparecchiature, dispositivi o programmi informatici predisposti o adattati proprio per commettere reati riguardanti strumenti di pagamento diversi dai contanti.

"Il mettere a disposizione o in qualsiasi modo procurare a sé o a altri" appare una clausola di chiusura e onnicomprensiva volta a includere nella sfera di rilevanza penale qualsiasi modalità con cui gli oggetti materiali sopra riportati vengano messi nella disponibilità di terzi da parte dell'agente.

Frode informatica (art. 640ter c.p.)

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, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.
La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o (Le parole "produce un trasferimento

di denaro, di valore monetario o di valuta virtuale o" sono state aggiunte dall'art. 2, comma 1, lett. c), D.lgs. 8 novembre 2021, n. 184.) è commesso con abuso della qualità di operatore del sistema.
La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età [, e numero 7] (Comma modificato dall'art. 2, comma 1, lett. p), D.lgs. 10 ottobre 2022, n. 150, che ha sostituito le parole "la circostanza prevista" alle parole taluna delle circostanze previste" e ha soppresso le parole", e numero 7"*).*

Il reato di frode informatica prevede quale elemento materiale del reato, in luogo degli artifizi e raggiri previsti per il reato di truffa, una mera attività materiale di alterazione o manipolazione di un sistema informatico o telematico posta in essere intervenendo, con qualsiasi modalità, su dati, informazioni o programmi contenuti in un sistema informatico o telematico. Sono quindi previste quindi due condotte alternative di realizzazione del reato: da un lato l'alterazione di un sistema informatico o telematico, attuabile con le modalità più diverse, attraverso la quale il sistema viene modificato o manipolato, dunque distratto dai suoi schemi predefiniti, in vista del perseguimento da parte dell'agente di un ingiusto profitto con altrui danno; da un altro lato l'intervento, con qualsiasi modalità attuativa, sui dati, le informazioni o i programmi contenuti nel sistema effettuato in modo da realizzare un ingiusto profitto con altrui danno.

La Cassazione ha, al riguardo, chiarito che il reato di frode informatica di cui all'art. 640*ter*, ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione

in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

3.3 Reati ex art. 25novies D.lgs. n. 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 n. 231/2001 inserisce come reati-presupposto solo la lettera a *bis*) del primo comma e il terzo comma.
La lett. a *bis*) del primo comma, introdotta dal D.L. 31 gennaio 2005 n. 7 punisce la messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa. attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere.
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 a 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 o alla

reputazione dell'autore.
Quest'ultima fattispecie, pertanto, è rivolta in particolare alla tutela dell'onore e della reputazione dell'autore dell'opera.
Passando 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 (SIAE).
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 a 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 e 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 a 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 "Modello organizzativo del sistema per la protezione dei dati e per la sicurezza delle informazioni" parte integrante del documento GDPR societario previsto dal D.Lgs 196/03 e s.m.i. e Regolamento (UE) 2016/679.

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:

- Organo Amministrativo;
- Collegio Sindacale;
- Ufficio Tecnico;
- Soggetti terzi incaricati dalla Società per il compimento di specifiche attività nell'interesse della medesima;
- Supporto esterno;
- Soggetti che, in base alla disciplina contenuta nel Titolo IV del D.Lgs. n. 81/2008 e/o in virtù della specifica disciplina dei contratti 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 necessari allo svolgimento delle attività che hanno richiesto il collegamento;

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

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 "Modello organizzativo del sistema per la protezione dei dati e per la sicurezza delle informazioni" e dal "Regolamento interno – Utilizzo dei Sistemi Informatici" e dal "Regolamento Generale di Protezione

Dati".

6. Le procedure adottate da T.N.E.

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 di Parte Speciale, nonché dalle procedure già esistenti e conformi alla disciplina normativa e alle regole tecniche di settore.

In seguito all'attività di monitoraggio sullo stato di attuazione del presente Modello e/o a seguito di specifiche segnalazioni che dovessero essere formulate all'Organo Amministrativo 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 da non poter 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 soggetti esterni esperti in materia, si è dotata di un

sistema di gestione informatica volto a prevenire i reati indicati dalla presente Sezione.
La Società cui è stata affidata l'amministrazione, la gestione, la manutenzione e l'aggiornamento del sistema informativo (hardware e software) è stata incaricata altresì della sicurezza dell'accesso alla rete aziendale e della protezione da intrusioni dall'esterno. A tale compito sovrintende una risorsa che ricopre il ruolo di Amministratore del Sistema Informatico di T.N.E. che, tra l'altro, cura, con cadenza trimestrale, il Report di verifica contenente le informazioni sulle navigazioni internet, sugli attacchi esterni, sulla efficacia del sistema firewall e sul funzionamento del sistema backup.

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 regolarmente aggiornato; sono altresì stati installati filtri antispam onde garantire una corretta ed efficace gestione della posta elettronica.

I programmi informatici scaricati sui *computers* (quali. 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 possano compromettere l'applicazione e 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 e istruzioni operative previste, si dovessero rendere alle stesse inosservanti.

Per quanto concerne invece i criteri di accertamento, contestazione e 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 e i responsabili delle singole funzioni aziendali comunicano all’OdV e all’Organo Amministrativo eventuali anomalie riscontrate ed afferenti all’oggetto della presente Sezione di 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 a 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 a informarne l’OdV.

L’Amministratore di Sistema Informatico 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 sintetica relazione sulle 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 e 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 proposizione 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 all'Organo Amministrativo e al Collegio Sindacale, nonché al responsabile della funzione aziendale interessata; in particolare, il flusso informativo nei confronti dell'Organo Amministrativo e del Collegio Sindacale deve consentire a tali organi di poter tempestivamente intervenire.