MODELLO DI ORGANIZZAZIONE E DI GESTIONE

PARTE SPECIALE N. 3

ARTT. 24 BIS E 25-NOVIES D. LGS. 231/01

(IN TEMA DI DELITTI INFORMATICI E DI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE)

Documento:	*Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01*		
Approvazione:	*Consiglio di Amministrazione*	**Verbale riunione del:**	19/12/2017
Revisione:			
Revisione:			

I Percorsi A PICCOLI PASSI

PROGETTO PERSONA ONLUS

0. PREMESSA

La presente Parte Speciale individua, in modo specifico, le condotte criminose che possono originare una responsabilità amministrativa dell'Ente in relazione alla realizzazione di reati informatici, ex art. 24 *bis* del Decreto, e dei reati di violazione del diritto d'autore, di cui all'art. 25 *novies* dello stesso.
A tal riguardo si sottolinea che, nonostante le due tipologie di reati tutelino beni giuridici differenti, si è ritenuto opportuno ricomprenderli in un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

1. I DELITTI INFORMATICI

Il legislatore attraverso la tutela della sicurezza informatica intende tutelare il buon andamento dell'intero sistema economico. Ed infatti l'informatica oggi governa l'intero sistema di comunicazione, di registrazione e conservazione dei dati.
Lo sviluppo della tecnologia informatica ha generato, nel corso degli anni, modifiche sostanziali nell'organizzazione del *business* di impresa e ha inciso sensibilmente sulle opportunità a disposizione di ciascun esponente aziendale per realizzare e occultare non soltanto schemi di condotte criminali già esistenti, ma anche fattispecie nuove, tipiche del cd. mondo virtuale.
A ciò si aggiunga l'ingresso massivo di dispositivi mobili (es. *tablet* e *smartphone*), l'utilizzo di *server* di *cloud computing* che moltiplicano le opportunità di realizzare un reato informatico e determinano la necessità per le imprese di adeguarsi rapidamente al fine di disciplinare correttamente la gestione di tali fenomeni.
Gran parte delle aziende è, infatti, dipendente dall'efficace gestione delle informazioni e delle relative tecnologie informatiche, dipendenza che porta, però, ad una crescente vulnerabilità in relazione ad un ampio spettro di minacce, quali *cyber* attacchi, gravi incidenti aziendali causati dal malfunzionamento dei sistemi, etc., anche considerando la notevole complessità portata dal moltiplicarsi di protocolli di accesso e comunicazione (UMTS, WiMax, ecc.), dei canali di trasmissione dei dati (ADSL, fibra, satellite, bluetooth, etc), dei contenuti e delle applicazioni multimediali e on-line, dell'*hardware* disponibile per accedere ai dati (palmare, PC, notebook, etc.).
Le tipologie di reato informatico si riferiscono ad una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e, in altri casi, lo strumento attraverso cui l'autore intende realizzare un'altra fattispecie penalmente rilevante.
Quanto ai soggetti esposti a tale fattispecie di reato, tale fenomeno può coinvolgere potenzialmente qualsiasi ente che utilizzi in maniera rilevante gli strumenti informatici e telematici per lo svolgimento delle proprie attività. Con riguardo alle aree aziendali più esposte al rischio di commissione di tale categoria di reato presupposto, è bene evidenziare che ve ne sono alcune (es. area amministrazione, finanza e controllo, marketing, area IT, area acquisti) che

risultano maggiormente esposte al rischio di commissione di reati informatici che possono determinare un interesse o vantaggio economico per l'azienda.
È, peraltro, possibile ipotizzare che i reati informatici possano essere anche strumentali alla commissione degli altri reati presupposto per l'insorgere di responsabilità amministrativa degli enti. A titolo esemplificativo, in relazione ai reati societari, l'alterazione di dati, la loro manipolazione o altra analoga condotta possono determinare un'alterazione delle comunicazioni sociali. Analogamente, è possibile ipotizzare che, tramite, per esempio, la detenzione e diffusione abusiva di codici d'accesso ai sistemi informatici o telematici (art. 615 *quater* c.p.) si verifichi l'accesso fraudolento ad un sistema di *Home Banking* al fine di erogare denaro per corrompere.

Definizioni:
Credenziali: l'insieme degli elementi identificativi di un utente o di un *account* (generalmente *User ID e Password).*
Dati Informatici: qualunque rappresentazione di fatti, informazioni, o concetti in forma idonea per l'elaborazione di un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.
Delitti Informatici: i reati di cui all'art. 24-*bis* del Decreto.
Documento/i Informatico/i: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
L.A. o Legge sul Diritto d'Autore: Legge 22 aprile 1941 n. 633 sul diritto d'autore.
Password: sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.
Peer to Peer: meccanismo di condivisione di contenuti digitali tramite una rete di personal computer, di regola utilizzati per scambio di file con contenuti audio, video, dati e *software*.
Documento Programmatico sulla Sicurezza (DPS): documento che definisce un insieme di attività coordinate che devono essere intraprese per implementare la politica di sicurezza del sistema.
Postazione di Lavoro: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.
Sicurezza Informatica: l'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.
Sistemi Informativi: l'insieme della rete, dei sistemi, dei *database* e delle applicazioni aziendali.
Spamming: invio di numerosi messaggi indesiderati, di regola attuato attraverso l'utilizzo della posta elettronica.
Virus: programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.

I delitti informatici considerati presupposto per l'applicazione della responsabilità amministrativa ai sensi del D. Lgs. 231/01, sono individuati dal citato articolo **24-*bis*[1]** come segue:

- falsità in documenti informatici (art. 491-bis del codice penale);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter del codice penale);

[1] Introdotto dall'art. 7, comma 1, L. 18 marzo 2008, n. 48.

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater del codice penale);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies del codice penale);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater del codice penale);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies del codice penale);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis del codice penale);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (art. 635-ter del codice penale);
- danneggiamento di sistemi informatici o telematici (art. 635-quater del codice penale);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies del codice penale);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies del codice penale).

Occorre, inoltre, ricordare il reato di frode informatica a danno dello Stato (art. 640 ter c.p.) codificato nell'art. 24 del Decreto 231/01 e rilevato nell'ambito delle attività a rischio in relazione ai reati contro la Pubblica Amministrazione.

Il D. Lgs. n° 7/2016 ha introdotto modifiche al alcuni dei reati presupposto di cui all' elenco.

Di seguito si analizzano le singole fattispecie criminose. Al riguardo, si precisa che verranno trattati i soli reati informatici che, sulla base della mappatura dei rischi condotta nella Cooperativa Progetto Persona, risultano avere attinenza, in astratto, con l'attività e le caratteristiche della cooperativa medesima.

FALSITÀ IN DOCUMENTI INFORMATICI (ART. 491-BIS C.P.)

[I]. 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
(art. modificato dal D. Lgs. n. 7/2016)

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 400 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) divieto di contrattare con la pubblica amministrazione; 2) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; 3) divieto di pubblicizzare beni o servizi. Tutte per una durata non inferiore a tre mesi e non superiore a due anni.

La norma estende la punibilità prevista dal Codice Penale per i reati di falso in atti anche alle falsità commesse in relazione a documenti informatici pubblici aventi efficacia probatoria.
Nella specie, per quanto interessa in questa sede, sono punite:

- la falsità materiale commessa dal privato (art. 482);

- la falsità ideologica commessa dal privato in atto pubblico (art. 483);
- la falsità in registri e notificazioni (art. 484);
- le altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488);
- l'uso di atto falso (art. 489);
- la soppressione, distruzione e occultamento di atti veri (art. 490);
- documenti equiparati agli atti pubblici agli effetti della pena (art. 491).

Con la norma in commento, il Legislatore ha inteso tutelare i dati informatici che circolano e si comunicano in quanto tali, anche a prescindere dai relativi supporti, ed il loro valore probatorio.
Con riguardo alle fattispecie richiamate dall'art. 491 bis, alcune precisazioni si impongono:

- 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 falsifichi documenti aziendali oggetto di flussi informatizzati, la falsificazione di documenti informatici correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche, in modo che queste risultino eseguite da altri, la falsificazione di documenti informatici da parte di enti che procedono a rendicontazione elettronica di attività o 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.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-TER C.P.)

[I]. 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.
[II]. 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.

[III]. 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.

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

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di pubblicizzare beni o servizi. Tutte per una durata non inferiore a tre mesi e non superiore a due anni.

Il reato punisce chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza, ovvero chi vi permane contro la volontà di chi ha il diritto di escluderlo.
Secondo la giurisprudenza[2], la norma incriminatrice descrive la condotta nel senso della mera introduzione nel sistema e non richiede né che ciò abbia comportato lesione della riservatezza dei legittimi utenti, né che l'intrusione sia stata effettuata allo scopo di insidiare detta riservatezza. Trattasi insomma di un reato di mera condotta. Va da sé che il bene tutelato è la riservatezza informatica, ma il legislatore ha inteso anticipare la tutela stabilendo la punibilità della semplice condotta di abusiva introduzione.
Il dolo richiesto è generico, e consiste nella coscienza e volontà di entrare in un sistema informatico o telematico protetto ovvero di permanervi contro la volontà di chi può escluderlo, con la consapevolezza dell'*abusività* di tale condotta.
Il delitto si consuma, nella prima ipotesi, con la semplice introduzione nel sistema, mentre, nella seconda, col permanervi dopo che chi ha il diritto di escluderlo ha appunto manifestato tale intenzione.
Il reato è facilmente realizzabile nei luoghi di lavoro dove l'intervento temporaneo sulla macchina del collega si rivela uno dei momenti più a rischio per l'integrità del sistema stesso. In molti casi, anche la semplice curiosità gioca degli "scherzi" che possono avere delle conseguenze notevolmente dannose, quali l'inopportuna cancellazione di alcuni file o, peggio, il danneggiamento di alcuni comandi fondamentali per il funzionamento del sistema stesso.
La fattispecie penale in questione restringe, tuttavia, il suo campo di azione ai soli casi di accesso ad un sistema informatico o telematico che sia protetto da "misure di sicurezza".
L'intenzione del legislatore è quella, cioè, di punire soltanto ove il titolare del sistema abbia dimostrato, attraverso l'inserimento di misure di sicurezza (che possono essere di vario tipo, come l'esperienza insegna; può trattarsi di: misure fisiche (come la vigilanza), logiche (*password*), biometriche (lettura dell'iride o dell'impronta digitale), la volontà di riservare l'accesso solo a persone da lui autorizzate.
A titolo esemplificativo, il delitto potrebbe essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*) per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, o

[2] Cass. pen., Sez. V, sent. 6 febbraio 2007, n. 11689.

acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa, o, ancora, nell'ipotesi di violazione dei sistemi informatici dei concorrenti per acquisire, a scopo di spionaggio industriale, la documentazione relativa ai loro prodotti o progetti.
Il 2° comma dell'art. 615 *ter* prevede tre aggravanti speciali, che ricorrono:

- se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso di 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;
- se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 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.

Il 3° comma dell'articolo, infine, prevede un'ulteriore aggravante, che sussiste se i fatti riguardano sistemi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-QUATER C.P.)

> *[I]. 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 euro 5.164.*
> *[II]. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.*

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 300 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 2) divieto di pubblicizzare beni o servizi. Tutte per una durata non inferiore a tre mesi e non superiore a due anni.

La norma mira a punire chi, 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 noto che a protezione dell'accesso a programmi riservati sono previste delle "*password*" (codici di accesso riservati, nominativi o numerici) la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico.

Con la disposizione in parola il legislatore ha configurato un'ipotesi di reato di pericolo tendente ad evitare la consumazione di più gravi delitti contro la riservatezza (es: art. 615 *ter*) o contro il patrimonio (es: art. 640 *ter*, frode informatica).
La norma incrimina due tipologie di condotte, volte, rispettivamente, ad acquisire i mezzi necessari per accedere al sistema informatico altrui ("si procura", "riproduce") ovvero a procurare ad altri tali mezzi o, comunque, le informazioni sul modo di eludere le barriere di protezione ("diffonde", "comunica", "consegna").
Ai sensi del secondo comma dell'art. 615 *quater* il delitto è aggravato se il fatto è commesso:

- 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;
- 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.

Potrebbe rispondere del delitto, ad esempio, il dipendente della cooperativa (A) che comunichi ad un altro soggetto (B) la *password* di accesso alla casella *email* di un proprio collega (C), allo scopo di garantire a B la possibilità di controllare le attività svolte da C, quando da ciò possa derivare un determinato vantaggio o interesse per la cooperativa.

DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-QUINQUIES C.P.)

> *[I]. 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.*

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 300 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 2) divieto di pubblicizzare beni o servizi. Tutte per una durata non inferiore a tre mesi e non superiore a due anni.

Viene punito chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o 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 di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
Con tale norma si mira a reprimere la diffusione dei famigerati "*virus*" informatici, forieri di gravi danni ai sistemi informatici e telematici, utilizzati spesso per scopi di sabotaggio.
Dalla lettera dell'articolo si deduce che il reato è configurabile sia in caso di messa in circolazione di programmi virus, sia in caso di produzione degli stessi o, finanche, il procurarsi, l'importare sia *software* che *hardware* adatti allo scopo.

Quanto all'elemento soggettivo, il reato è punibile a titolo di dolo generico, consistente nella coscienza e volontà della condotta con la consapevolezza dell'idoneità del virus a danneggiare un sistema informatico o telematico, a prescindere dalla finalità dell'agente.
Tale delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico dell'ente.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUATER C.P.)

> *[I]. 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.*
> *[II]. 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.*
> *[III]. 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.*

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di pubblicizzare beni o servizi. Tutte per una durata non inferiore a tre mesi e non superiore a due anni.

La disposizione in esame punisce diverse condotte. In particolare,

- ai sensi del co. 1, la condotta può consistere, alternativamente,
  - nell'intercettare fraudolentemente, o
  - nell'impedire o interrompere

  comunicazioni relative ad un sistema informatico o telematico;
- ai sensi del co. 2, poi, la punibilità è estesa a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

Intercettare una comunicazione, come noto, significa prendere cognizione del suo contenuto, intromettendosi nella fase della sua trasmissione.

Al fine di configurare la fattispecie penalmente rilevante non è, tuttavia, sufficiente l'intercettazione, ma questa deve essere realizzata fraudolentemente, ossia eludendo eventuali sistemi di protezione della trasmissione in corso, o, comunque, in modo tale da rendere non percettibile o riconoscibile a terzi l'abusiva intromissione.
Parallelamente, si ha impedimento di una comunicazione informatica o telematica allorché se ne renda impossibile la trasmissione, intervenendo sul sistema informatico che deve inviare o ricevere i dati. L'interruzione di una comunicazione già in corso di trasmissione, invece, può estrinsecarsi sia agendo sul sistema che invia o che riceve la comunicazione, sia, ad esempio, deviando il flusso dei dati in corso di trasmissione da un elaboratore a un altro.
A differenza di quanto affermato con riguardo all'intercettazione, le modalità di condotta predette (impedimento e interruzione) non necessitano di essere realizzate fraudolentemente.
La rivelazione delle comunicazioni può avvenire mediante qualsiasi mezzo di informazione al pubblico. Deve certamente trattarsi, però, di un mezzo idoneo a divulgare la notizia a una genericità di soggetti.
Per comunicazione informatica si intende qualsiasi scambio di dati intercorrente tra due o più sistemi informatici: si pensi al semplice scambio di e-mail, alle *mailing list*, ai *forum*, ai *newsgroup* o alle *chat*.
Per poter parlare di intercettazione abusiva, è necessario poter determinare il numero dei destinatari ai quali tale comunicazione è diretta, al fine di poter distinguere le comunicazioni a carattere privato, con quelle a carattere pubblico, per la quale non è ipotizzabile alcuna riservatezza (es., siti web).
Le condotte sopra descritte devono avere ad oggetto "comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi". A tal proposito, si impone considerare che:

- hanno comunicazioni relative ad un sistema informatico o telematico quando le comunicazioni intercorrano tra due apparecchi, uno solo dei quali è rappresentato da un sistema informatico/telematico (es. invio di un fax ad un computer);
- diversamente, la comunicazione intercorre tra più sistemi quando sia l'apparecchio che trasmette la comunicazione sia quello che la riceve siano sistemi informatici/telematici.

Il dolo è generico, e consiste nella consapevolezza e volontà di intercettare fraudolentemente, impedire o interrompere una comunicazione come sopra descritta, ovvero di rivelare, con un mezzo di comunicazione al pubblico, tutto o parte del contenuto di una comunicazione intercettata.
I delitti sono aggravati qualora il fatto sia 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.

A mero titolo esemplificativo, il reato potrebbe configurarsi allorché un dipendente o un amministratore intercetti fraudolentemente un consiglio di amministrazione di un ente concorrente che si tenga via *conference call* per acquisire informazioni riservate.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-BIS C.P.)

[I]. 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.
(art. modificato dal D. Lgs. n. 7/2016)

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di pubblicizzare beni o servizi. Tutte queste sanzioni interdittive possono avere una durata non inferiore a tre mesi e non superiore a due anni.

La condotta di danneggiamento deve necessariamente e tassativamente estrinsecarsi nella distruzione, nel deterioramento, nella cancellazione, nell'alterazione o nella soppressione di informazioni, dati o programmi informatici altrui.
Il danneggiamento potrebbe essere commesso, ad esempio, mediante la diffusione di virus.
Sempre a titolo esemplificativo, il vantaggio dell'ente potrebbe ritenersi integrato laddove l'eliminazione o l'alterazione dei *files* o di un programma informatico siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti" di cui altro soggetto sia in possesso.

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.)

[I]. 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.
[II]. 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.
[III]. 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.
(art. modificato dal D. Lgs. n. 7/2016)

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3)

divieto di pubblicizzare beni o servizi. Tutte per una durata non inferiore a tre mesi e non superiore a due anni.

Sebbene la condotta incriminata ricalchi quella prevista dall'art. 635-bis c.p., tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.
Tale reato potrebbe, ad esempio, essere commesso nell'interesse dell'ente qualora un dipendente invii un virus al computer di un ufficio pubblico (es. cancelleria di un Tribunale) allo scopo di distruggere documenti informatici aventi efficacia probatoria e relativi ad un procedimento penale e/o amministrativo o tributario che penda a carico della Società.
Per quanto tale rischio non possa considerarsi del tutto inesistente, la probabilità della sua realizzazione, alla luce del *risk assessment* effettuato, si considera del tutto remota.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER C.P.)

> *[I]. 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.*
> *[II]. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635[3] ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di pubblicizzare beni o servizi. Tutte le sanzioni interdittive possono avere una durata non inferiore a tre mesi e non superiore a due anni.

Tale delitto, che richiama le condotte incriminate dall'art. 635-bis c.p., punisce il danneggiamento ed il grave ostacolo al funzionamento di sistemi informatici o telematici altrui. Poiché il danneggiamento deve derivare da un intervento sui dati, esso difficilmente potrà interessare le componenti materiali del sistema.
Anche in questo caso, il danneggiamento potrebbe essere commesso, ad esempio, mediante la diffusione di virus, che, però, devono intaccare lo stesso funzionamento del *computer* altrui.

[3] *"Con violenza alla persona o con minaccia".*

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635-QUINQUIES C.P.)

> *[I]. Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, 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.*
> *[II]. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635*[4] *ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di pubblicizzare beni o servizi. Tutte le sanzioni interdittive possono avere una durata non inferiore a tre mesi e non superiore a due anni.

Analogamente a quanto rilevato in relazione al reato di cui all'art. 635-ter c.p. (*supra*), la condotta incriminata dalla norma in commento ricalca quella prevista dall'art. 635-quater c.p. che precede. Differisce, però, l'oggetto materiale del reato, perché il danneggiamento deve, in questa ipotesi, riguardare sistemi informatici o telematici di pubblica utilità.
Tale reato potrebbe, ad esempio, essere commesso nell'interesse della società qualora un dipendente invii un virus al computer di un ufficio pubblico (es. cancelleria di un Tribunale) allo scopo di distruggere non solo documenti informatici aventi efficacia probatoria relativi ad un procedimento penale e/o amministrativo o tributario che penda a carico della Società, ma lo stesso funzionamento del computer.
Per quanto tale rischio non possa considerarsi del tutto inesistente, la probabilità della sua realizzazione, alla luce del *risk assessment* effettuato, si considera del tutto remota.

2. I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

I delitti in materia di violazione del diritto d'autore considerati presupposto per l'applicazione della responsabilità amministrativa ai sensi del D. Lgs. 231/01, sono individuati dall'articolo **25-*novies***[5] come segue:

- art. 171, primo comma, lettera a-*bis*), e terzo comma della legge 22 aprile 1941, n. 633;
- art. 171 *bis* della legge 22 aprile 1941, n. 633;
- art. 171 *ter* della legge 22 aprile 1941, n. 633;
- art. 171 *septies* della legge 22 aprile 1941, n. 633;
- art. 171 *octies* della legge 22 aprile 1941, n. 633.

[4] *"Con violenza alla persona o con minaccia".*
[5] Introdotto dall'art. 15, comma 7, lett. c), L. 23 luglio 2009, n. 99.

Essi concernono condotte quali, ad esempio, l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE; la riproduzione o il reimpiego del contenuto di banche dati; l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico; l'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.
Tali reati potrebbero essere compiuti nel perseguimento degli interessi della Società a prescindere dall'eventuale impiego – a tal fine – di beni aziendali (come gli strumenti informatici o i sistemi di diffusione di informazioni).

Da un'analisi preliminare è emersa l'immediata inapplicabilità a Fila S.p.A. delle fattispecie di cui agli artt. 171ter, 171septies e 171octies L.A.. Si provvede pertanto a fornire qui di seguito una breve descrizione delle due fattispecie di cui all'art. 25-*nonies* del Decreto ritenute *prima facie* di potenziale rilevanza per la Società, previste dagli artt. 171 comma 1 lett. a-*bis*) e comma 3, e 171-*bis* L.A

ART. 171, PRIMO COMMA, LETTERA A-*BIS*), E TERZO COMMA L. 633/1941

[I]. Salvo quanto previsto dall'articolo 171 bis e dall'articolo 171 ter è punito con la multa da euro 51 ad euro 2.065 chiunque, senza averne diritto, a qualunque scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana;

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

e) soppressa

f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o

ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

[II] Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

[III] La pena è della reclusione fino ad un anno o della multa non inferiore ad euro 516 se i reati di cui sopra sono commessi sopra 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.

[IV] La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione dell'attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da euro 1.032 a euro 5.164 (due a dieci milioni di lire).

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 4) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; 5) divieto di pubblicizzare beni o servizi. Tutte le sanzioni interdittive possono avere una durata da 3 mesi ad un anno.

In relazione alla fattispecie delittuosa di cui all'art. 171, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

- la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa;
- la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, 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.

Nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete; nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.
Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero caricati sul sito Internet aziendale dei contenuti coperti dal diritto d'autore o laddove nell'attività di call center venisse utilizzato un *giungle* associabile a società diversa da quella per la quale si presta il servizio.

ART. 171 BIS L. 633/1941

[I]. 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), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 (lire cinque milioni) a euro 15.493 (lire trenta milioni). La stessa pena si applica 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. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 (lire trenta milioni) se il fatto è di rilevante gravità.
[II] 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-quinquies 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, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 (lire cinque milioni) a euro 15.493 (lire trenta milioni). La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 (lire trenta milioni) se il fatto è di rilevante gravità.

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 100 a 500 quote;
Sanzioni interdittive ex D. Lgs. 231/01: 1) interdizione dall'esercizio dell'attività; 2) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; 3) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; 4) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; 5) divieto di pubblicizzare beni o servizi. Tutte le sanzioni interdittive possono avere una durata da 3 mesi ad un anno.

La norma in esame è volta a tutelare il corretto utilizzo dei *software* e delle banche dati. Per i *software*, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".
Il reato in ipotesi si configura nel caso in cui qualcuno abusivamente duplichi, 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 SIAE.
Il fatto è punito, altresì, se la condotta ha ad oggetto 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.
Il secondo comma punisce, inoltre, 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 ovvero esegue l'estrazione o il reimpiego della banca di dati ovvero distribuisce, vende o concede in locazione una banca di dati.

Tale reato potrebbe, ad esempio, essere commesso nell'interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali al fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un *software* originale.

3. I PROCESSI E LE AREE A RISCHIO INDIVIDUATE

Con riferimento specifico ai delitti informatici, ai fini della presente Parte Speciale i processi sensibili e le aree a rischio, suddivisi per macro-aree, sono i seguenti:

a) Controllo e gestione della sicurezza del sistema informatico;
b) Gestione dei beni strumentali e delle utilità aziendali (es. autovetture, cellulari, personal computer, carte di credito aziendali, ecc.);
c) Rilevazione, controllo e rendicontazione del servizio;
d) Utilizzo apparecchiature informatiche aziendali.

Con riferimento specifico ai delitti in materia di violazione del diritto d'autore, ai fini della presente Parte Speciale, i processi sensibili e le aree a rischio sono i seguenti:

a) Comunicazione commerciale;
b) Controllo e gestione della sicurezza del sistema informatico;
c) Rilevazione, controllo e rendicontazione del servizio;
d) Utilizzo apparecchiature informatiche aziendali;

4. I PRESIDI DI CONTROLLO

Le procedure e gli ulteriori presidi che verranno di seguito rappresentati si propongono di garantire che tutti i soggetti coinvolti nell'attività di Fila S.p.A., ciascuno nell'ambito del proprio ruolo, adottino e mantengano condotte lecite e corrette, così da prevenire la commissione dei reati descritti ai precedenti paragrafi 1 e 2.

Con riferimento specifico ai delitti informatici, di cui all'art. 24-*bis* del Decreto:

PROCESSO O AREA A RISCHIO	PRESIDI DI CONTROLLO ESISTENTI
Controllo e gestione della sicurezza del sistema informatico, in particolare in relazione alla gestione della sicurezza "logica", con particolare riferimento agli accessi ai sistemi della pubblica amministrazione e/o delle Autorità di Vigilanza	Codice etico Sistema informativo Procedura sistema informativo

Gestione dei beni strumentali e delle utilità aziendali (es. autovetture, cellulari, personal computer, carte di credito aziendali, ecc.)	Codice etico
Rilevazione, controllo e rendicontazione del servizio	Codice etico Erogazione servizio SFA Erogazione servizio CSE Procedura fatturazione Procedura conservazione ed archiviazione documenti sull'attività rivolta all'ospite Procedura fatturazione Progettazione e sviluppo Verifiche ispettive interne Comunità alloggio e pronto intervento Interventi educativi SAD
Utilizzo apparecchiature informatiche aziendali	Codice etico

Con riferimento specifico ai delitti in materia di violazione del diritto d'autore, di cui all'art. 25-*novies* del Decreto:

PROCESSO O AREA A RISCHIO	PRESIDI DI CONTROLLO ESISTENTI
Comunicazione commerciale	Codice etico
Controllo e gestione della sicurezza del sistema informatico, in particolare in relazione alla gestione della sicurezza "logica", con particolare riferimento agli accessi ai sistemi della pubblica amministrazione e/o delle Autorità di Vigilanza	Codice etico Sistema informativo Procedura sistema informativo
Rilevazione, controllo e rendicontazione del	Codice etico Erogazione servizio SFA Erogazione servizio CSE

servizio	Procedura fatturazione Procedura conservazione ed archiviazione documenti sull'attività rivolta all'ospite Procedura fatturazione Progettazione e sviluppo Verifiche ispettive interne Comunità alloggio e pronto intervento Interventi educativi SAD
Utilizzo apparecchiature informatiche aziendali	Codice etico

5. COMPITI DELL'ORGANISMO DI VIGILANZA E FLUSSI INFORMATIVI

Fermo restando quanto previsto nella Parte Generale del Modello, e salvo il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, è compito dell'O.d.V.:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei reati di cui agli artt. 24-*bis* e 25-*novies* del Decreto. A tal fine, l'O.d.V. condurrà – avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia – controlli a campione sulle attività connesse ai processi sensibili potenzialmente a rischio dei reati qui in esame, diretti a verificare la corretta esplicazione delle stesse in relazione ai principi ed alle procedure interne in essere;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- vigilare sull'effettiva applicazione del Modello e rilevare le violazioni comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e nomine in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

Allo scopo di svolgere i propri compiti, all'O.d.V. viene garantito libero accesso a tutta la documentazione aziendale rilevante e a tutte le sedi rilevanti per lo svolgimento dei propri compiti.
Ove l'Organismo di Vigilanza nominato dovesse difettare della idonea competenza tecnica, il medesimo, nell'ambito del proprio potere discrezionale ed autonomia di spese si avvarrà dei più accreditati professionisti del settore.

La Società garantisce, inoltre, a favore dello stesso Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio delle criticità, nonché notizie di eventuali problematiche accertate o presunte. Nell'espletamento delle attività di cui sopra, l'O.d.V. può avvalersi di tutte le risorse competenti della Società. A tale scopo, l'O.d.V. viene informato semestralmente dalle funzioni aziendali interessate (tramite apposite relazioni) in merito alla conduzione delle attività della Società nelle aree sensibili e, immediatamente, in caso di commissione di reati o di condotte potenzialmente idonee al integrare le fattispecie di reato rilevanti ai fini della presente Parte Speciale, nonché nell'ipotesi di:

- violazioni, accertate o sospette, del Modello o delle procedure ad esso correlate o degli elementi che lo compongono;
- condotte e/o pratiche non in linea con le disposizioni del Codice Etico adottato dalla Società.

La funzione preposta deve dare immediata comunicazione all'Organismo di Vigilanza di ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione ed ogni anomalia significativa riscontrata.
A sua volta, l'Organismo di Vigilanza deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati contro la pubblica Amministrazione, al Consiglio di Amministrazione, secondo i termini indicati nella Parte Generale del Modello e nel Regolamento di cui l'Organismo di Vigilanza vorrà dotarsi.