

Modello di Organizzazione  
Gestione e Controllo

**World International School s.r.l. a socio unico**  
**(in forma abbreviata “WINS SRL”)**  
approvato dall’organo amministrativo in data 1 settembre 2017

D.lgs. 231/2001  
approvato dall’organo amministrativo in data 1 settembre 2017





## PARTE GENERALE



## Indice

Indice .....	3
1.0 PREMESSE.....	6
1.1 Il quadro normativo .....	6
1.2 Il reato presupposto e i termini di applicabilità del Decreto.....	8
1.3 Le Sanzioni .....	8
1.4 Condotte Esimenti.....	10
1.5 Linee Guida .....	11
1.6 Definizioni.....	12
2. LA WORLD INTERNATIONAL SCHOOL SRL .....	13
2.1 Storia ed attività .....	13
2.2 Oggetto sociale .....	13
3.0 IL MODELLO.....	13
3.1 Finalità del Modello .....	13
3.2 Destinatari del Modello.....	14
3.3 Struttura del Modello .....	14
3.4 Diffusione del Modello .....	15
3.5 Adozione, modifiche e integrazioni del Modello .....	16
4. ORGANISMO DI VIGILANZA.....	17
4.1 Caratteristiche.....	17
4.2 Funzionamento durata e cessazione .....	17
4.3. Funzioni, compiti e poteri.....	19
4.4. Flussi informativi .....	20
4.4.1 Informazioni verso l'O.d.V. ....	20
4.4.2. Informazioni dall'O.d.V. ....	21
5. SISTEMA SANZIONATORIO.....	22
PARTE SPECIALE.....	24
Premessa .....	25
SEZIONE A.....	30
1. Delitti nei rapporti con la Pubblica Amministrazione .....	30
1.2 Le fattispecie rilevanti (ex artt. 24, 25, 25-bis D.lgs. 231/2001).....	30
1.3 Reati di tipo corruttivo .....	30
1.4 La concussione .....	33

1.5 Le ipotesi di truffa.....	34
2. Identificazione delle aree e attività sensibili nei reati interessati con la P.A.....	35
3. Gestione dei rapporti con la PA con compiti di controllo e vigilanza .....	37
4. Principi di controllo .....	38
5. Principi di condotta.....	38
6. Sistema di controllo.....	41
SEZIONE “B” .....	42
1. Delitti informatici e trattamento illecito dei dati. Privacy (cd. Cybercrime) .....	42
1.1 Le fattispecie rilevanti (ex art. 24-bis, D.lgs. n. 231/2001) .....	42
1.2 Falsità in un documento informatico pubblico o con efficacia probatoria. Documenti informatici (ex art. 491-bis c.p.).....	42
1.3 Accesso abusivo ad un sistema informatico/telematico (ex art. 615-ter c.p.).....	43
1.4 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (ex art. 615-quater c.p.) .....	45
1.5 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (ex art. 615-quinquies c.p.) .....	45
1.6 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (ex art. 617 quater c.p.).....	46
1.7 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (ex art. 617-quinquies c.p.).....	47
1.8 Danneggiamento di informazioni, dati e programmi informatici (ex art. 635-bis c.p.)	47
1.9 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (ex art. 635-ter c.p.).....	48
1.10 Danneggiamento di sistemi informatici o telematici (ex art. 635-quater c.p.) .....	49
1.11 Danneggiamento di sistemi informatici o telematici di pubblica utilità (ex art. 635-quinquies c.p.).....	49
2. Le “attività sensibili” in relazione ai delitti informatici. Privacy e Cybercrime .....	49
SEZIONE “C” .....	54
1. Reati societari.....	54
1.1 Le fattispecie rilevanti (ex art. 25-ter, D.lgs. n. 231/2001).....	54
1.2 False comunicazioni sociali e le false comunicazioni sociali in danno della Società, dei soci o dei creditori (ex art. 2621 e 2622 c.c.).....	54
1.3 Impedito controllo (ex art. 2625 c.c.).....	54
2. Attività sensibili e sistema di controlli.....	54
SEZIONE “D” .....	56
1. Delitti contro la personalità individuale. ....	56

1.1 Le fattispecie rilevanti (ex art. 25-quinquies, D.lgs. n. 231/2001).....	56
1.2 I reati contro la personalità individuale.....	56
1.2.1 Prostituzione minorile (ex art. 600-bis c.p.) .....	56
1.2.2 Pornografia minorile (ex art. 600-ter c.p.).....	56
1.2.3 Detenzione di materiale pornografico (ex art. 600-quater c.p.) .....	57
1.2.4 Pornografia virtuale (ex art. 600-quater c.p.).....	57
1.2.5 Iniziative turistiche volte allo sfruttamento della prostituzione minorile (ex art. 600-quinquies c.p.) .....	58
2. Attività sensibili e sistema di controllo .....	58
SEZIONE “E” .....	59
1.1 Le fattispecie rilevanti e i criteri di imputazione (ex art. 25-septies, D.lgs. 231/2001) ..	59
1.1.2 Omicidio colposo (ex art. 589 c.p.).....	59
1.1.3 Lesioni personali colpose (ex art. 590 c.p.) .....	59
2. Attività sensibili e sistema di controllo.....	60
SEZIONE “F”.....	63
1.1 Delitti in materia ricettazione, riciclaggio ed autoriciclaggio.....	63
1.2 Le fattispecie rilevanti e i criteri di imputazione (ex art. 25-octies, D.lgs. 231/2001)..	63
1.2.1 Ricettazione – Art. 648 c.p. ....	63
1.2.2 Riciclaggio – Art. 648-bis c.p.....	64
1.2.3 Impiego di denaro, beni o utilità di provenienza illecita – Art. 648-ter c.p. ....	65
1.2.3 Autoriciclaggio – Art. 648-ter.1 c.p.....	66
SEZIONE “G”.....	68
1. Delitti in materia di violazione del diritto d’autore.....	68
1.1 Le fattispecie rilevanti e i criteri di imputazione (ex art. 25-novies, D.lgs. 231/2001). ..	68
1.1.1 Art. 171 co. I lett. a bis) e co. III .....	68
1.1.2 Art. 171-bis .....	70
1.1.3 Art. 171-ter .....	70
1.1.4 Art. 171-septies .....	73
1.1.5 Art. 171-octies.....	74
2. Miscellanee Scuola - Diritto d’autore.....	75

## 1.0 PREMESSE

Il presente documento ha lo scopo di descrivere il modello di organizzazione, gestione e controllo *ex D.lgs. 231/2001* (nel seguito anche indicato in forma breve come "**Modello**" o come "**Modello Organizzativo**") della Società World International School s.r.l. a socio unico, in forma abbreviata WINS SRL (nel seguito anche indicata come la "**Scuola**", "**Società**" o "**WINS**").

Il Modello, di seguito descritto, rappresenta una parte del più ampio sistema di gestione della WINS, il quale stabilisce e norma:

- i) il modello di governo societario della Scuola;
- ii) i processi operativi ed il sistema di controllo interno, finalizzato a garantire il raggiungimento degli obiettivi di efficacia/efficienza delle attività operative, affidabilità delle informazioni di bilancio, conformità alle leggi ed ai regolamenti obbligatori, prevenendo i rischi correlati agli stessi obiettivi.

La presente descrizione del Modello Organizzativo *ex D.lgs. 231/2001* fa riferimento al sopra citato sistema di gestione di WINS, per tutta la normativa di dettaglio che costituisce la regolamentazione interna in vigore, applicabile e finalizzata ad attuare concretamente tutte le misure di prevenzione e di controllo indicate dal Modello stesso.

Il documento si compone di:

- (i) una **Parte Generale**, contenente gli obiettivi, la struttura, gli elementi e le modalità di gestione del Modello Organizzativo; e
- (ii) una **Parte Speciale**, che riporta, per ciascuna categoria di reati applicabili *ex D.lgs. 231/2001*, gli esiti dell'analisi dei rischi rilevanti ai fini dell'adeguamento strutturale del Modello (aree/attività sensibili, situazioni di rischio), integrandoli per le finalità del Modello stesso con i criteri di condotta e con i protocolli stabiliti per la prevenzione dei reati presi in considerazione.

### 1.1 Il quadro normativo

In generale, il *D.lgs. 231/2001* (nel seguito anche il "**Decreto**") rappresenta il riferimento normativo per l'adozione del Modello Organizzativo, avendo lo stesso introdotto e disciplinato la responsabilità amministrativa delle persone giuridiche (come da rubrica della norma "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni*").

*anche prive di personalità giuridica, a norma dell'art. 11 della Legge 29 settembre 2000, n. 300*"), conseguente alla commissione di specifici reati previsti nel Decreto stesso.

Quest'ultimo provvedimento è ricompreso in una serie di misure internazionali, finalizzate a contrastare i reati nelle operazioni economiche ed è frutto del recepimento delle indicazioni emanate a livello europeo in materia di corruzione nel commercio internazionale e contro la frode ai danni della Comunità Europea, con estensione anche ad altre fattispecie. Più in generale, il Decreto si colloca in un'ottica di prevenzione di reati commessi all'interno delle imprese e degli enti.

Il Decreto tratta di reati (consumati o tentati) commessi, in Italia o all'estero<sup>1</sup>, da parte di soggetti funzionalmente legati alla Società nell'interesse o a vantaggio di essa. L'inosservanza della disciplina contenuta nel Decreto, può comportare per WINS sanzioni (pecuniarie e/o interdittive) che possono incidere fortemente anche sull'esercizio della propria attività. La responsabilità di WINS non sostituisce ma si aggiunge alla responsabilità personale dell'individuo che ha commesso il reato.

WINS risponde per la commissione o la tentata commissione di taluni reati da parte di soggetti ad essi funzionalmente legati.

I soggetti che, commettendo un reato nell'interesse o a vantaggio della Società, possono determinarne la responsabilità sono:

- i) **gli Apicali;**
- ii) **i Subordinati.**

Resta fermo che, ai sensi dell'art. 5 comma secondo del detto Decreto, la Società non risponde, se i predetti soggetti hanno agito nell'interesse esclusivo proprio o di terzi.

In ogni caso, il comportamento dei soggetti menzionati, deve essere riferibile a quel rapporto "organico" per il quale gli atti della persona fisica possono essere imputati alla Società.

---

<sup>1</sup> I reati commessi all'estero sono perseguibili a condizione che: a) lo Stato del luogo in cui è stato commesso il reato non proceda già nei confronti dell'ente; b) l'ente abbia la propria sede principale nel territorio dello Stato italiano; c) il reato sia stato commesso all'estero da un soggetto apicale o subordinato ai sensi dell'art. 5 comma 1, D.lgs. 231/01; d) sussistano le condizioni di procedibilità previste dagli artt. 7, 8, 9, 10 del Codice Penale.

## 1.2 Il reato presupposto e i termini di applicabilità del Decreto

L'ente può essere chiamato a rispondere solo in relazione a determinati reati (c.d. reato presupposto), individuati dal Decreto, nonché dalle leggi che espressamente richiamano la disciplina del Decreto.

Pertanto, in sintesi, la responsabilità dell'ente presuppone:

- la commissione (consumazione o tentativo) di uno dei reati presupposti;
- che il reato presupposto sia stato commesso da parte di un soggetto funzionalmente legato all'ente (Apicali o Subordinati);
- che il reato sia stato commesso nell'interesse o a vantaggio dell'ente (o meglio che esso non sia stato commesso nell'interesse esclusivo dell'autore del reato presupposto o di terzi).

## 1.3 Le Sanzioni

Sotto il profilo sanzionatorio, occorre considerare che le sanzioni sono irrogate dal giudice penale ancorché vengano qualificate come sanzioni amministrative e possono consistere in:

- a) **sanzione pecuniaria**: si tratta di una sanzione necessaria, ovvero l'effetto negativo della violazione del contenuto precettivo delle norme, la quale consegue sempre come effetto del riconoscimento della responsabilità dell'ente<sup>2</sup>;

---

<sup>2</sup> Il Legislatore ha adottato un criterio innovativo di commisurazione della sanzione, sulla base di "quote" che devono essere determinate dal Giudice. Ha, infatti, affidato al Giudice l'obbligo di procedere a due diverse e successive operazioni di apprezzamento, allo scopo di assicurare al sistema sanzionatorio caratteristiche di massimo adeguamento alla gravità del fatto ed alle condizioni economiche dell'Ente.

Il Giudice deve, in primo luogo, determinare il numero delle quote (in ogni caso non inferiore a cento, né superiore a mille) tenendo conto: 1) della gravità del fatto; 2) del grado di responsabilità dell'Ente; 3) dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

In secondo luogo, il Giudice determina, entro i valori minimi e massimi predeterminati in relazione agli illeciti sanzionati, il valore di ciascuna quota, da un minimo di Euro 258,00 ad un massimo di Euro 1.549,00. Tale importo è fissato "sulla base delle condizioni economiche e patrimoniali dell'Ente allo scopo di assicurare l'efficacia della sanzione" (artt. 10 e 11, comma 2, D.lgs. n. 231/2001). Si legge, al punto 5.1. della relazione ministeriale al Decreto: "*Quanto alle modalità di accertamento delle condizioni economiche e patrimoniali dell'ente, il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazione le dimensioni dell'ente e la sua posizione sul mercato. (...) Il giudice non potrà fare a meno di calarsi, con l'ausilio di consulenti, nella realtà dell'impresa, dove potrà attingere anche le informazioni relative allo stato di solidità economica, finanziaria e patrimoniale dell'ente*".

L'art. 12 del Decreto prevede una serie di casi di riduzione della sanzione pecuniaria. Essa infatti viene dimezzata nel caso in cui l'autore del reato presupposto abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne abbia ricavato un vantaggio o ne abbia ricavato un vantaggio minimo o nel caso in cui il danno patrimoniale cagionato è di particolare tenuità. La riduzione oscilla da 1/3 a metà nel caso in cui, prima della dichiarazione di apertura del dibattimento, l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato, ovvero se è stato adottato e reso operativo un Modello idoneo a prevenire la commissione di ulteriori reati. In caso di concorso delle due ipotesi di riduzione, la riduzione è da 1/2 a 2/3.



b) **sanzioni interdittive**: queste, come le altre sanzioni sono sempre aggiuntive rispetto alla sanzione pecuniaria. Si applicano solo per i reati per i quali sono espressamente previste dal Decreto, purché:

- 1) l'ente abbia tratto dal reato un profitto rilevante e il reato sia stato commesso da un soggetto apicale, o da un soggetto subordinato, ma solo qualora la commissione del reato sia stata agevolata da gravi carenze organizzative;
- 2) in caso di reiterazione dei reati (cd. recidiva).

Inoltre, le sanzioni interdittive sono generalmente temporanee e possono essere applicate anche in via cautelare<sup>3</sup>.

Esse consistono in:

- **interdizione dall'esercizio dell'attività**, che ha natura residuale rispetto alle altre sanzioni interdittive;
- **sospensione o revoca delle autorizzazioni, licenze o concessioni** funzionali alla commissione dell'illecito;
- **divieto di contrattare con la Pubblica Amministrazione**, salvo che per ottenere le prestazioni di un pubblico servizio;
- **esclusione da agevolazioni, finanziamenti, contributi o sussidi** e l'eventuale **revoca** di quelli già concessi;
- **divieto di pubblicizzare beni o servizi**;
- **confisca**: viene sempre disposta con la sentenza di condanna con riferimento al prezzo o profitto del reato, anche per equivalente;
- **pubblicazione della sentenza**.

Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni (art. 13 co.2, D.lgs. n. 231/2001) e la scelta della misura da applicare e della sua durata viene

---

<sup>3</sup> L'applicazione in via cautelare delle misure interdittive è subordinata alla seguente triplice condizione: gravi indizi di colpevolezza; pericolo di reiterazione; rilevante entità del profitto tratto dall'Ente in conseguenza dell'illecito. In ogni caso, non si procede all'applicazione delle sanzioni interdittive, quando il reato è stato commesso nel prevalente interesse dell'autore o di terzi e l'Ente ne ha ricavato un vantaggio minimo o nullo, ovvero il danno patrimoniale cagionato è di particolare tenuità.

L'applicazione delle sanzioni interdittive è altresì esclusa dal fatto che l'Ente abbia posto in essere le condotte riparatrici previste dall'articolo 17, D.lgs. n. 231 del 2001 e, più precisamente, quando concorrono le seguenti condizioni:

- "l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso";
- "l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi";
- "l'ente ha messo a disposizione il profitto conseguito ai fini della confisca".

effettuata dal Giudice, sulla base degli stessi criteri validi per la commisurazione della sanzione pecuniaria, “*tenendo conto dell’idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso*” (art. 14, D.lgs. n. 231 del 2001).

#### **1.4 Condotte Esimenti**

La responsabilità dell’ente sussiste se non sono stati adottati o non sono stati rispettati gli *standard* doverosi di sana gestione e di controllo attinenti alla sua organizzazione e allo svolgimento della sua attività. La responsabilità dell’ente, la rilevanza della sua condotta, dipende dall’accertamento di una politica di impresa in cui si rilevano carenze strutturali nell’organizzazione aziendale che non abbiano prevenuto la commissione di uno dei reati presupposto.

Il Decreto esclude, infatti, la responsabilità dell’ente, nel caso in cui, prima della commissione del reato, lo stesso si sia dotato e abbia efficacemente attuato un Modello, idoneo a prevenire la commissione di reati della specie di quello che è stato consumato.

Il Modello opera quale esimente, sia che il reato presupposto sia stato commesso da un soggetto Apicale sia che sia stato commesso da un soggetto Subordinato.

Tuttavia, per i reati commessi dagli Apicali, il Decreto introduce una sorta di presunzione di responsabilità dell’ente, dal momento che si prevede l’esclusione della sua responsabilità, solo se l’ente dimostra che:

- a) l’organo amministrativo ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della stessa specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l’osservanza del Modello e di curare il loro aggiornamento è stato affidato ad un organismo dell’ente dotato di autonomi poteri di iniziativa e di controllo (cd. “**Organismo di Vigilanza**”, di seguito per brevità “**O.d.V.**”);
- c) il reato è stato commesso eludendo fraudolentemente il Modello;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell’O.d.V.

Per i reati commessi dai Subordinati, l’ente risponde, invece, solo se venga provato che “*la commissione del reato è stata resa possibile dall’inosservanza degli obblighi di direzione o vigilanza*” che gravano tipicamente sul vertice aziendale.

Anche in questo caso, comunque, l’adozione e l’efficace attuazione del Modello, prima della commissione del reato, esclude l’inosservanza degli obblighi di direzione o vigilanza ed esonera l’ente da responsabilità.

L'adozione e l'efficace attuazione del Modello, pur non costituendo un obbligo giuridico, è quindi l'unico strumento a disposizione dell'ente per dimostrare la propria estraneità ai fatti di reato e, in definitiva, per andare esente dalla responsabilità stabilita dal Decreto.

Il Modello opera, pertanto, quale esimente della responsabilità dell'ente, solo se idoneo al prevenire i reati e solo se efficacemente attuato.

Il Decreto, tuttavia, non indica analiticamente le caratteristiche e i contenuti del Modello, ma si limita a dettare alcuni principi di ordine generale ed alcuni elementi essenziali di contenuto. In generale - secondo il Decreto - il Modello deve prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge ed a rilevare nonché ad eliminare tempestivamente situazioni di rischio di commissione di specifici reati.

In particolare, il Modello deve:

- i) individuare le attività nel cui ambito possono essere commessi reati (c.d. attività sensibili);
- ii) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente, in relazione ai reati da prevenire;
- iii) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- iv) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- v) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Con riferimento all'efficace attuazione del Modello, il Decreto prevede inoltre la necessità della verifica periodica e dell'aggiornamento/modifica dello stesso, qualora siano scoperte significative violazioni delle prescrizioni ovvero qualora intervengano mutamenti nell'organizzazione o nell'attività dell'ente.

## **1.5 Linee Guida**

Il D.lgs. 231/2001 prevede espressamente che il Modello possa ispirarsi a codici di comportamento redatti da associazioni rappresentative di categoria la cui idoneità sia approvata dal Ministero della Giustizia.

Il presente Modello è, pertanto, ispirato alle Linee Guida per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.lgs. 231/2001. In particolare esso la redazione di esso è ispirata alle Linee Guida emanate da Confindustria.

Eventuali divergenze rispetto a punti specifici delle Linee Guida, dipendono dall'esigenza di adeguare le misure organizzative e gestionali all'attività concretamente svolta dalla Società ed al contesto nel quale essa opera.

## 1.6 Definizioni

Nel testo, per semplicità espositiva, sono utilizzati termini specifici i quali intendono delineare concetti complessi o comunque riferiti a definizioni normative date dal D.lgs. 231/2001 e successive modificazioni.

Nell'elenco che segue sono enunciate le relative definizioni: i termini definitivi sono riportati con maiuscola iniziale nel testo del documento:

- a) **Apicali:** persone fisiche che rivestono posizioni di vertice (rappresentanza, amministrazione o direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale o persone che esercitano, di fatto, la gestione ed il controllo) e destinatarie del Modello, ex art. 6 del Decreto;
- b) **Aree di Rischio:** le aree operative della società oggetto di mappatura e ritenute a rischio commissione Reato;
- c) **Codice:** il Codice Disciplinare adottato ex art. 6 comma 2 lett. e) Decreto;
- d) **Codice Etico:** il Codice Etico adottato dalla Società;
- e) **Decreto:** il D.lgs. n. 231/2001 nel testo vigente, comprensivo di ogni successiva modificazione e integrazione;
- f) **Destinatari:** tutti coloro a cui il Codice si rivolge e che sono tenuti al suo rispetto;
- g) **Linee Guida:** le linee guida di elaborazione del Modello adottate da Confindustria, nella versione vigente;
- h) **Modello:** il modello di organizzazione Gestione e Controllo come definito nell'art. 6 comma 1 lett. a) del Decreto;
- i) **Reato:** ogni reato-presupposto individuato dal Decreto, la cui commissione comporta, salvo le esimenti previste nel decreto stesso, responsabilità amministrativa e l'applicazione delle relative sanzioni;
- j) **Sanzioni:** le sanzioni disciplinari previste dal Codice;
- k) **Società, Scuola o WINS:** la società World International School s.r.l. a socio unico o, in forma abbreviata WINS S.r.l.;

- l) **Terzi:** persone che intrattengono con la Società rapporti di collaborazione senza vincolo di subordinazione (a titolo esemplificativo e non esaustivo: rapporti di consulenza, rapporti di agenzia, rapporti di rappresentanza commerciale e altri rapporti che si concretizzano in una prestazione professionale, non a carattere subordinato, sia continuativa sia occasionale ivi inclusi i soggetti che agiscono per i fornitori e i partners, anche sotto forma di associazione temporanea di imprese, nonché *joint-venture*);
- m) **O.d.V.:** l'Organismo di Vigilanza definito dall'art. 6 comma 1 lett. b) del Decreto.

## **2. LA WORLD INTERNATIONAL SCHOOL SRL**

### **2.1 Storia ed attività**

A tal riguardo si rimanda al paragrafo intitolato "Chi siamo" del Codice Etico.

### **2.2 Oggetto sociale**

A tal riguardo si rimanda al paragrafo intitolato "Chi siamo" del Codice Etico.

## **3.0 IL MODELLO**

Il Modello è elaborato ispirandosi ai principi contenuti nel Codice Etico e sulla base delle disposizioni contenute negli artt. 6 e 7 del Decreto.

### **3.1 Finalità del Modello**

L'obiettivo del Modello è definire un sistema strutturato e organico di protocolli gestionali e di controllo, per la prevenzione della commissione dei fatti costituenti reato.

Più in generale, il Modello, in esito alla definizione delle aree di rischio nell'attività aziendale, si propone le seguenti finalità:

- a) sensibilizzare tutti i destinatari a tenere comportamenti corretti e trasparenti;
- b) determinare la vigenza di un sistema di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale;
- c) rendere tutti coloro che operano in nome e per conto di WINS, ed in particolare quelli impegnati nelle "aree di attività a rischio", consapevoli di poter incorrere, in caso di violazione delle disposizioni in esso riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti della WINS;

- d) informare tutti coloro che operano con WINS che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni e anche la risoluzione del rapporto contrattuale;
- e) confermare che WINS non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità e che, in ogni caso, tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi cui è ispirata l'attività imprenditoriale della WINS.

### 3.2 Destinatari del Modello

Destinatari del Modello sono i soggetti Apicali e Subordinati come già definiti: in primo luogo a tutti gli Amministratori, dirigenti e collaboratori interni, con particolare riferimento a quelli impiegati nelle attività soggette a rischio.

Le disposizioni sono indirizzate sia ai soggetti interni alla Società che ai soggetti esterni purché operanti con WINS nell'ambito di rapporti giuridici ed economici di qualsiasi natura e specie.

### 3.3 Struttura del Modello

Per Modello deve intendersi una pluralità di documenti tutti costituenti il sistema di gestione e controllo della Società, esimente ai sensi del D.lgs. 231/2001.

Il Modello si compone di:

- a) una “**Parte Generale**”, che contiene i principi cardine dello stesso;
- b) un “**Codice Etico**” adottato da WINS;
- c) un “**Sistema Disciplinare**” trasposto nel Codice;
- d) un “**Sistema di deleghe e procure**”, nonché tutti i documenti aventi l'obiettivo di descrivere e attribuire responsabilità e/o mansioni a chi opera all'interno della WINS nelle cd. Aree a “Rischio Reato” (i.e. organigrammi, ordini di servizio, *job description*, mansionari, funzionigramma, etc.);
- e) un “**Sistema di Controllo Interno**” costituito dall'insieme degli “strumenti” volti a fornire una ragionevole garanzia in ordine al raggiungimento degli obiettivi di efficienza e di efficacia operativa, affidabilità delle informazioni finanziarie e gestionali, rispetto delle leggi e dei regolamenti, nonché salvaguardia del patrimonio sociale, anche contro possibili frodi.
- f) da una “**Parte Speciale**”, sulle diverse categorie di reati previsti dal Decreto e ritenuti rilevanti, con condotte e procedure atte a prevenire la commissione del reato stesso. Per

ciascuna categoria di reati presupposto, ogni sezione prevede una sintetica descrizione degli illeciti che possono costituire fonte di una responsabilità amministrativa della Società, l'indicazione delle Aree a "Rischio Reato" individuate e la descrizione delle principali regole di comportamento implementate dal WINS, cui i Destinatari si devono attenere al fine di prevenire la commissione di tali reati.

### **3.4 Diffusione del Modello**

È obiettivo di WINS garantire una corretta conoscenza da parte dei Destinatari circa il contenuto del Decreto e gli obblighi derivanti dal medesimo affinché essi seguano, nell'espletamento delle proprie attività, comportamenti in linea con i valori etico-sociali cui si ispira WINS.

Ai fini dell'efficace attuazione del presente Modello, la formazione e l'informativa verso i Destinatari è gestita in stretto coordinamento con l'O.d.V. e con i responsabili delle altre funzioni aziendali di volta in volta coinvolte nella applicazione del Modello.

In particolare è prevista:

- a) una **pubblicità generale** mediante pubblicazione dello stesso sul sito web della società.
- b) una **comunicazione iniziale**. A tale proposito, l'adozione del Modello è comunicata a tutte le risorse presenti in Società. Ai nuovi assunti viene consegnato il Codice Etico. Agli stessi, viene inoltre fatto sottoscrivere un modulo con il quale prendono atto che il Modello è disponibile sul sito internet societario e presso la direzione amministrativa e si impegnano ad osservare i contenuti della normativa citata;
- c) una **specificativa attività di formazione**. Tale attività di formazione "continua" è obbligatoria e sviluppata attraverso strumenti e procedure, eventualmente anche informatiche (e-mail di aggiornamento, strumenti di autovalutazione), nonché incontri e seminari di formazione ed aggiornamento periodici. Tale attività è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'aver o meno funzioni di rappresentanza della Società.

WINS prevede altresì la diffusione del Modello ai Terzi attraverso la predisposizione di idonee informative e clausole di conoscenza circa il contenuto del Modello e delle conseguenze sul suo mancato rispetto, da inserirsi all'interno dei testi contrattuali di riferimento.

In ogni caso, le funzioni aziendali competenti assicurano il recepimento nelle procedure della Società, dei principi e delle norme di comportamento contenuti nel Modello e nel Codice Etico.

### **3.5 Adozione, modifiche e integrazioni del Modello**

L'organo amministrativo ha la competenza esclusiva per l'adozione, la modifica e l'integrazione del Modello. A tal fine l'organo amministrativo, conformemente all'art. 6, comma 1, lett. b) e dall'art. 7, comma 4, lett. a) del Decreto, ha l'obbligo di valutare le proposte di modifica formulate dall'O.d.V., e le segnalazioni provenienti da questo circa fatti, circostanze o carenze organizzative riscontrate nell'attività di vigilanza che evidenzino la necessità o l'opportunità di modificare o integrare il Modello.

In ogni caso, il Modello deve essere tempestivamente modificato o integrato dall'organo amministrativo, anche su proposta e comunque previa consultazione dell'O.d.V., quando siano intervenute:

- a) violazioni o elusioni delle prescrizioni del Modello che ne abbiano dimostrato l'inefficacia o l'incoerenza ai fini della prevenzione dei reati;
- b) significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- c) modifiche normative.

Le modifiche, gli aggiornamenti o le integrazioni al Modello devono sempre essere comunicati all'O.d.V. per le opportune verifiche.

Le procedure operative adottate in attuazione del presente Modello sono modificate a cura delle funzioni aziendali competenti, qualora si dimostrino inefficaci ai fini di una corretta attuazione delle disposizioni del Modello. Le funzioni aziendali competenti curano altresì le modifiche o integrazioni alle procedure operative necessarie per dare attuazione alle eventuali revisioni del presente Modello.

L'O.d.V. è tempestivamente informato dell'aggiornamento e dell'implementazione delle nuove procedure operative.



## 4. ORGANISMO DI VIGILANZA

### 4.1 Caratteristiche

L'Organismo di Vigilanza è nominato dall'organo amministrativo con delibera e può essere monocratico o collegiale.

Secondo le disposizioni del Decreto (artt. 6 e 7), nonché le indicazioni contenute nella Linee Guida, le caratteristiche dell'O.d.V., tali da assicurare un'effettiva ed efficace attuazione del Modello, devono essere:

- a) **autonomia ed indipendenza:** tali requisiti sono necessari affinché l'O.d.V. non subisca condizionamenti o interferenze da parte dell'organo dirigente e si possono ottenere garantendo all'O.d.V. la posizione gerarchica più elevata possibile, nonché prevedendo un'attività di reporting all'organo amministrativo;
- b) **professionalità:** l'O.d.V. deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio;
- c) **continuità d'azione:** l'O.d.V. deve svolgere in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine.

I componenti dell'O.d.V. possono essere sia esterni che interni alla Società. I membri dell'O.d.V. non sono soggetti, in tale qualità e nell'ambito dello svolgimento della propria funzione, al potere gerarchico e disciplinare di alcun organo o funzione societaria. I componenti dell'O.d.V. non dovranno essere coinvolti in qualsiasi situazione che possa generare conflitto di interessi con la WINS, fatto salvo l'eventuale pagamento del compenso per l'attività svolta.

Non potranno essere nominati componenti dell'O.d.V. coloro i quali abbiano riportato una condanna, anche non definitiva, per uno dei reati previsti dal Decreto.

Ciascun componente dell'O.d.V. deve possedere un profilo professionale e personale che garantisce l'imparzialità di giudizio, l'autorevolezza e l'eticità della condotta e ispirare i propri comportamenti a irreprensibili valori etici e morali.

L'O.d.V. nel suo complesso deve comprendere adeguate competenze organizzative, giuridiche e di gestione di audit.

### 4.2 Funzionamento durata e cessazione

Una volta insediato, l'O.d.V. provvede a dotarsi di un piano delle attività da svolgere su base annuale. L'O.d.V. resta in carica per la durata indicata nell'atto di nomina e può essere rinnovato.

La cessazione dall'incarico dell'O.d.V. può avvenire per una delle seguenti cause:

- a) scadenza dell'incarico;
- b) revoca da parte dell'organo amministrativo;
- c) rinuncia di un componente, formalizzata mediante apposita comunicazione scritta inviata all'organo amministrativo;
- d) sopraggiungere di una delle cause di decadenza.

La revoca dell'O.d.V. può essere disposta solo per giusta causa e tali devono intendersi, a titolo esemplificativo, le seguenti ipotesi:

- a) coinvolgimento del componente in un processo penale avente ad oggetto la commissione di un delitto;
- b) accertata violazione degli obblighi di riservatezza previsti a carico dell'O.d.V.;
- c) grave negligenza nell'espletamento dei compiti connessi all'incarico;
- d) possibile coinvolgimento della Società in un procedimento, penale o civile, connesso ad un'omessa o insufficiente vigilanza, anche colposa.

La revoca è disposta con delibera dell'organo amministrativo.

In caso di scadenza, revoca o rinuncia, l'organo amministrativo nomina senza indugio il nuovo componente dell'O.d.V., mentre il componente uscente rimane in carica fino alla sua sostituzione.

Costituiscono motivi di ineleggibilità e/o di decadenza del componente dell'O.d.V.:

- a) l'interdizione, l'inabilitazione, il fallimento o, comunque, la condanna penale, anche non passata in giudicato, per uno dei reati previsti dal Decreto o, comunque, ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;
- b) l'esistenza di rapporti di natura patrimoniale tra il componente e WINS tali da compromettere l'indipendenza del componente stesso.

Qualora, nel corso dell'incarico, dovesse sopraggiungere una causa di decadenza, il componente l'O.d.V. è tenuto ad informare immediatamente l'organo amministrativo.

### 4.3. Funzioni, compiti e poteri

La funzione dell'O.d.V. è la seguente:

- a) **vigilare** sull'effettiva applicazione del Modello in relazione alle diverse tipologie di reati presi in considerazione dallo stesso;
- b) **verificare** l'efficacia del Modello e la sua reale capacità di prevenire la commissione dei reati in questione;
- c) **individuare** e proporre all'organo amministrativo aggiornamenti e modifiche del Modello stesso in relazione alla mutata normativa o alle mutate necessità o condizioni aziendali;
- d) **verificare** che le proposte di aggiornamento e modifica formulate dall'organo amministrativo siano state effettivamente recepite nel Modello.

All'O.d.V. sono assegnati i seguenti compiti:

- a) **verificare** l'efficienza e l'efficacia del Modello, anche in termini di rispondenza tra le modalità operative adottate in concreto, gli standard di comportamento e le procedure formalmente previste dal Codice di Comportamento e dal sistema di gestione aziendale;
- b) **presidiare** l'attualità del Modello, formulando, quando necessario, proposte per eventuali aggiornamenti e adeguamenti;
- c) **assicurare** il periodico aggiornamento dell'analisi delle attività sensibili, quando necessario;
- d) **rilevare** gli eventuali scostamenti comportamentali che dovessero emergere dalle attività di verifica, dall'analisi dei flussi informativi e dalle segnalazioni;
- e) **informare** tempestivamente l'organo amministrativo, per gli opportuni provvedimenti, in merito alle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;
- f) **collaborare** alle iniziative per la diffusione della conoscenza e della comprensione dei contenuti del Modello;
- g) **predisporre** un'efficace sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del Decreto, garantendo la tutela e la riservatezza del segnalante;
- h) **referire** periodicamente all'organo amministrativo circa lo stato di attuazione e di operatività del Modello.

Per lo svolgimento dei compiti sopra elencati, all'Organismo è data la possibilità di:

- a) **accedere ad informazioni**, documenti e/o dati, ritenuti necessari per lo svolgimento dei compiti attribuiti, presso qualsiasi struttura aziendale;
- b) **promuovere** l'attivazione di eventuali procedimenti disciplinari e proporre le eventuali sanzioni previste dal sistema disciplinare dell'ente;
- c) **ricorrere** a consulenti esterni nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello 231/2001.

L'organo amministrativo assegna all'O.d.V. le risorse umane e finanziarie ritenute opportune ai fini dello svolgimento dell'incarico assegnato. In particolare, all'O.d.V. sono attribuiti autonomi poteri di spesa, nonché la facoltà di stipulare, modificare e/o risolvere incarichi professionali a soggetti terzi in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico.

#### **4.4. Flussi informativi**

##### **4.4.1 Informazioni verso l'O.d.V.**

L'O.d.V. deve essere informato, mediante apposite segnalazioni da parte dei Destinatari in merito ad eventi che potrebbero comportare la responsabilità della Società ai sensi del Decreto. I flussi informativi verso l'O.d.V. si distinguono in informazioni di carattere generale ed informazioni specifiche obbligatorie.

Con riferimento alle informazioni di tipo generale:

- a) i Destinatari sono tenuti a segnalare all'O.d.V. le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei reati od a pratiche non in linea con le procedure e le norme di comportamento emanate o che verranno emanate da WINS;
- b) i Terzi sono tenuti a segnalare all'O.d.V. le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei reati nei limiti e secondo le modalità previste contrattualmente;

E' fatto obbligo segnalare all'O.d.V. le informazioni concernenti:

- a) i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, inerenti lo svolgimento di indagini che vedano coinvolta la WINS od i componenti degli organi sociali;

- b) i rapporti eventualmente predisposti dai responsabili di altri organi nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza del Decreto;
- c) le notizie relative a procedimenti disciplinari nonché ad eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di reati o violazione delle regole di comportamento o procedurali del Modello;
- d) le commissioni di inchiesta o relazioni/comunicazioni interne da cui emerga la responsabilità per le ipotesi di reato di cui al Decreto;
- e) i cambiamenti organizzativi;
- f) gli aggiornamenti del sistema delle deleghe e dei poteri;
- g) le operazioni significativamente svolte nell'ambito delle Aree a "Rischio Reato";
- h) i mutamenti nelle Aree a "Rischio Reato" o potenzialmente a rischio;
- i) le eventuali comunicazioni in merito ad aspetti che possono indicare carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società;
- j) la dichiarazione di veridicità e completezza delle informazioni contenute nelle comunicazioni sociali;
- k) la copia dei verbali delle riunioni dell'organo amministrativo.

La Società adotta specifici canali informativi dedicati (mail box create *ad hoc* o altri canali in caso di necessità) al fine di garantire la riservatezza di cui sopra e facilitare il flusso di segnalazioni ed informazioni verso l'O.d.V.

Quest'ultimo organo, valuta le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine può ascoltare l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere. In ogni caso, i segnalanti in buona fede saranno garantiti da qualsiasi forma di ritorsione o penalizzazione e ad essi sarà assicurata la massima riservatezza, fatti salvi gli obblighi di legge e le esigenze di tutela di WINS o delle persone accusate erroneamente o in malafede.

#### **4.4.2. Informazioni dall'O.d.V.**

Mentre spetta all'organo amministrativo la responsabilità di adottare ed efficacemente implementare il Modello, l'O.d.V. riferisce in merito all'attuazione del Modello e al verificarsi di eventuali criticità.

In particolare, l'O.d.V. ha la responsabilità nei confronti dell'organo amministrativo di:

- comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere al fine di adempiere ai compiti assegnati;
- comunicare periodicamente lo stato di avanzamento del programma unitamente alle eventuali modifiche apportate allo stesso;
- comunicare tempestivamente eventuali problematiche connesse alle attività, laddove rilevanti;
- relazionare, con cadenza almeno annuale, in merito all'attuazione del Modello.
- comunicare le informazioni ricevute circa la violazione del Modello, al fine dell'esercizio del potere disciplinare.

Gli incontri in cui l'O.d.V. riferisce devono essere sempre verbalizzati. Copia di tali verbali sarà custodita dall'O.d.V. e dagli organi di volta in volta coinvolti.

Fermo restando quanto sopra, l'O.d.V. potrà, inoltre, comunicare, valutando le singole circostanze:

- (i) i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'O.d.V. ottenga dai responsabili dei processi un piano delle azioni, con relativa tempistica, per l'implementazione delle attività suscettibili di miglioramento nonché il risultato di tale implementazione;
- (ii) comportamenti/azioni non in linea con il Modello al fine di:
  - a) acquisire dall'organo amministrativo tutti gli elementi per effettuare eventuali comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
  - b) dare indicazioni per la rimozione delle carenze onde evitare il ripetersi dell'accadimento.

## **5. SISTEMA SANZIONATORIO**

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle norme contenute nel Modello, è necessaria essenziale per assicurare l'effettività del Modello stesso. L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dalla Società in piena autonomia ed indipendentemente dalla tipologia di reati che le violazioni possano determinare.



La Società ha, pertanto, adottato un Codice che costituisce parte integrante del Modello e che dettaglia le sanzioni previste, le loro modalità di irrogazione e gradua la gravità delle condotte. All' O.d.V. è demandato il compito di verificare e valutare l'idoneità del sistema disciplinare alla luce del Decreto. L'O.d.V. deve, altresì, puntualmente indicare, nella propria relazione semestrale periodica le possibili aree di miglioramento e sviluppo, soprattutto alla luce degli sviluppi della normativa in materia.



## PARTE SPECIALE





## Premessa

La presente “**Parte Speciale**”, nelle sue articolazioni, riguarda l’applicazione nel dettaglio dei principi richiamati nella “**Parte Generale**” con riferimento ai Reati, che WINS ha stabilito di prendere in considerazione in ragione delle caratteristiche della propria attività.

In ragione del numero significativo di fattispecie di reato, che attualmente costituiscono presupposto della responsabilità amministrativa degli Enti ai sensi del Decreto, talune di esse non sono state ritenute rilevanti ai fini della costruzione del presente Modello, in quanto si è reputato che il rischio relativo alla commissione di tali reati fosse solo astrattamente e non concretamente ipotizzabile.

In particolare, a seguito di un’attenta valutazione dell’attività in concreto svolta da WINS, sono state escluse dall’analisi di rilevanza dei reati le seguenti fattispecie:

1. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (*ex art. 24, D.lgs. n. 231/2001*);
2. Delitti di criminalità organizzata (*ex art. 24-ter, D.lgs. n. 231/2001*)<sup>4</sup>;
3. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (*ex art. 25-bis, D.lgs. n. 231/2001*)<sup>5</sup>;
4. Delitti contro l’industria ed il commercio (*ex art. 25-bis 1, D.lgs. n. 231/2001*)<sup>6</sup>;
5. Reati con finalità di terrorismo o di eversione dell’ordine democratico previsti dal codice penale e dalle leggi speciali (*ex art. 25-quater, D.lgs. n. 231/2001*)<sup>7</sup>;
6. Pratiche di mutilazione degli organi genitali femminili (*ex art. 25-quater1, D.lgs. 231/2001*)<sup>8</sup>;
7. Reati di abuso di mercato (*ex art. 25-sexies, D.lgs. n. 231/2001*)<sup>9</sup>;
8. Reati ambientali (*ex art. 25-undecies, D.lgs. n. 231/2001*)<sup>10</sup>;
9. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (*ex art. 25-duodecies, D.lgs. n. 231/2001*)<sup>11</sup>;
10. Reati transnazionali (L. n. 146/2006).

---

<sup>4</sup> Articolo inserito dall’art. 2, co. 28, della L. 94/2009.

<sup>5</sup> Articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001, poi modificato dalla L. n. 99/2009.

<sup>6</sup> Articolo aggiunto dall’art. 17, co. 7, lett. b), dalla L. 99/2009.

<sup>7</sup> Articolo aggiunto dalla L. n. 7/2003.

<sup>8</sup> Articolo inserito dall’articolo 3 della legge 9 gennaio 2006, n. 7.

<sup>9</sup> Articolo aggiunto dalla L. n. 62/2005.

<sup>10</sup> Articolo inserito dall’art. 2, co. 2, del D. Lgs. n. 121/2001.

<sup>11</sup> Articolo aggiunto dal D.lgs. n. 109/2012.

Qualora dovessero emergere condizioni tali da giustificare una valutazione differente, la stessa WINS procederà alla conseguente revisione del Modello, secondo le disposizioni del Decreto. In ogni caso, i principi etici su cui si fonda il Modello e la sua struttura di *governance* sono finalizzati a prevenire in linea generale anche quelle fattispecie di reato che non sono state valutate come a rischio. L'adozione del Modello quale strumento capace di orientare il comportamento dei soggetti che operano all'interno della Società e di promuovere a tutti i livelli aziendali comportamenti improntati a legalità e correttezza si riverbera positivamente sulla prevenzione di qualsiasi reato o illecito previsto dall'ordinamento.

La “**Parte Speciale**” è suddivisa in Sezioni, come di seguito, in cui in ciascuna di esse sono analizzati rispettivamente:

- A. **Sezione “A”** - Delitti nei rapporti con la Pubblica Amministrazione (*ex art. 24 e 25, 25-bis D.lgs. 231/2001*);
- B. **Sezione “B”** - Delitti informatici e trattamento illecito dei dati (*ex art. 24-bis, D.lgs. n. 231/2001*)<sup>12</sup>, con violazione della Privacy (cd. *Cybercrime*);
- C. **Sezione “C”** - Reati societari (*ex art. 25-ter, D.lgs. n. 231/2001*);
- D. **Sezione “D”** - Delitti contro la personalità individuale (*ex art. 25-quinquies, D.lgs. n. 231/2001*)<sup>13</sup>;
- E. **Sezione “E”** - Delitti con violazione delle norme poste a tutela della salute e sicurezza nei luoghi di lavoro (*ex 25-septies, D.lgs. 231/2001*);
- F. **Sezione “F”** – Delitti in materia ricettazione, riciclaggio ed autoriciclaggio (*ex art. 25-octies e 25-ter, D.lgs. 231/2001*);
- G. **Sezione “G”** - Delitti in materia di violazione del diritto d'autore (*ex art. 25-novies, D.lgs. n. 231/2001*)<sup>14</sup>.

Ciascuna “Sezione” della “Parte Speciale” contiene la descrizione delle fattispecie rilevanti, l'identificazione delle aree e delle attività a rischio della WINS (di seguito anche “**attività sensibili**”), alla luce dell'attività di analisi dei rischi, svolta in conformità a quanto prescritto dall'art. 6, co. 2 lettera a) del Decreto, che ha consentito di individuare le strutture aziendali coinvolte in processi astrattamente esposti al rischio di commissione di fatti rilevanti ai sensi del Decreto e contiene i principi di comportamento e di attuazione dei processi decisionali.

---

<sup>12</sup> Articolo aggiunto dalla L. n. 48/2008.

<sup>13</sup> Articolo aggiunto dalla L. n. 228/2003.

<sup>14</sup> Articolo aggiunto dalla L. n. 99/2009.

Ciascuna Sezione deve essere correlata ai principi comportamentali contenuti nelle procedure interne di WINS, nel Codice Etico e nel Codice Disciplinare, che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive della WINS.

Gli strumenti di controllo di seguito individuati sono vincolanti per i destinatari del Modello e si sostanziano in obblighi di *facere* (il rispetto delle procedure, le segnalazioni agli organismi di controllo) e in obblighi di *non facere* (il rispetto dei divieti), di cui pure viene data espressa contezza.

Il rispetto di tali obblighi, come già dichiarato nella “**Parte Generale**” e come qui si intende riaffermare, ha una precisa valenza giuridica; in caso di violazione di tali obblighi, infatti, la WINS reagirà applicando il sistema disciplinare e sanzionatorio da essa previsto, in conformità al D.lgs. 231/2001.

Nello specifico, la “**Parte Speciale**” del Modello ha lo scopo di:

- indicare le procedure che i membri degli organi sociali, i dipendenti, i collaboratori esterni sono chiamati a osservare ai fini della corretta applicazione del Modello, per la prevenzione degli illeciti;
- fornire all’O.d.V. ed ai responsabili delle altre funzioni della Società, che cooperano con lo stesso organo di controllo, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

In linea generale, si dovranno adottare, ciascuno per gli aspetti di propria competenza e per il ruolo ricoperto, comportamenti conformi al contenuto dei seguenti documenti:

- Modello;
- Codice Etico;
- Codice Disciplinare;
- Linee guida/procedure/regolamenti;
- Procure, deleghe e disposizioni organizzative;
- ogni altro documento che verrà comunicato fare parte integrante del sistema di gestione e controllo.

E’ inoltre, espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge, oltre che alle fonti precedentemente menzionate.

Il sistema dei controlli, perfezionato da WINS, anche sulla base delle indicazioni fornite dalle Linee guida di Confindustria, prevede:

- standard di controllo “**generali**”, applicabili a tutte le attività sensibili;
- standard di controllo “**specifici**”, applicabili a determinate attività sensibili e riportati nelle singole Parti Speciali

Gli *standard di controllo generale* da considerare e applicare con riferimento a tutte le attività sensibili sono i seguenti:

- **poteri autorizzativi e di firma**

I poteri autorizzativi e di firma devono: (a) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l’indicazione delle soglie di approvazione delle spese; (b) essere chiaramente definiti e conosciuti all’interno della Società;

- **tracciabilità e segregazione**

Ogni operazione relativa all’attività sensibile deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento dell’attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali e, in ogni caso, deve essere previsto espressamente il divieto di cancellare o distruggere le registrazioni effettuate ovvero, a seconda dei casi, deve essere disciplinata in dettaglio la possibilità di cancellare o distruggere dette registrazioni. WINS si impegna affinché non vi sia identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

- **remissione all’organo amministrativo delle questioni controverse**

Ogni questione controversa deve essere portata all’attenzione dell’organo amministrativo. Sulla base degli standard di controllo generali sopra riportati, gli *standard di controllo specifici*, che ai primi fanno riferimento, sono elaborati affinché:

- tutte le operazioni, la formazione e l’attuazione delle decisioni di WINS rispondano ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell’atto costitutivo, del Codice Etico, del Codice Disciplinare e delle procedure aziendali;
- siano definite e adeguatamente comunicate le disposizioni societarie, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- tutte le operazioni:

- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno di WINS;
- siano sempre documentabili e ricostruibili le fasi di formazione degli atti e i livelli autorizzativi di formazione degli atti, a garanzia della trasparenza delle scelte effettuate;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti operazioni economiche;
- l'accesso e l'intervento sui dati della Società sia consentito esclusivamente alle persone autorizzate, in conformità al D.lgs. 196/2003 (Codice della Privacy) e successive modifiche o integrazioni, anche regolamentari;
- sia garantita la riservatezza nella trasmissione delle informazioni;
- i documenti riguardanti la formazione delle decisioni e l'attuazione delle stesse siano archiviati e conservati, a cura della funzione competente.

WINS provvederà a mettere in atto e ad implementare ogni controllo specifico, anche se non previsto dal presente Modello, che si renda opportuno o necessario al fine di prevenire e monitorare ogni singola area di rischio. Del controllo specifico adottato ne sarà data comunicazione all'OdV che provvederà a riportarlo per iscritto nei propri verbali periodici e avrà cura di specificarlo in sede di aggiornamento del Modello.

## SEZIONE A

### 1. Delitti nei rapporti con la Pubblica Amministrazione

#### 1.2 Le fattispecie rilevanti (*ex artt. 24, 25, 25-bis D.lgs. 231/2001*)

La presente Sezione della “Parte Speciale” nasce per individuare nei rapporti con la Pubblica Amministrazione (di seguito anche “PA”) tutte le fattispecie di reato, ipotizzabili nell’ambito dei rapporti tra WINS e la PA.

Agli effetti della Legge penale vigente in Italia, rientra nell’ambito della Pubblica Amministrazione qualsiasi soggetto che:

- svolga attività legislativa, giurisdizionale o amministrativa disciplinata da norme di diritto pubblico;
- persegua, realizzi o gestisca interessi pubblici.

A titolo meramente esemplificativo ed avendo riguardo all’operatività della WINS, si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione:

- i) lo Stato, le Regioni, le Province, i Comuni;
- ii) i Ministeri, i Dipartimenti, le Commissioni;
- iii) gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT, INPDAP);
- iv) l’Autorità Giudiziaria.

Tra le fattispecie penali qui di seguito considerate, il reato di concussione e di corruzione, nelle sue varie tipologie, presuppone il coinvolgimento di una persona fisica che assuma, ai fini della legge penale, la qualifica di “Pubblico Ufficiale” e/o di “Incaricato di Pubblico Servizio”, nell’accezione rispettivamente attribuita dagli artt. 357 e 358 c.p.

Di seguito vengono descritte brevemente le singole fattispecie contemplate nel D.lgs. 231/2001 agli artt. 24, 25, 25-ter lett. *s-bis*).

#### 1.3 Reati di tipo corruttivo

##### 1.3.1 Corruzione per l’esercizio della funzione (*ex artt. 318 e 320 c.p.*)

L’ipotesi di reato di cui all’art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per l’esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altre utilità o ne accetta la promessa. La pena prevista per il soggetto che realizzi la

suddetta fattispecie criminosa è la reclusione da uno a sei anni.<sup>15</sup> Ai sensi dell'art. 320 c.p. le disposizioni di cui all'art. 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio: in tali casi, tuttavia, le pene sono ridotte fino a un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

### **1.3.2 Corruzione per un atto contrario ai doveri di ufficio, circostanze aggravanti** (*ex artt. 319, 319-bis e 320 c.p.*)

L'ipotesi di reato di cui all'art. 319 c.p. si configura nel caso in cui il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altre utilità, o ne accetta la promessa. Ai fini della configurabilità di tale reato in relazione al compimento di un atto contrario ai doveri di ufficio vanno considerati sia gli atti illegittimi o illeciti (vietati, cioè, da norme imperative o contrastanti con norme dettate per la loro validità ed efficacia) sia quegli atti che, pur formalmente regolari, siano stati posti in essere dal pubblico ufficiale violando il dovere d'imparzialità o asservendo la sua funzione a interessi privati o comunque estranei a quelli proprio della Pubblica Amministrazione.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei a dieci anni<sup>16</sup>. Per questa fattispecie di reato la pena può essere aumentata ai sensi dell'art. 319-bis c.p. qualora l'atto contrario ai doveri di ufficio abbia ad oggetto il conferimento di pubblici impieghi, stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene. Ai sensi dell'art. 320 c.p., le disposizioni dell'art. 319 c.p. si applicano anche all'incaricato di un pubblico servizio: in tali casi, tuttavia, le pene sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale. Ai sensi dell'art. 321 c.p. le pene previste dagli artt. 318 e 319 c.p. si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il danaro o altre utilità. Si sottolinea, infine, come le ipotesi di reato di cui agli artt. 318 e 319 c.p. si differenziano dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale.

---

<sup>15</sup> Articolo 1, L. 27 maggio 2015, n. 69.

<sup>16</sup> Articolo 1, L. 27 maggio 2015, n. 69.

### **1.3.3 Corruzione in atti giudiziari** (*ex art. 319-ter c.p.*)

Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario, si corrompa un pubblico ufficiale, e dunque un magistrato, un cancelliere o altro funzionario dell'autorità giudiziaria. È importante sottolineare come il reato possa configurarsi a carico della Società indipendentemente dal fatto che la stessa sia parte del procedimento. La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da quattro a venti anni, a seconda se dal fatto derivi un'ingiusta condanna e del tipo di ingiusta condanna inflitta. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni.

### **1.3.4 Istigazione alla corruzione** (*ex art. 322 c.p.*)

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso danaro o altre utilità ad un pubblico ufficiale o incaricato di pubblico servizio (per l'esercizio delle sue funzioni o dei suoi poteri, per omettere o a ritardare un atto del suo ufficio, ovvero per fare un atto contrario ai suoi doveri) e tale offerta o promessa non venga accettata. La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la pena prevista per la fattispecie di cui all'art. 318 c.p., ridotta di un terzo, qualora l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio a compiere un atto nell'esercizio delle sue funzioni o dei suoi poteri; qualora invece l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o ritardare un atto del suo ufficio, la pena è quella prevista per la fattispecie di cui all'art. 319 c.p., ridotta di un terzo.

### **1.3.5 Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati** (*ex art. 322-bis c.p.*)

Le disposizioni degli artt. 314, 316, da 317 a 320 e 322, co.3 e 4, c.p., si applicano anche a membri delle istituzioni comunitarie europee, nonché ai funzionari delle stesse e dell'intera



struttura amministrativa comunitaria, e alle persone comandate presso la Comunità con particolari funzioni o addette ad enti previsti dai trattati. Le stesse disposizioni si applicano anche alle persone che nell'ambito degli stati membri dell'Unione Europea svolgono attività corrispondenti a quelle che nel nostro ordinamento sono svolte da pubblici ufficiali o da incaricati di un pubblico servizio. Ciò premesso, va detto che l'art. 322-*bis* c.p. incrimina altresì – e questo è d'interesse per i privati che abbiano a che fare con i soggetti sopra elencati – tutti coloro che compiano le attività colpite dagli artt. 321 e 322 c.p. (cioè attività corruttive) nei confronti delle persone medesime, e non solo i soggetti passivi della corruzione. Inoltre, l'art. 322-*bis* c.p. incrimina anche l'offerta o promessa di denaro o altra utilità *“a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o altri un indebito vantaggio in operazioni economiche internazionali, al fine di ottenere o di mantenere un'attività economica o finanziaria”*. Le menzionate persone sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti ed agli incaricati di un pubblico servizio negli altri casi.

## **1.4 La concussione**

### **1.4.1 Concussione** (*ex art. 317 c.p.*)

Il reato si configura nel caso in cui il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altre utilità. Anche la concussione, al pari della corruzione, è un reato bilaterale, in quanto richiede la condotta di due distinti soggetti, il concussore e il concusso. Tuttavia, a differenza della corruzione, solo il concussore è assoggettato a pena, in quanto il concusso è la vittima del reato: pertanto, per la natura privatistica dell'attività svolta dalla Società, i suoi esponenti non potrebbero commettere il reato in proprio in quanto sprovvisti della necessaria qualifica pubblicistica; i medesimi potrebbero al massimo concorrere in un reato di concussione commesso da un pubblico ufficiale ai sensi dell'art. 110 c.p. Inoltre, è astrattamente possibile che un dipendente della Società rivesta, al di fuori dell'attività lavorativa, una pubblica funzione. In tale ipotesi, questi, nello svolgimento del proprio ufficio o servizio, dovrà astenersi dal tenere comportamenti che, in violazione dei propri doveri d'ufficio e/o con abuso

delle proprie funzioni, siano idonei a recare un vantaggio alla Società. La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei a dodici anni.<sup>17</sup>

#### **1.4.2 Induzione indebita a dare o promettere utilità** (*ex art. 319-quater c.p.*)

Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o un terzo, denaro o altre utilità. La pena prevista per il pubblico ufficiale o l'incaricato di pubblico servizio è la reclusione da sei anni a dieci anni e sei mesi<sup>18</sup>; la pena per chi dà o promette denaro o altre utilità al pubblico ufficiale o all'incaricato di pubblico servizio è la reclusione sino a tre anni.

### **1.5 Le ipotesi di truffa**

#### **1.5.1 Truffa in danno dello stato o di altro ente pubblico** (*ex art. 640, co. 2, n. 1 c.p.*)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici e raggiri (intendendosi ricompresa in tale definizione anche l'eventuale omissione di informazioni che, se conosciute, avrebbero certamente determinato in senso negativo la volontà dello Stato, di altro ente pubblico o dell'Unione Europea) tali da indurre in errore e da arrecare un danno (di tipo patrimoniale) a tali enti. La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da uno a cinque anni e la multa da Euro 309 a Euro 1.549.

#### **1.5.2 Truffa aggravata per il conseguimento di erogazioni pubbliche** (*ex art. 640-bis c.p.*)

Il reato in oggetto si perfeziona allorquando i fatti di cui al precedente art. 640 c.p. riguardano l'ottenimento di contributi, finanziamenti o altre erogazioni concesse dallo Stato, da altri enti pubblici o dall'Unione Europea. La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da uno a sei anni.

#### **1.5.3 Frode informatica** (*ex art. 640-ter c.p.*)

---

<sup>17</sup> Articolo sostituito dall'art. 3, L. 27 maggio 2015, n. 69.

<sup>18</sup> Pena innalzata con l'art. 1, L. 27 maggio 2015, n. 69.

Si configura il reato di frode informatica quando, al fine di procurare a sé o ad altri un ingiusto profitto, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico. La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a cinque anni e con la multa da Euro a 309 a Euro 1549.

## **2. Identificazione delle aree e attività sensibili nei reati interessati con la P.A.**

Sono state individuate come attività sensibili tutte quelle che prevedono l'instaurazione di rapporti con le Pubbliche Amministrazioni. Va premesso che WINS non partecipa a gare d'appalto bandite dalla Pubblica Amministrazione o comunque in relazione alle quali risulti applicabile la disciplina di derivazione comunitaria in materia di contratti pubblici (D.lgs. 163/2006), né riceve contributi, finanziamenti o sovvenzioni di tipo pubblico.

Non vengono pertanto identificate come attività a rischio:

1. Negoziazione/stipulazione e/o esecuzione di contratti con soggetti pubblici (si tratta dell'attività di società che decide di partecipare, o negoziare/stipulare/eseguire contratti/convenzioni di concessione con la Pubblica Amministrazione mediante procedure negoziate, affidamento o trattativa privata);
2. Gestione delle attività di richiesta / acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici<sup>19</sup>.

---

<sup>19</sup> Si riportano di seguito le ipotesi di malversazione e di indebita percezione di erogazioni disciplinate dal codice penale e richiamate dal Decreto.

*Malversazione a danno dello Stato (ex art. 316-bis c.p.)*

Tale ipotesi di reato si configura nei confronti di chiunque, avendo ottenuto dallo Stato, da altro ente pubblico o dall'Unione Europea contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina a tali attività.

Per l'integrazione del reato è sufficiente che anche solo una parte delle attribuzioni ricevute sia stata impiegata per scopi diversi da quelli previsti, non rilevando, in alcun modo, che l'attività programmata sia stata comunque svolta. Sono altresì irrilevanti le finalità che l'autore del reato abbia voluto perseguire, poiché l'elemento soggettivo del reato medesimo è costituito dalla volontà di sottrarre risorse destinate a uno scopo prefissato.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a quattro anni.

*Indebita percezione di erogazioni a danno dello Stato (ex art. 316-ter c.p.)*

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato, da altri enti pubblici o dalla Unione Europea.

In questo caso, contrariamente a quanto visto in merito al reato precedente, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a tre anni e, nei casi meno gravi, una sanzione amministrativa tra Euro 5.164 ed Euro 25.822.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie di cui all'art. 640-bis c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi del reato di cui a quest'ultima disposizione. La linea di demarcazione tra l'ipotesi di indebita percezione di erogazioni a danno dello Stato (ex art. 316-ter c.p.) e quella di *truffa aggravata* per il conseguimento di erogazioni pubbliche (ex art. 640-bis c.p.)

Tuttavia, viene stabilito con il presente Modello che è fatto divieto ai Destinatari di porre in essere attività che rientrino nelle predette aree di rischio, senza che prima ne sia stato avvisato l'organo amministrativo di WINS che provvederà a valutare l'effettivo interesse della Società e stabilirà, in caso di positiva valutazione, in accordo con l'O.d.V. i principi di condotta che dovranno essere seguiti e i soggetti responsabili.

Vengono altresì identificate come attività a rischio:

1. Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali e richiesta di provvedimenti amministrativi occasionali/*ad hoc* necessari allo svolgimento di attività strumentali a quelle tipiche aziendali; e
2. Rapporti con soggetti pubblici:
  - a) per la gestione di adempimenti, verifiche, ispezioni, qualora lo svolgimento delle attività aziendali comporti la produzione di rifiuti solidi, liquidi o gassosi, ovvero l'emissione di fumi o la produzione di inquinamento acustico/elettromagnetico soggetti a controlli da parte di soggetti pubblici;
  - b) per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (D.lgs. n. 81/2008) e il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni;
  - c) relativi all'assunzione di personale anche con riferimento alle categorie protette o la cui assunzione è agevolata;
  - d) per la gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni;
  - e) per la predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere e relative ispezioni;
  - f) per indagini in corso, con Autorità Giudiziaria, Magistratura, Carabinieri, Polizia e Guardia di Finanza e altri organi di Polizia Giudiziaria;
  - g) per la gestione dei contenziosi pendenti e stragiudiziali;
  - h) preposti all'adempimento degli obblighi legislativi in materia di privacy;
  - i) per l'acquisizione di finanziamenti/contributi;
  - j) per la gestione dei flussi finanziari;

---

risiede nel tipo di condotta criminosa del reo che, nel primo caso, si limita a presentare documenti falsi o ad omettere informazioni dovute; mentre nella seconda ipotesi pone in essere artifici o raggiri che provocano l'induzione in errore della Pubblica Amministrazione.

k) per la gestione attiva di omaggi, liberalità e sponsorizzazioni.

### **3. Gestione dei rapporti con la PA con compiti di controllo e vigilanza**

Vi sono altri processi, da considerarsi come potenzialmente “strumentali” alle attività sopra esaminate (esso infatti, pur non essendo caratterizzati dall’esistenza di rapporti diretti con la PA, possono costituire supporto e presupposto – finanziario ed operativo – per la commissione dei reati nei rapporti con la PA).

Essi sono i seguenti:

- a. Acquisto di lavori, beni e servizi;
- b. Assunzione del personale;
- c. Omaggi, regali e benefici;
- d. Sponsorizzazioni;
- e. Spese di rappresentanza;
- f. Donazioni;
- g. Selezione di partners commerciali;
- h. Selezione di agenti/procacciatore d'affari;
- i. Spese di trasferta ed anticipi.

Tuttavia, in considerazione della specifica modalità operativa di WINS, della sua recente costituzione (start-up) e l’assenza di pendenti rapporti con la P.A., i processi sopra descritti sono da considerarsi non rilevanti, non dando luogo a circostanze di rischio ai fini della presente analisi.

Ciò vale, allo stato, sulla base della mappatura operata, che ha evidenziato quanto segue:

- Gli acquisti di WINS sono ancorati ai valori di mercato correnti. E’ sempre agevole eseguire una comparazione tra i fornitori. Per i servizi, se esterni, vengono commissionati sulla base di regolari preventivi e con mandati specifici, anche sotto il controllo dell’organo amministrativo se superiore a determinate soglie;
- WINS non emette sponsorizzazioni, donazioni ecc. e limita a riconoscere omaggi, sempre e solo di modico valore (calendari e simili);
- WINS affronta solo le spese di rappresentanza strettamente necessarie e quelle di trasferta sono limitate con liquidate a piè di lista, con conservazione dei giustificativi.

#### **4. Principi di controllo**

Ci si riferisce alle attività svolte per l'ottenimento (e successiva gestione del rapporto con la PA, anche in fase di controllo) di qualsiasi genere di licenza, concessione, autorizzazione, tra le quali ad esempio provvedimenti amministrativi per l'autorizzazione/approvazione/realizzazione di impianti o processi, o per le concessioni di spazi per l'ubicazione di uffici o autorizzazioni richieste *ex lege* dalle strutture scolastiche.

Il contatto con il soggetto pubblico si riferisce, in particolare, alle attività:

- a) che comportano la produzione di rifiuti ovvero la produzione di inquinamento acustico soggetti a controlli da parte di soggetti pubblici;
- b) inerenti agli aspetti che riguardano la sicurezza e l'igiene sul lavoro (D.lgs. 81/08) ed il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni;
- c) in materia di assunzione di personale, anche con riferimento alle categorie protette o soggetti la cui assunzione è agevolata;
- d) riguardanti i trattamenti previdenziali del personale;
- e) relative alla predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
- f) riguardanti indagini in corso.

Tali processi presentano uno sviluppo articolato in una o più delle seguenti fasi:

- istruttoria interna e predisposizione documentale;
- contatto con la PA per la rappresentazione dell'esigenza;
- predisposizione e invio della documentazione;
- rilascio dell'autorizzazione/concessione ed atti conseguenti;
- gestione dei rapporti in costanza di autorizzazione/concessione, con conclusiva verifica e/o collaudo;
- gestione di ispezioni/accertamenti e/o dell'eventuale contenzioso.

#### **5. Principi di condotta**

La presente sezione della "Parte Speciale" prevede l'espresso divieto a carico degli organi sociali, degli Apicali, dei lavoratori subordinati e dei Terzi di:

- a) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente,

le fattispecie di reato rientranti tra quelle sopra considerate (*ex artt. 24, 25, 25-ter lett. s)-bis* del D.lgs. 231/2001);

- b) violare i principi e le procedure aziendali previste nella presente sezione ed in tutto il sistema di gestione e controllo della Società.

Tale sezione comporta, conseguentemente, l'obbligo a carico dei soggetti sopra indicati di rispettare scrupolosamente tutte le leggi vigenti ed in particolare di:

- non offrire, promettere, fare regali, atti di cortesia, quali omaggi o forme di ospitalità, o altre utilità se non nei limiti del modico valore. In ogni caso, tali spese devono sempre essere autorizzate, documentate e nel rispetto dei limiti di *budget*;
- non esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della PA a titolo personale;
- non sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti;
- non effettuare "*facilitation payments*", cioè pagamenti di modico valore non ufficiali effettuati allo scopo di velocizzare, favorire o assicurare l'effettuazione di un'attività di *routine* o comunque prevista nell'ambito dei doveri dei soggetti pubblici o privati con cui WINS si relaziona;
- non richiedere prestazioni da parte dei consulenti che non trovino adeguata giustificazione nel contesto del rapporto costituito con gli stessi;
- non fornire, in qualsiasi forma, informazioni non veritiere o incomplete alla Pubblica Amministrazione;
- non condizionare in qualsiasi forma e con qualsiasi mezzo la libertà di determinazione di soggetti che, a qualsiasi titolo, siano chiamati a rendere dichiarazioni innanzi all'Autorità Giudiziaria;
- non promettere o dare seguito a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio a WINS;
- non porre in essere o istigare altri affinché pongano in essere pratiche corruttive di ogni genere.

Lo svolgimento dell'attività prevede:

- l'individuazione del responsabile/i delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda, di presentazione della domanda e di gestione della concessione e/o dell'autorizzazione, con la previsione, caso per caso, della funzione/organo e della/e persona/e deputata al controllo e degli specifici sistemi di controllo (ad es. l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo;
- la supervisione della domanda e del contenuto degli elaborati, se di contenuto tecnico, mediante l'attivazione di un consulente specializzato, con la specifica pattuizione dell'impegno al controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la concessione e/o autorizzazione;
- la previsione, caso per caso, di sistemi di reporting idonei a consentire verifica e tracciabilità dell'attività;
- la definizione di ruoli e compiti della funzione responsabile del controllo sulle fasi di ottenimento e gestione delle concessioni e/o autorizzazioni, con particolare riguardo ai presupposti di fatto e di diritto per la presentazione della relativa richiesta. In difetto di diversa indicazione, la funzione di controllo è attribuita all'organo amministrativo.

In tutte le fasi suddette è fatto divieto di tenere comportamenti che possano essere idonei ad indurre a favorire indebitamente gli interessi della WINS, ad eludere obblighi di legge, ad influenzare indebitamente, nell'interesse della Società, il giudizio/parere della Pubblica Amministrazione, ad evitare, anche in parte, l'osservanza degli adempimenti di legge/amministrativi o, comunque, a determinare indebiti privilegi per la Società, (in sede di collaudo/verifica da parte della PA) ad influenzare indebitamente, nell'interesse della WINS, il giudizio dei collaudatori/verificatori, (in sede di adempimenti conseguenti agli obblighi di legge/normativi e di attività di gestione in genere) a rappresentare alla PA dati/informazioni non corretti, con la finalità di perseguire “*posizioni privilegiate*” nell'interesse della Società o di eludere obblighi di legge/normativi.

Con specifico riguardo all'ipotesi di ispezioni controlli e accertamenti in genere, si prevede:

- che per ogni visita, controllo, accesso ecc. sia nominato un responsabile interno;
- che lo stesso attivi ove possibile un consulente specializzato;
- che lo stesso provveda a redigere un *report* informativo dell'attività svolta nel corso dell'ispezione, contenente, fra l'altro, i nominativi dei funzionari incontrati, i documenti



richiesti e/o consegnati, i soggetti coinvolti ed una sintesi delle informazioni verbali richieste e/o fornite;

- uno specifico sistema di controllo (ad es. l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo.

## **6. Sistema di controllo**

Il sistema di controllo si basa sull'elemento qualificante della tracciabilità degli atti e sulla formalizzata separazione di ruolo nelle fasi chiave del processo.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati da:

- a) tracciabilità degli atti e delle fonti informative, nelle singole fasi dei processi con specifico riferimento ad impiego di risorse e tempi;
- b) selezione ed utilizzo di professionisti esterni qualificati ed indipendenti;
- c) formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della Società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla Società;
- d) rendicontazione dei rapporti formali con rappresentanti della Pubblica Amministrazione e tracciabilità degli atti e delle fonti documentali che ne stanno alla base.

La funzione preposta deve comunicare tempestivamente all'O.d.V.:

- elenco delle richieste per licenze, autorizzazioni, concessioni ecc.;
- elenco provvedimenti ottenuti e contratti stipulati;
- elenco contestazioni che la Pubblica Amministrazione ha formalmente inoltrato alla Società;
- elenco ispezioni, visite e controlli in genere subiti;
- elenco delle sanzioni eventualmente comminate.

## SEZIONE “B”

### 1. Delitti informatici e trattamento illecito dei dati. *Privacy (cd. Cybercrime)*

#### 1.1 Le fattispecie rilevanti (ex art. 24-bis, D.lgs. n. 231/2001)

La presente sezione si riferisce ai delitti informatici e le fattispecie penalmente rilevanti introdotte con l’art. 24-bis del D.lgs. 231, con l’art. 7 della L. 18 marzo 2008 n. 48. La casistica dell’illecito informatico, che si caratterizza nell’abuso della tecnologia informatica (hardware e software) per la commissione di reati, è molto ampia, con una variegata tipologia (spam, frode, accesso a contenuti sensibili, molestie e cyberbullismo, spaccio di sostanze illecite e terrorismo). Di seguito si considerano le condotte “a rischio” ai sensi del Decreto, senza escludere l’attenzione anche per le altre fattispecie specie in ragione della specificità dell’oggetto sociale della WINS e della tipologia di utenti (minori), che si avvalgono del servizio informativo erogato.

#### 1.2 Falsità in un documento informatico pubblico o con efficacia probatoria.

##### Documenti informatici (ex art. 491-bis c.p.)

“Se alcuna delle falsità previste dal presente capo (i.e. capo III c.p.) riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici”<sup>20</sup>.

A tal fine per documento informatico si intende qualunque “rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti”<sup>21</sup>. L’art. 491-bis c.p. fornisce una definizione di documento informatico basata sull’elemento materiale del supporto di memoria e non sui dati in esso contenuti: può definirsi supporto informatico qualsiasi supporto di memoria (interno e/o esterno all’elaboratore elettronico) – sul quale possono essere registrati e conservati per un certo periodo di tempo dei dati destinati ad essere letti ed eventualmente elaborati da un sistema informatico. Non costituisce supporto informatico, ai sensi dell’art. 491-bis c.p., il tabulato emesso dal computer al termine del processo di elaborazione: il tabulato – così come ogni *output* stampato – è normalmente costituito da un foglio di carta sul quale il contenuto dei dati è riprodotto in caratteri alfanumerici per consentirne la lettura da parte dell’uomo;

---

<sup>20</sup> Il presente articolo, aggiunto dall’art. 3, L. 23.12.1993, n. 547, poi modificato dall’art. 3, L. 18.03.2008, n. 48 (G.U. 04.04.2008, n. 80, S.O. n. 79), con decorrenza dal 05.04.2008, è stato da ultimo così sostituito dall’art.2 del D.lgs. 15.01.2016, n. 7 con decorrenza dal 06.02.2016. Il testo recitava: “Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private”.

<sup>21</sup> Codice dell’Amministrazione Digitale, il cd. CAD, introdotto con il D.lgs. 82/2005, aggiornato con D.lgs. 179/2016.

rientrano invece nella nozione di documento informatico le carte di pagamento a banda magnetica e le carte a microprocessore (ad es. carte prepagate, carta Viacard a scalare e alcune carte telefoniche). È, inoltre, considerato documento informatico il supporto informatico che contenga il programma specificamente destinato ad elaborare i dati, ossia il programma memorizzato all'interno del sistema informatico o su un supporto esterno che svolga la funzione di elaborare dati. In merito alla formazione del documento informatico, può dirsi tale se vengono utilizzate una delle seguenti principali modalità:

- a) redazione tramite l'utilizzo di appositi strumenti *software*;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti inter-operanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico assume la caratteristica di immutabilità, se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta ed accesso, nonché se ne sia garantita la staticità nella fase di conservazione. Il detto documento, inoltre, identificato in modo univoco e persistente, può essere memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta è delegabile a soggetti terzi.

### **1.3 Accesso abusivo ad un sistema informatico/telematico (ex 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 (co.1). 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 (co.2).*

*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 (co.3). Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio” (co.4).*

Tale disposizione è rivolta a tutelare la riservatezza dei dati e dei programmi contenuti in un sistema informatico. In particolare per sistema informatico, ai fini della configurabilità del delitto di cui all'art. 615-ter c.p., deve intendersi una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche. Il sistema è dunque tale se gestisce ed elabora dati, mentre tutto ciò che in un sito web o nel mondo dell'informatica non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è sistema informatico. L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema, ossia tutte quelle misure di protezione al cui superamento è possibile subordinare l'accesso ai dati e ai programmi contenuti nel sistema, quali a titolo esemplificativo codici di accesso, alfabetici o numerici da digitare su una tastiera o memorizzati su una banda magnetica di una tessera da introdurre in apposito lettore. Oltre a queste misure logiche possono rilevare anche misure fisiche quali l'uso di chiavi metalliche per l'accensione dell'elaboratore. La condotta rilevante consiste nell'introdursi abusivamente in un sistema protetto o nel permanervi contro la volontà espressa o tacita del titolare del diritto di escludere gli altri dall'uso del sistema.

Si verifica introduzione quando si oltrepassano le barriere logiche e/o fisiche che presidiano l'accesso alla memoria interna del sistema e si è quindi in condizione di richiamare i dati ed i programmi che vi sono contenuti. L'introduzione può avvenire sia a distanza, sia per via elettronica e sia da vicino da parte di chi si trovi a diretto contatto con l'elaboratore. Oltre all'introduzione rileva anche l'ipotesi del mantenersi in un sistema protetto contro la volontà espressa o tacita del titolare dello *ius excludendi*. Tale caso ricorre quando, in seguito ad un'introduzione involontaria o causale o solo inizialmente autorizzata, l'agente (colui che agisce) permanga nel sistema informatico altrui, nonostante il dissenso del soggetto che ha interesse alla riservatezza dei dati e dei programmi in esso contenuti.

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

*“Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino ad Euro 5.164. La pena è della reclusione da uno a due anni e della multa da Euro 5.164 a Euro 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater”<sup>22</sup>.*

L'art. 615-quater è rivolto a punire la condotta di detenzione e di diffusione abusiva di codici di accesso che può cagionare la commissione di altri reati informatici. Infatti, chiunque entri in possesso abusivamente di codici d'accesso, può commettere un accesso abusivo ad un sistema o può diffondere tali codici ad altre persone, le quali a loro volta potrebbero accedere abusivamente al sistema. L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico, indipendentemente dalla natura del mezzo; infatti, può trattarsi di una password, di un codice d'accesso o semplicemente di una informazione che consentano di eludere le misure di protezione. La disposizione in esame incrimina due tipi di condotte, volte rispettivamente ad acquisire i mezzi necessari per accedere al sistema informatico altrui oppure a procurare ad altri tali mezzi o comunque le informazioni sul modo di eludere le barriere di protezione. La semplice detenzione di codici di accesso o di strumenti similari da parte di chi non sia autorizzato a farne uso, non costituisce fatto penalmente rilevante e pertanto punibile.

#### **1.5 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (ex art. 615-quinquies c.p.)**

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

---

<sup>22</sup> Per un'ulteriore ipotesi di aumento della pena, si veda art. 36 della L. 5 febbraio 1992, n. 104.

*reclusione fino a due anni e con la multa sino a euro 10.329*<sup>23</sup>. L'art. 615-quinques c.p. è rivolto a tutelare il patrimonio informatico, inteso come *hardware*, *software* e dati da attacchi con virus informatici. La condotta punita è la diffusione (divulgazione), la comunicazione (portare a conoscenza) o la consegna (dare in senso materiale) di un programma informatico che ha lo scopo o l'effetto di danneggiare il sistema informatico o telematico altrui, o di danneggiare dati o programmi in esso contenuti o ad esso pertinenti, oppure l'interruzione parziale o totale del suo funzionamento o la sua alterazione. La normativa vigente non distingue la provenienza soggettiva dei virus, se sono creati da chi commette il reato o da terzi, né tanto meno tra programma informatico, che reca concretamente un danno al sistema informatico, e quello che non lo provoca. Un programma, pertanto, può essere considerato "infetto", ai sensi della norma in esame, se è in grado non solo di danneggiare le componenti logiche di un sistema informatico, ma anche di interrompere o alterare il funzionamento di quest'ultimo.

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

*"Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni (co.1). 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 (co.2). I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa (co.3). 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"* (co.4).

Ai sensi della presente disposizione in esame, la condotta illecita può consistere alternativamente nell'intercettare fraudolentemente una comunicazione informatica o telematica oppure nell'impedirla o interromperla. Il secondo comma prevede, altresì, l'ipotesi della rivelazione in tutto o in parte mediante qualsiasi mezzo di informazione al pubblico del contenuto di una conversazione intercettata. Intercettare una comunicazione informatica o

---

<sup>23</sup> Articolo inserito dall'art. 4 L. 23 dicembre 1993, n. 547 e successivamente sostituito dall'art. 4 L. 18 marzo 2008, n. 48.

telematica significa prendere cognizione del suo contenuto, intromettendosi nella fase della sua trasmissione. L'intercettazione deve essere realizzata fraudolentemente, ossia eludendo eventuali sistemi di protezione della trasmissione in corso (ad es. decodificando dei dati trasmessi in forma cifrata o superando delle barriere logiche poste a difesa del sistema che invia o riceve la comunicazione) o comunque in modo tale da rendere non percepibile o riconoscibile a terzi l'intromissione abusiva. La comunicazione è invece impedita quando se ne renda impossibile la trasmissione, intervenendo sul sistema informatico che deve inviare o ricevere i dati; una comunicazione può invece essere interrotta sia agendo sul sistema che invia i dati e che deve ricevere la comunicazione, sia ad esempio deviando il flusso dei dati in corso di trasmissione da un elaboratore ad un altro.

### **1.7 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche** (ex art. 617-quinquies c.p.)

*“Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni (co.1). La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater” (co. 2).* Tale disposizione mira a reprimere una condotta antecedente e preparatoria rispetto a quella prevista dall'art. 617-quater c.p., vietando l'installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Il reato contemplato dall'art. 617-quinquies c.p. è stato ravvisato nel caso di utilizzazione di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione, con il sistema rientra nella nozione di "intercettare" di cui alla norma incriminatrice.

### **1.8 Danneggiamento di informazioni, dati e programmi informatici** (ex 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 (co.1). 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 (co.2)<sup>24</sup>.*

---

<sup>24</sup> Comma sostituito dall'art. 2 D.lgs. 15 gennaio 2016, n. 7. V. art. 635 c.p.



Oggetto del danneggiamento può essere in primo luogo un sistema informatico di qualsiasi tipo e dimensione, eventualmente collegato a distanza con altri elaboratori come nel caso dei sistemi telematici. L'aggressione può rivolgersi tanto al sistema nel suo complesso, quanto a una o più delle sue componenti materiali, quali a titolo esemplificativo le periferiche. Non possono invece essere considerati componenti di un sistema informatico i supporti magnetici o ottici sui quali non siano memorizzati dati o programmi, in quanto il loro danneggiamento non è idoneo ad arrecare nessun pregiudizio alla funzionalità del sistema informatico nel quale dovrebbero essere utilizzati. Oltre al sistema informatico, il danneggiamento può avere ad oggetto dati e programmi informatici per dati si intendono quelle rappresentazioni di informazioni o di concetti che, essendo destinate all'elaborazione da parte di un computer, sono codificate in una forma (elettronica, magnetica ottica o simile) non percettibile visivamente. Suscettibili di danneggiamento possono essere anche dati o programmi immagazzinati nella memoria interna dell'elaboratore, oppure su un supporto esterno come un disco magnetico ovvero ottico. Tra i beni suscettibili di danneggiamento, l'art. 635-*bis* c.p. include anche il bene "informazione". Poiché l'informazione è un'entità di per sé astratta, questa espressione assume significato solo in quanto la si riferisca alle informazioni incorporate su un supporto materiale, cartaceo o di altro tipo. Le condotte rilevanti per l'illecito in esame sono la distruzione, il deterioramento e l'inservibilità totale o parziale. L'ipotesi di distruzione di dati e di programmi più frequente e significativa, è rappresentata dalla loro cancellazione, sia attraverso la smagnetizzazione del supporto, sia sostituendo i dati originari con nuovi dati diversi, sia impartendo all'elaboratore, in cui si trovano i dati o i programmi, uno dei comandi in grado di provocarne la scomparsa.

Alla luce della circostanza che la distruzione deve essere totale, non ricorre questa ipotesi quando i dati o i programmi cancellati siano ancora recuperabili in una zona remota dell'elaboratore, utilizzando un determinato tipo di programma oppure ne sia stata solo impedita la visualizzazione sullo schermo del computer.

### **1.9 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (ex art. 635-ter c.p.)**

*“Salvo che il fatto costituisca un 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 (co.1). 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 (co.2). 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 (co.3)<sup>25</sup>.

### **1.10 Danneggiamento di sistemi informatici o telematici (ex 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 (co.1). 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 (co.2)<sup>26</sup>”.

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

“Se il fatto di cui all'art. 635-quater c.p. 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 (co.1). 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 (co.2). 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 (co.3)<sup>27</sup>”.

### **1.12 Frode informatica del certificatore di firma elettronica (ex 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 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 Euro 51 ad Euro 1.032”.

## **2. Le “attività sensibili” in relazione ai delitti informatici. Privacy e Cybercrime**

L'attività svolta dalla WINS richiede l'utilizzo da parte dei dipendenti e studenti (anche minori di età) di *personal computer* per il normale svolgimento del proprio lavoro o per le attività formative, con corsi interattivi ed aule informatizzate. Le postazioni PC, le aule e le piattaforme

<sup>25</sup> Comma sostituito dall'art. 2 D.lg. 15 gennaio 2016, n. 7. V. *sub art.* 635 c.p.

<sup>26</sup> Comma sostituito dall'art. 2 D.lg. 15 gennaio 2016, n. 7. V. *sub art.* 635 c.p.

<sup>27</sup> Comma sostituito dall'art. 2 D.lg. 15 gennaio 2016, n. 7. V. *sub art.* 635 c.p.

sono dotati di programmi necessari per lo svolgimento delle varie attività, tutti con le rispettive licenze. I dispositivi sono dotati di password di accesso ad uso esclusivo ed il server si trova custodito in apposito locale con chiusura di sicurezza. Tutti i software utilizzati dalle postazioni fisse di PC e dai PC portatili sono caricati da un tecnico e/o da un docente di informatica all'uopo incaricato che ne cura gli aggiornamenti.

I PC sono programmati in modo tale da non consentire al singolo utente di caricare software diversi sull'unità locale e l'accesso ad Internet (sia dai laboratori didattici che al wi-fi) viene limitato, in modo che tutti i PC non possano accedere a siti pornografici di qualsiasi tipo, a siti con contenuto immorale, o che contengano materiale detestabile o di dubbio gusto, specie in ragione della presenza di utenti minorenni presso la struttura della WINS.

Per comodità di consultazione, anche in ragione della particolare realtà lavorativa della Società, qui di seguito viene trattato quanto regolamentato in materia di *privacy*. La realtà scolastica nella quale sono presenti professori, alunni e operatori del settore richiede di mostrare una particolare attenzione al “corretto trattamento dei dati personali (cd. *Privacy*)” ed alla relativa normativa contenuta nel D.lgs. 196/2003 (cd. Codice sulla *Privacy*).

Il corretto trattamento dei dati sensibili costituisce una condizione essenziale per il rispetto della dignità delle persone, della loro identità, del loro diritto alla riservatezza, valida sia per gli studenti che per i dipendenti della Società, nonché per tutti i soggetti che entrino in contatto con la stessa. In particolare, in ragione della preminente funzione formativa, vengono trattate numerose tematiche relative alle famiglie degli studenti, ai loro problemi sanitari, a situazioni di disagio sociale, ad abitudini alimentari o tematiche relative all'educazione sessuale ed è facile, che si palesino aspetti che possano contrastare con la *privacy* e la tutela dei dati sensibili. Per tali motivi è necessario poter adottare alcuni accorgimenti per prevenire condotte che possano esporre WINS al regime di responsabilità previsto dal Decreto. In particolare, seguono alcune aree su cui si ritiene opportuno richiamare l'attenzione degli organi di vertice e di tutti i soggetti interessati, che possano in modo diretto o indiretto invocare a loro vantaggio la violazione della normativa sulla *Privacy*.

### ***Trattamento dei dati nelle scuole***

Per poter trattare i dati personali, le scuole sono obbligate non solo a presentare un'informativa completa ma anche a ottenere il consenso puntuale e liberamente espresso dei soggetti interessati (studenti maggiorenni, famiglie). Nel caso di trattamento di dati giudiziari e sensibili,

le scuole sono tenute a rispettare anche le prescrizioni contenute nelle autorizzazioni generali del Garante sulla Privacy, le quali esplicitano i trattamenti consentiti.

Alcune tematiche di rilievo in materia:

▪ **Origini razziali, etniche e fede religiosa**

I dati sulle origini razziali ed etniche e sulle convinzioni religiose degli studenti possono essere trattati da WINS per favorire l'integrazione degli alunni e contribuire alla maturazione umana e religiosa degli stessi, senza che ciò costituisca una forma di limitazione della libertà di religione e del principio di eguaglianza, costituzionalmente garantiti (art. 2 e 3 Cost.).

▪ **Stato di salute**

I dati idonei a rivelare lo stato di salute del personale o degli studenti possono essere trattati da WINS per distinte finalità, quali l'assegnazione del sostegno agli alunni disabili, per la composizione delle classi, per la gestione delle assenze per malattia, per l'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, nonché per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione.

▪ **Diritto di accesso ai dati personali**

Anche in ambito scolastico, ogni persona ha diritto di accesso ai propri dati e conoscere se sono conservate informazioni strettamente personali che la riguardano, di apprenderne il contenuto, di farle rettificare se erranee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento" anche tramite suoi incaricati o responsabili. Se non si ottiene risposta, o se il riscontro non è sufficiente, è possibile rivolgersi alla Magistratura o al Garante sulla Privacy.

La normativa che regola l'accesso ai dati personali contenuti negli atti amministrativi, è la L. n. 241 del 1990 (e successive modifiche).

▪ **Voti ed esami, temi in classe degli studenti**

Non commette violazione della *privacy*, l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare. Nel momento in cui gli elaborati vengono letti in classe - specialmente se sono presenti argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto

d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

- **Informazioni sugli studenti - Circolari e comunicazioni scolastiche**

Il diritto–dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori. È quindi necessario, ad esempio, evitare di inserire nelle comunicazioni scolastiche elementi che consentano di risalire, anche indirettamente, all'identità di minori coinvolti in vicende particolarmente delicate.

- **Orientamento, formazione e inserimento professionale**

Su richiesta degli studenti interessati e loro genitori esercenti la potestà genitoriale, con loro consenso, WINS può comunicare, anche a privati e per via telematica, i dati relativi a risultati scolastici per aiutarli nell'orientamento, la formazione e l'inserimento professionale anche all'estero, senza che ciò costituisca violazione della normativa a tutela della *privacy*.

- **Pubblicità**

La conoscibilità a chiunque degli esiti scolastici (ad esempio attraverso il tabellone affisso nella Scuola) risponde a essenziali esigenze di trasparenza. Ciò non autorizza soggetti terzi a utilizzare tali nominativi per altre finalità come, ad esempio, l'invio di materiale pubblicitario.

- **Questionari per attività di ricerca**

Svolgere attività di ricerca, con la raccolta di informazioni personali, spesso anche sensibili, tramite questionari da sottoporre agli alunni, è consentito soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate. Gli intervistati, inoltre, devono sempre avere la facoltà di non aderire all'iniziativa.

- **Foto, audio e video**

Le aree di rischio in materia sono: recite, viaggi di istruzione, viaggi di studio e foto di classe. Sono vietate le riprese audiovisive in classe durante le ore di lezione e la loro registrazione. Non violano la *privacy* le riprese video e le fotografie raccolte dai genitori durante le recite, i viaggi di studio e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione con finalità altresì commerciale, che è vietata senza previo consenso. A riguardo si precisa

la necessità di mostrare particolare attenzione per l'eventuale pubblicazione delle medesime immagini su Internet ed in particolare sui *social network*. In caso di comunicazione sistematica o diffusione di dette immagini, diventa necessario ed imprescindibile ottenere il consenso delle persone presenti nelle fotografie e nei video, la cui immagine ed i dati personali costituiscono diritti personalissimi.

- **Videosorveglianza**

L'installazione del sistema di videosorveglianza esistente ed è finalizzato a garantire il diritto dello studente alla sicurezza, senza che ciò possa costituire una violazione della privacy e del diritto alla riservatezza. Le telecamere presenti sono installate, per ragioni di sicurezza del personale e dell'utenza in genere della Scuola, all'interno della struttura, nell'area verde circostante, comprese le aree comuni. Le immagini registrate possono essere conservate per brevi periodi. I cartelli, che segnalano il sistema di videosorveglianza, devono essere visibili anche di notte.

## SEZIONE “C”

### 1. Reati societari

#### 1.1 Le fattispecie rilevanti (*ex art. 25-ter, D.lgs. n. 231/2001*)

Nel novero di reati societari è ravvisabile l’interesse del legislatore ad assicurare la trasparenza nella gestione societaria, la corretta tenuta dei documenti contabili, la corretta informazione ai terzi ed al mercato in generale, a tutelare il capitale sociale, il patrimonio sociale, il regolare funzionamento della Società, nonché le funzioni di controllo. Si elencano qui di seguito le fattispecie contemplate dall’art. 25-ter del Decreto che possono assumere rilevanza nei confronti di WINS.

#### 1.2 False comunicazioni sociali e le false comunicazioni sociali in danno della Società, dei soci o dei creditori (*ex art. 2621 e 2622 c.c.*)

La consumazione di questi reati avviene con l’esposizione “*consapevole*” nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette alle competenti autorità o al pubblico, di fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società, in “modo concretamente idoneo ad indurre altri in errore”, sono puniti con la pena della reclusione da uno a cinque anni. La stessa pena si applica anche se la falsità o le omissioni riguardano beni posseduti o amministrati dalla Società per conto di terzi. La condotta deve essere finalizzata a conseguire per sé o per altri un ingiusto profitto.

#### 1.3 Impedito controllo (*ex art. 2625 c.c.*)

L’illecito si verifica nell’ipotesi in cui gli amministratori della Società, occultano documenti o con altri idonei artifici, impediscano o comunque ostacolano, occultando documenti o con altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci o ad altri organi sociali. Tale condotta è punita con la sanzione amministrativa pecuniaria fino a Euro 10.239. Laddove, la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa la condotta ha cagionato.

### 2. Attività sensibili e sistema di controlli

Le attività potenzialmente sensibili sono le seguenti:

- tenuta della contabilità;
- formazione e redazione del bilancio e di ogni altra comunicazione sociale;
- formazione e redazione delle relazioni e delle altre comunicazioni previste dalle singole disposizioni di legge e relative alla situazione economica, patrimoniale o finanziaria della Società;
- attività di controllo contabile;
- disposizione dei beni sociali;
- conservazione della documentazione inerente l'attività della Società, al fine di consentire le attività di controllo o di revisione previste dalla legge;
- preparazione delle riunioni assembleari, formazione della volontà assembleare, svolgimento e verbalizzazione delle assemblee;
- rapporti con gli organi (interni ed esterni) deputati al controllo e alla vigilanza.

Il sistema di controlli prevede:

- che in ogni funzione aziendale competente siano adottate misure idonee a garantire che tutte le operazioni contabili, la redazione del bilancio, le situazioni economiche infrannuali e i comunicati sociali in genere, siano effettuate con correttezza e nel rispetto dei principi di veridicità, completezza e accuratezza e siano tempestivamente segnalate eventuali situazioni anomale.
- Documentazione: il progetto di bilancio è trasmesso all'organo amministrativo con congruo anticipo rispetto alla riunione per l'approvazione del progetto di bilancio.

## SEZIONE “D”

### 1. Delitti contro la personalità individuale.

#### 1.1 Le fattispecie rilevanti (ex art. 25-quinquies, D.lgs. n. 231/2001)

Si riporta, di seguito, una breve descrizione di taluni dei reati richiamati dall’art. 25-quinquies, del D.lgs. 231/2001, rubricato “*Delitti contro la personalità individuale*”, presi in considerazione in quanto ritenuti sensibili e potenzialmente rientranti nella “area di rischio” per la Società, per la cui ragione si intende concentrare l’attenzione in tale sede.

Le misure contenute nell’art. 25-quinquies, sono state introdotte nel Decreto, con l’art. 5 L. 228/2003, per reprimere il fenomeno della tratta di persone, le forme di sfruttamento di situazioni di vulnerabilità o di inferiorità psico-fisica ed il prelievo di organi. La disposizione si completa con la previsione oltre di sanzioni pecuniarie, anche di quelle interdittive definitiva nei confronti delle società, allorché i soggetti che li rappresentino, o che ricoprano le particolari cariche previste dal Decreto, commettano i reati contro la personalità individuale contemplati nell’art. 25-quinquies, allo scopo unico o prevalente di consentire o agevolare la commissione di detti reati. Seguono i delitti presi in considerazione nell’analisi della Società.

#### 1.2 I reati contro la personalità individuale

##### 1.2.1 Prostituzione minorile (ex art. 600-bis c.p.)<sup>28</sup>

*“È punito con la reclusione da sei a dodici anni e con la multa da Euro 15.000 ad Euro 150.000 chiunque:*

- 1) recluta o induce alla prostituzione una persona di età inferiore agli anni diciotto;*
- 2) favorisce, sfrutta, gestisce, organizza o controlla la prostituzione di una persona di età inferiore agli anni diciotto, ovvero altrimenti ne trae profitto (co.1). Salvo che il fatto costituisca più grave reato [609-quater c.p], chiunque compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi, è punito con la reclusione da uno a sei anni e con la multa da euro 1.500 a euro 6.000 (co.2)”.*

##### 1.2.2 Pornografia minorile (ex art. 600-ter c.p.)

*Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero recluta o induce minori di anni diciotto a partecipare ad esibizioni o spettacoli pornografici*

---

<sup>28</sup> Articolo così sostituito dall’art. 4, L. 1° ottobre 2012, n. 172.



*ovvero da essi trae altrimenti profitto, è punito con la reclusione da sei a dodici anni e con la multa da Euro 24.000 ad Euro 240.000 (co.1).*

*Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma (co.2). Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da 2.582 euro a 51.645 euro (co.3). Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164 (co.4).*

*Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità (co.5). Salvo che il fatto costituisca più grave reato, chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto è punito con la reclusione fino a tre anni e con la multa da euro 1.500 a euro 6.000 (co.6). Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali (co.7)<sup>29</sup>.*

### **1.2.3 Detenzione di materiale pornografico (ex art. 600-quater c.p.)**

*“Chiunque, al di fuori delle ipotesi previste dall'art. 600-ter c.p., consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità (co.2)”.*

### **1.2.4 Pornografia virtuale (ex art. 600-quater c.p.)<sup>30</sup>**

*“Le disposizioni di cui agli art. 600-ter e 600-quater (c.p.) si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo (co.1). Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali (co.2)”.*

---

<sup>29</sup> Comma inserito dall'art. 4, L. 1° ottobre 2012, n. 172.

<sup>30</sup> Articolo inserito dall'art. 4, L. 6 febbraio 2006, n. 38.

### **1.2.5 Iniziative turistiche volte allo sfruttamento della prostituzione minorile** (*ex art. 600-quinques c.p.*)

*“Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da Euro 15.493 ad Euro 154.937”*

## **2. Attività sensibili e sistema di controllo**

Il sistema di controllo prevede che:

- siano previste modalità efficienti e costantemente aggiornate per prevenire i profili di rischio e siano definite specifiche attività di risk assessment;
- lo svolgimento delle attività a rischio avvenga in conformità alle cautele, alle regole individuate nel punto precedente;
- siano immediatamente interrotte o, comunque, non sia data esecuzione ad operazioni che vedano coinvolti soggetti che non rispettano le leggi nazionali e internazionali applicabili;
- siano definite le regole di base per la sicurezza delle informazioni quando si utilizza una postazione di lavoro, fisica o virtuale, al fine di proteggere la proprietà, le risorse, gli studenti ed il personale di WINS, contro tutte le forme di minacce, interne o esterne, deliberate o accidentali.

## SEZIONE “E”

### 1. Delitti per violazione delle norme per la tutela della salute e sicurezza sul lavoro

#### 1.1 Le fattispecie rilevanti e i criteri di imputazione (*ex art. 25-septies, D.lgs. 231/2001*)

L’art. 9 della Legge n. 123/2007 ha introdotto nel Decreto, l’art. 25-*septies*, che estende la responsabilità amministrativa degli enti ai reati di omicidio colposo (*ex art. 589 c.p.*) e lesioni personali colpose gravi o gravissime (*ex art. 590 c.p.*), commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro (quali ad esempio quelle previste dal D.lgs. 9 aprile 2008, n. 81 “*Testo unico sulla salute e sicurezza sul lavoro*” e successive integrazioni e modificazioni). Si riportano di seguito i riferimenti normativi delle fattispecie rilevanti in materia di illeciti inerenti alla salute ed alla sicurezza sul lavoro, considerati “sensibili” per la Società, da attenzionare in accordo a quanto previsto dal Decreto, con una descrizione sintetica di alcuni aspetti significativi per ciascuno dei reati presupposto contemplati in detta fonte.

#### 1.1.2 Omicidio colposo (*ex art. 589 c.p.*)

*“Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni (co.1). Se il fatto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena è della reclusione da due a sette anni (co.3)<sup>31</sup>.(co.4)<sup>32</sup> Nel caso di morte di più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici”(co.6).*

#### 1.1.3 Lesioni personali colpose (*ex art. 590 c.p.*)

*“Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino ad Euro 309 (co.1). Se la lesione è grave, la pena è della reclusione da uno a sei mesi o della multa da Euro 123 ad Euro 619. Se è gravissima, della reclusione da tre mesi a due anni o della multa da Euro 309 ad Euro 1.239(co.2). Se i fatti di cui al secondo comma sono commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena per le lesioni gravi è della reclusione da tre mesi ad un anno o della multa da Euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni (co.3). Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle*

---

<sup>31</sup> Articolo modificato dall’art. 1, co. 3, lett. c) L. 23 marzo 2016, n. 41.

<sup>32</sup> Il co. 5 dell’articolo 589 c.p. è stato abrogato dall’art. 1, comma 3 lett. d), l. 23 marzo 2016, n. 41, con effetto a decorrere dal 25 marzo 2016, ai sensi dell’art. 1, comma 8, L. n. 41, cit.

*violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque (co.4). Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale (co.5).*

## **2. Attività sensibili e sistema di controllo**

Le attività ritenute sensibili con riferimento ai reati previsti dall'art. 25-septies del Decreto sono quelle relative a:

- i) Pianificazione delle attività del servizio di prevenzione e protezione della salute e sicurezza dei lavoratori.
- ii) Organizzazione della struttura con riferimento alle attività in tema di salute e sicurezza sul lavoro.
- iii) Sistema di deleghe e funzioni. L'attività sensibile è quella relativa alla realizzazione di un adeguato sistema di deleghe di funzioni in materia di salute e sicurezza.
- iv) Individuazione, valutazione e mitigazione dei rischi. Si tratta dell'attività di periodica valutazione dei rischi al fine di: i) individuare i pericoli e valutare i rischi per la sicurezza e la salute dei lavoratori e gli utenti della Scuola e della Boarding School; ii) identificare le misure in atto per la prevenzione ed il controllo dei rischi e per la protezione dei lavoratori e gli utenti della Scuola e della Boarding School; iii) definire il piano di attuazione di eventuali nuove misure ritenute necessarie.
- v) Gestione del sistema di prevenzione e protezione della salute e sicurezza.
- vi) Attività di informazione. Si tratta della gestione di un sistema interno di diffusione delle informazioni tale da garantire a tutti i livelli aziendali e agli utenti della Scuola e della Boarding School un corretto approccio alle tematiche riguardanti la sicurezza e la salute.
- vii) Attività di formazione. Consiste nell'attivazione e nella gestione di piani sistematici di formazione e sensibilizzazione con la partecipazione periodica di tutti i dipendenti ed utenti, nonché di seminari di aggiornamento per i soggetti che svolgono particolari ruoli.
- viii) Rapporti con i fornitori con gli appaltatori e subappaltatori. Si tratta dell'attività di gestione dei rapporti con i terzi al fine di coordinare i lavori e di prevenire i rischi derivanti dall'attività posta in essere presso la Scuola da terze parti.
- ix) Gestione degli asset aziendali. Si tratta dell'attività di gestione degli asset che ne garantisca integrità e adeguatezza con riferimento agli aspetti di salute e sicurezza.

- x) Attività di monitoraggio. Si tratta della gestione dell'attività di monitoraggio sistemico e continuo dei dati e indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il sistema e dell'implementazione delle eventuali azioni correttive.
- xi) Doveri dei lavoratori e degli utenti della Scuola e della Boarding School. Si tratta della definizione dei principali doveri dei in tema di salute e sicurezza in merito allo specifico ruolo svolto in azienda e/o alla specifica condizione personale (ad esempio, minorenni, portatori di handicap ecc.).

Per i reati colposi in esame, quanto ai *criteri oggettivi di imputazione* della responsabilità all'ente, si rileva che ai sensi dell'art. 5 del Decreto, i reati-presupposto sono riferibili a WINS solo se commessi nel suo interesse o a suo vantaggio. Si tratta, per esempio, del caso di un *risparmio* realizzato dalla Società nell'evitare di conformarsi alla norma prevenzionistica.

In merito al *criterio di imputazione soggettiva*, l'adozione del Modello secondo quanto previsto dal Decreto, mantiene la propria funzione esimente della responsabilità della Società (occorre cioè dimostrare l'adozione del Modello, la sua idoneità preventiva e che la sua violazione non è dipesa da un difetto di controllo e di vigilanza).

L'art. 30 del D.lgs. n. 81/2008 (*Testo Unico in materia di salute e sicurezza del lavoro*) stabilisce che il menzionato Modello sia idoneo ad avere efficacia esimente della responsabilità amministrativa, adottato ed efficacemente attuato, deve assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici individuati dalla norma relativi al rispetto degli standard tecnico-strutturali di legge sui luoghi di lavoro, alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione, alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione di eventuali appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza, alle attività di sorveglianza sanitaria, alle attività di informazione e formazione dei lavoratori, alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori, all'acquisizione di documentazioni e certificazioni obbligatorie di legge, alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate. Inoltre ai fini del rispetto della normativa sulla sicurezza, è necessario che il Modello preveda idonei sistemi di registrazione dell'avvenuta effettuazione delle menzionate attività e, compatibilmente con la natura, le dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicurino le competenze tecniche e i poteri necessari per la verifica, la

valutazione, la gestione ed il controllo del rischio in materia con un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni ed all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico, sulla base dell'evoluzione della legislazione, dei rischi per la salute e la sicurezza, della consultazione ed il coinvolgimento dei lavoratori.

WINS ha adottato un Documento di Valutazione Dei Rischi (di seguito il "DUVRI") al cui contenuto interamente si rimanda per la specificazione delle procedure seguite. Esso è disponibile in formato digitale e in formato cartaceo e a disposizione degli studenti del personale interno ed esterno.

Il DUVRI è redatto secondo il D.lgs. 81/2008 e deve essere aggiornato come da disposizioni legislative.

La figura che assicura e verifica che siano recepite e applicate le norme cogenti e volontarie che garantiscono la qualità e la sicurezza degli spazi, delle attrezzature e degli strumenti relativamente è il Responsabile del servizio prevenzione e protezione (di seguito il "RSPP"), i cui compiti specifici sono riportati nello stesso DUVRI.

Attraverso l'informazione e la formazione periodica nonché gli aggiornamenti annuali, il personale è edotto dei rischi connessi all'attività lavorativa, al possibile sviluppo d'incendio, sull'uso dei dispositivi di spegnimento, delle disposizioni relative all'evacuazione dei locali. Sono attivati incontri di informazione e formazione relativi agli interventi e all'uso della cassetta di primo soccorso.

## SEZIONE “F”

### 1.1 Delitti in materia ricettazione, riciclaggio ed autoriciclaggio

### 1.2 Le fattispecie rilevanti e i criteri di imputazione (*ex art. 25-octies, D.lgs. 231/2001*)<sup>33</sup>

L'art. 25-*octies* del D.lgs. n. 231/2001 contempla un complesso di fattispecie che possono determinare per la Società fonte di responsabilità amministrativa, in particolare con riferimento ai reati di ricettazione (*ex art. 648 c.p.*), al reato di riciclaggio (*ex art. 648-bis c.p.*), all'impiego di denaro, beni o utilità di provenienza illecita (*ex art. 648-ter c.p.*) ed il reato di autoriciclaggio inserito con L. 186/2014 e modificato da ultimo con il D.lgs. 90/2017 (*ex art. 648-ter 1 c.p.*). Si riportano di seguito i riferimenti normativi delle fattispecie rilevanti, relative alle attività svolte dal WINS ed ascrivibili nella categoria delle “attività sensibili”, per le quali la Società, pone in essere una specifica attività di controllo, in accordo a quanto previsto dal Decreto, riportando altresì una descrizione sintetica di alcuni aspetti significativi per ciascuno dei reati presupposti contemplati nelle citate disposizioni. Si precisa, tuttavia, che WINS si impegna ad adottare protocolli specifici per il controllo dei flussi finanziari con specifico riferimento alle modalità di pagamento effettuate dalla Società nei confronti di fornitori, soci, dipendenti, nonché quelli ricevuti dalle famiglie per la formazione e/o l'organizzazione di attività scolastiche, extra-scolastiche e relative alla Boarding School. I protocolli dovranno sempre prevedere, la segregazione dei compiti fra le funzioni coinvolte nel processo.

WINS adotta tutte le misure necessarie per favorire l'utilizzo di pagamenti tracciati, con l'esclusione di utilizzo dei pagamenti in contanti o con strumenti di pagamento analoghi, fatto salvo l'ambito di applicazione della procedura per la piccola cassa e le somme consentite dalla legge, per le quali non vige il divieto di utilizzo del contante.

#### 1.2.1 Ricettazione – Art. 648 c.p.

La disposizione contenuta nell'art. 648 c.p., richiamata nell'art. 25-*octies* del D.lgs. 231/2001, prende in esame la condotta da chiunque commessa consistente nell'utilizzo di denaro o cose provenienti da altri illeciti per scopi fraudolenti, quali il proprio o di latro ingiusto profitto. WINS attenziona che sia rispettato il contenuto di detta disposizione e che siano posti in essere

---

<sup>33</sup> Articolo inserito dall' art. 63 del D.lgs. 21 novembre 2007, n. 231, successivamente modificato dall'articolo 3, comma 5, lettera b), della Legge 15 dicembre 2014, n. 186 e da ultimo sostituito dall'art. 72, co. 3, del D.lgs. 21 novembre 2007, n. 231, come modificato dall'art. 5, co. 1, del D.lgs. 25 maggio 2017, n. 90

gli opportuni controlli. Si riporta il contenuto della norma, precisando che la stessa si applica anche ai casi in cui l'autore del delitto, non è imputabile<sup>34</sup> o non è punibile nonché manchi una condizione di procedibilità.

Si riporta il contenuto della norma:

*“Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da 516 euro a 10.329 euro. La pena è aumentata quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata ai sensi dell'articolo 628, terzo comma, di estorsione aggravata ai sensi dell'articolo 629, secondo comma, ovvero di furto aggravato ai sensi dell'articolo 625, primo comma, n. 7-bis) (co.1). La pena è della reclusione sino a sei anni e della multa sino a 516 euro, se il fatto è di particolare tenuità (co.2). Le disposizioni di questo articolo si applicano anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto (co.3).”*

### **1.2.2 Riciclaggio – Art. 648-bis c.p.**

La disposizione contenuta nell'art. 648-bis c.p., richiamata nell'art. 25-octies del D.lgs. 231/2001, prende in esame la figura delittuosa del riciclaggio di denaro o di altre utilità, proventi di altro illecito (non colposo). La norma contempla la pena della reclusione, oltre alla multa fino ad un massimo di Euro 25.000 per chi sostituisce o trasferisce detti proventi in modo da ostacolare l'identificazione della loro origine illecita, salvo che l'ipotesi di correatità nel reato, che la norma esclude con previsione di altra disciplina.

WINS garantisce che sia rispettato il contenuto di detta disposizione e che vi siano in essa gli opportuni controlli per evitare responsabilità dell'Ente.

Si riporta il contenuto della norma, precisando che la norma è stata oggetto di una modifica recente con la L. 186/2014<sup>35</sup>, che ha incrementati la multa, prima “da Euro 1.032 ad Euro 15.493” con l'attuale previsione “da Euro 5.000 ad Euro 25.000”:

*“Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da 5.000 euro a 25.000 euro (co.1). La pena è aumentata [64] quando il fatto è commesso nell'esercizio di un'attività*

---

<sup>34</sup> Ai sensi dell'art. 97 c.p. rubricato “Minore degli anni quattordici”, non è imputabile anche il soggetto che, nel momento in cui ha commesso il fatto, non aveva gli anni quattordici.

<sup>35</sup> La L. 15 dicembre 2014, n. 186, ha sostituito le parole «1.032 euro a 15.493» con le parole: «5.000 euro a 25.000».



*professionale (co.2) La pena è diminuita [65] se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni (co.3). Si applica l'ultimo comma dell'articolo 648<sup>36</sup> (co.4)».*

### **1.2.3 Impiego di denaro, beni o utilità di provenienza illecita – Art. 648-ter c.p.**

La disposizione contenuta nell'art. 648-ter c.p., richiamata nell'art. 25-*octies* del D.lgs. 231/2001, è stata inserita nel codice penale dalla L. 55/1990<sup>37</sup>, poi modificata da successive norme e da ultimo dalla L. 186/2014<sup>38</sup> e prende in esame la figura delittuosa dell'impiego di denaro o beni o utilità di provenienza illecita, come figura residuale di illecito, al di fuori dei casi contemplati negli artt. 648 e 648-*bis* c.p., come si legge nella norma di seguito riportata. L'impiego di detti proventi illeciti ex lege deve essere destinata in attività economiche o finanziarie; la sanzione comminata per detto illecito oltre a quella della reclusione è la medesima contemplata per le fattispecie principali (i.e. art. 648 e 648-*bis* c.p.) da quattro a dodici anni, salvo i casi di diminuzione di pena previsti dal secondo comma dell'art. 648 c.p. Si riporta di seguito il contenuto della disposizione e si precisa che WINS pone in essere tutti gli opportuni controlli per escludere che via siano condotte non conformi a tale disposizione, da parte delle figure apicali e di tutti soggetti che siano chiamati a svolgere attività di controllo a riguardo. Questi ultimi sono tenuti a monitorare costantemente tutte le operazioni finanziarie ed economiche, nonché a segnalare le operazioni sospette all'O.d.V., anche al fine delle modifiche da apportare al presente Modello, laddove necessarie.

*“Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da 5.000 euro a 25.000 euro (co.1). La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale (co.2). La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648 (co.3). Si applica l'ultimo comma dell'articolo 648 (co.4)».*

---

<sup>36</sup> Si veda art. 648 c.p. “Ricettazione”, di cui alla pagina precedente del presente documento.

<sup>37</sup> Articolo inserito dall'art. 24, L. 19 marzo 1990, n. 55 e successivamente sostituito dall'art. 5 L. 9 agosto 1993, n. 328.

<sup>38</sup> L'art. 3, comma 2, L. 15 dicembre 2014, n. 186, ha sostituito le parole dell'art. 648-ter, comma 1, da Euro “Euro 1.032 ad Euro 15.493” con le parole: «Euro 5.000 ad Euro 25.000».

### 1.2.3 Autoriciclaggio – Art. 648-ter.1 c.p.

La disposizione contenuta nell'art. 648-ter.1 c.p., richiamata nell'art. 25-octies del D.lgs. 231/2001, è stata inserita nel codice penale con l'art. 3 della L. 186/2014, che ha rubricato l'attività di occultamento dei proventi derivanti da propri crimini, sotto la rubrica di “Autoriciclaggio”. Detta figura di illecito si riscontra tipicamente a seguito della commissione di altri reati, come ad esempio il reato di evasione fiscale, di corruzione o di appropriazione di beni sociali, da cui derivino denaro, beni o altre attività che il reo, con l'intenzione di ostacolare concretamente l'identificazione della loro provenienza illecita, li rimpiega in attività economiche, finanziarie, imprenditoriali o di tipo speculative. Tuttavia, al di fuori di quanto contemplato nei primi tre commi della presente disposizione, come di seguito riportato, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale. Infine, sul piano sanzionatorio, la pena contemplata per tale *crimen*, è quella della reclusione da due ad otto anni, salvo riduzioni o incrementi (*ex art. 648-ter.1 co.5 e co.6*) e della multa da Euro 5000 ad Euro 25.000, salvo che se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni, per cui la reclusione è diminuita da uno a quattro anni e la multa è dimezzata nel *minum* e nel *maximum*.

WINS adotta tutte le misure necessarie al controllo delle operazioni interne e che le condotte di ciascun utente, nonché delle figure apicali, sia tale da non costituire fonte di responsabilità per essa, anche in relazione al reato in parola. Gli organi preposti al controllo sono tenuti a comunicare tempestivamente la necessità di implementare le misure di prevenzione di detto reato, per le finalità previste dal D.lgs. 231/2001.

Si riporta di seguito il contenuto della disposizione in esame:

*“Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa (co.1). Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni (co.2). Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio*

*1991, n. 203, e successive modificazioni (co.3). Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale (co.4). La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale (co.5) La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto (co.6). Si applica l'ultimo comma dell'articolo 648 (co.7)”*

## SEZIONE “G”

### 1. Delitti in materia di violazione del diritto d'autore

#### 1.1 Le fattispecie rilevanti e i criteri di imputazione (*ex art. 25-novies, D.lgs. 231/2001*)<sup>39</sup>

Si riportano di seguito i riferimenti normativi delle fattispecie rilevanti ed una descrizione sintetica di alcuni aspetti significativi per i reati presupposto rientranti nelle violazioni del diritto d'autore, che ai sensi del D.lgs. 231/2001 costituiscono nell'attività svolta da WINS un'area sensibile da sottoporre all'attenzione delle figure apicali, in conformità a quanto prescritto ex art. 5 del detto Decreto. La Legge n. 99 del 2009 ha inserito tra i reati presupposto una serie di fattispecie contenute nella c.d. “*legge sul diritto d'autore*” (L. 633/1941). Il nuovo articolo 25-novies prevede per l'ente sanzioni pecuniarie e sanzioni interdittive per la durata massima di un anno. Si analizziamo di seguito le fattispecie previste dal nuovo art. 25-novies del Decreto, che costituiscono oggetto di interesse della WINS come “area sensibile” ai fini della normativa in esame.

##### 1.1.1 Art. 171 co. I lett. a bis) e co. III

Delle numerose norme contenute nell'art. 171 della L. 633/1941, vengono inseriti come reati presupposto solo la lettera *a)-bis* del primo comma e il terzo comma del detto articolo, come di seguito riportati. Per la **lettera a-bis)** <sup>40</sup>**del primo comma:**

*“Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter, è punito con la multa da lire 100.000<sup>41</sup> a lire 4.000.000<sup>42</sup> chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma 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”.*<sup>43</sup> Il delitto punisce la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa. In questa norma ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete. Anche WINS,

---

<sup>39</sup> Disposizione inserita dall'art. 15, co.7, lettera c), della L. 23 luglio 2009, n.99.

<sup>40</sup> Lettera aggiunta dall'art. 3, comma 3-ter, del D.L. 31 gennaio 2005, n. 7 .

<sup>41</sup> Ammontare espresso in lire come da lettera della norma, da convertire nella valuta vigente.

<sup>42</sup> Ammontare espresso in lire come da lettera della norma, da convertire nella valuta vigente.

<sup>43</sup> Si noti che ai sensi dell'art. 171, co.2, L. 633/1941 “*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*”. La detta disposizione è stata aggiunta dall'art. 3, comma 3-quater, del D.L. 31 gennaio 2005, n. 7.”

in qualità di Ente formativo deve preservare la tutela delle menzionate opere da parte degli utenti e dare agli studenti l'opportuna informazione a riguardo. L'inserimento, infatti, del delitto *de quo* nel D.lgs. 231/2001 risponde ad una visione di responsabilizzazione di tutte quelle aziende che gestiscono o si avvalgono di piattaforme digitali o *servers* attraverso cui si mettono a disposizione del pubblico (in particolare studenti) opere protette da diritto d'autore. WINS, per contenere il rischio di tale reato, dovrà predisporre controlli più accurati sui contenuti che "transitano" sul proprio server e sulle piattaforme digitali utilizzate per l'erogazione dei servizi didattici. Ciò, a stretto rigore, anche qualora siano gli utenti stessi a pubblicare (atecnicamente il c.d. "postare") contenuti direttamente sulla piattaforma interna didattica e forzando i sistemi di filtro preventivo da parte del "Gestore della Rete e della sicurezza informatica", soggetto nominato per svolgere tale tipologia di controllo. Nei detti casi, WINS per evitare che si configuri una responsabilità per essa stessa, deve porre in essere tutte le misure necessarie per prevenire tale rischio di reato, pena la rilevanza giuridica ai fini del Decreto, della sua condotta (attraverso le figure apicali – *criterio rappresentanza organica dell'Ente attraverso l'azione di persone fisiche*).

Inoltre, invece, il delitto di cui al comma 3 dell'art. 171 L. 633/1941, punisce le condotte sopra menzionate ove commesse su una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera o con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore. Infatti, si legge dalla disposizione: *"La pena è della reclusione fino ad un anno o della multa non inferiore a lire 1.000.000<sup>44</sup> 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 (co.3).*

In quest'ultima fattispecie di danno il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera ma il suo onore e la sua reputazione, per tale ragione diversa è la sanzione applicabile con la reclusione in luogo della sanzione pecuniaria. WINS adotta tutti gli opportuni controlli affinché sia garantito il rispetto della reputazione e dell'onore degli autori delle opere utilizzate dagli utenti di essa, perché sia arginata ogni forma di responsabilità in materia.

---

<sup>44</sup> Ammontare espresso in lire come da lettera della norma, da convertire nella valuta vigente.

### **1.1.2 Art. 171-bis**

La presente disposizione prende in considerazione nell'ambito dei delitti in materia di violazione del diritto di autore, una delle fattispecie incluse nell'art. 25-*novies* D.lgs. 231/2001, relativa ai contenuti in supporti non contrassegnati dalla S.I.A.E. (Società Italiana degli autori ed editori, di seguito "SIAE") ed all'utilizzo illecito di banche dati. La WINS adotta tutte le procedure di controllo al fine di escludere una responsabilità della Scuola per i fatti di seguito contemplati:

*“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 a euro 15.493. 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 se il fatto è di rilevante gravità (co.1). Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-*quinqüies* e 64-*sexies*, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter*, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità (co.2).*

### **1.1.3 Art. 171-ter**

La lunga disposizione di seguito, nell'ambito dei delitti in materia di violazione del diritto di autore, richiamati nell'art. 25-*novies* D.lgs. 231/2001, ha come scopo precipuo quello della tutela di una serie numerosa di opere dell'ingegno, quali:

- opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali;
- opere letterarie, scientifiche o didattiche.

Le numerose condotte sanzionate, che non vengono analizzate capillarmente per ragioni di sintesi del Modello, evitando che lo stesso possa perdere di efficacia vista la prolissità, si inseriscono, tuttavia, nell'ottica di una pretesa “penalizzazione” che il Legislatore negli ultimi

anni ha perseguito nei confronti della tutela del *software* e del diritto della proprietà intellettuale, più in generale. A restringere l'ambito di applicabilità della disposizione riportata di seguito, però, vi sono due requisiti. Il primo di essi prevede che le condotte per essere penalmente rilevanti, siano poste in essere per fare un uso non personale dell'opera dell'ingegno; il secondo requisito necessario è per l'elemento psicologico della condotta illecita che via sia dolo specifico ovvero l'intento specifico di lucrare; quest'ultimo requisito è necessario per integrare il fatto tipico. A seguito della novella di cui alla Legge 179 del 2009, ha inasprito l'esposizione delle Società al rischio di violazione delle norme contemplate nell'art. 171-ter della L.633/1941, pertanto la stessa WINS pone in essere tutte le misure necessarie ai controlli da parte delle figure di vertice nonché all'idonea formazione del personale perché non siano poste in essere condotte penalmente rilevanti per l'Ente stesso ai sensi del Decreto.

Dal primo comma dell'art. 171-ter della L. 633/1941 emerge che:

*‘È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:*

- a) Abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;*
- b) Abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;*
- c) Pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);*
- d) Detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;*

e) *In assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;*

f) *Introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;*

*f-bis)<sup>45</sup> fabbrica, importa distribuisce, vende noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-  
quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;*

*<sup>46</sup>g) Abusivamente rimuove o altera le informazioni elettroniche di cui all'art. 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (co.1).”*

Per il secondo comma:

*È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:*

a) *Riproduce, duplica trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;*

*a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche,*

*mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;*

b) *Esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;*

c) *Promuove o organizza attività illecite di cui al comma 1.*

---

<sup>45</sup> Lettera inserita dall'art. 26, co. 2, del D.lgs. 9 aprile 2003, n. 68.

<sup>46</sup> Lettera inserita dall'art. 26, co. 2, del D.lgs. 9 aprile 2003, n. 68.



Infine la medesima norma, negli ultimi commi (co.3 e co.4), indica una causa di non punibilità dell'Ente, ovvero il caso in cui il fatto commesso sia caratterizzato dalla qualificazione di "particolare tenuità". Ai casi punibili, per le pene applicabili, il quarto comma dell'art. 171-ter, come di seguito riportato, contempla per gli illeciti indicati primo comma, oltre alla sanzione pecuniaria, le pene accessorie *ex artt.* 30 e 32 c.p., l'applicabilità della sanzione della pubblicazione della sentenza sui giornali di rilievo nazionale ed eventuali sanzioni inibitorie con sospensione dei servizi di radiodiffusione.

Per il **terzo comma**:

*"La pena è diminuita se il fatto è di particolare tenuità (co.3)"*

Per il **quarto comma**:

*"La condanna per uno dei reati previsti nel comma 1 comporta:*

- a) L'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;*
- b) La pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale<sup>47</sup>;*
- c) La sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale (co.4).*

Per il **quinto comma**:

*"Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici. (co.5)".*

#### **1.1.4 Art. 171-septies**

La disposizione in esame è posta a tutela delle funzioni di controllo della SIAE, in un'ottica di *tutela anticipata* del diritto d'autore. Si tratta, pertanto, di un reato di ostacolo che si consuma con la mera violazione dell'obbligo. La disposizione estende la pena prevista all'art. 171-ter della L. 633/1941, comma primo, anche ai produttori e agli importatori dei supporti non soggetti al contrassegno SIAE, che non comunichino alla stessa entro trenta giorni dall'importazione o dalla commercializzazione i dati necessari all'univoca identificazione dei supporti "importati o acquistati per scopi commerciali" non soggetti al contrassegno SIAE (*ex art 181-bis L.633/1941*). Il secondo comma, invece, punisce una diversa fattispecie, ovvero, la falsa comunicazione alla SIAE dei dati menzionati. Pertanto, il Legislatore richiamando la

---

<sup>47</sup> Lettera sostituita dall'art. 2, co. 217, della Legge 23 dicembre 2009, n. 191.

disposizione dell'art. 171-*septies*, con l'art. 25-*novies*, ha voluto accordare anche con il D.lgs. 231/2001 un rilievo alle funzioni di vigilanza delle Autorità preposte al controllo del settore. Nell'ottica di tale normativa, la WINS dovrà implementare nel Modello specifiche misure volte a regolamentare lo scambio informativo con la SIAE, laddove necessarie per l'importazione di supporti non soggetti al contrassegno.

Di seguito la disposizione in esame:

*“La pena di cui all'articolo 171-ter, comma 1, si applica anche:*

*a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;*

*b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge (co.1).*

#### **1.1.5 Art. 171-octies**

La disposizione in esame, richiamata dall'art. 25-*novies* del D.lgs. 231/2001, contenuta nella norma istitutiva della tutela del diritto d'autore (L. 633/1941) introduce la responsabilità di colui il quale, a fini fraudolenti, produce, pone in vendita, promuove, installa, modifica o utilizza per uso pubblico o privato, apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato, da intendersi come possibilità di accedere ai segnali audiovisivi trasmessi da emittenti italiane o estere in forma esclusiva per gruppi chiusi di utenti selezionati dal soggetto erogante il segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio. Tuttavia, vale a restringere l'ambito di applicabilità della norma l'elemento soggettivo della condotta penalmente rilevante, ovvero la presenza di dolo specifico che si sostanzia nel perseguimento di fini fraudolenti.

La WINS dovrà implementare nel Modello adottato, di volta in volta, le misure necessarie, per il rispetto del contenuto della disposizione seguente:

*“Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 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. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio (co.1).*

*La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità (co.2)<sup>48</sup>”.*

## **2. Miscellanee Scuola - Diritto d'autore**

WINS intende richiamare in modo schematico talune attività soggette a limitazioni che possano nel corso della sua attività determinare per gli utenti, studenti e personale interno ipotesi di responsabilità per l'Ente stesso. Al fine di escludere ciò, WINS per i destinatari di tale Modello intende precisare taluni aspetti, che ricoprono anche un importante rilievo pratico

### **Fotocopie - Limite del 15%**

La Legge del 18 agosto 2000, n.248, che integra e modifica la Legge sul diritto d'autore, contiene alcune disposizioni che disciplinano la reprografia, cioè la riproduzione delle opere dell'ingegno mediante fotocopia, xerocopia o simili. La normativa riguarda le opere protette dalla legge sul diritto d'autore (cioè le opere di natura creativa che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro, alla cinematografia), per tutta la vita dell'autore e fino al 31 dicembre del 70° anno dopo la sua morte. Trascorso tale termine l'opera è considerata di pubblico dominio e può essere riprodotta liberamente. La Legge consente la fotocopia di opere protette ma solo "per uso personale" e nel limite massimo del 15% di ciascun volume o fascicolo di periodico, escluse le pagine di pubblicità. La riproduzione "per uso personale" è quella che può essere effettuata per propri scopi di lettura, studio, consultazione e non per uso commerciale o per trarre altre copie da distribuire ad altri, a pagamento o anche gratuitamente. E' comunque esclusa ogni utilizzazione fatta in concorrenza con i diritti di utilizzazione economica spettanti all'autore. La riproduzione, invece, di alcune pagine di un testo, non rientranti nella nozione di "uso personale" per essere lecito implicherà, in quanto non autorizzato dalla legge, la necessità della stipula di un accordo specifico tra l'editore e la Scuola. Al di fuori di tali accordi, resi pubblici se esistenti, non sarà

---

<sup>48</sup> Si rammenta che in merito alla detta disposizione ed alla sanzione applicabile, la Corte costituzionale, con sentenza 29 dicembre 2004, n. 426, ha dichiarato l'illegittimità costituzionale del presente articolo, nella parte in cui, limitatamente ai fatti commessi dall'entrata in vigore del presente articolo fino all'entrata in vigore della legge 7 febbraio 2003, n. 22 (*Modifica al D.lgs.15 novembre 2000, n. 373, in tema di tutela del diritto d'autore*), punisce con sanzione penale, in luogo di sanzione amministrativa prevista dall'art. 6 del D.lgs.15 novembre 2000, n. 373 (*Attuazione della direttiva 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato*), l'utilizzazione per uso privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

ammessa la duplicazione per “uso non personale”. Pertanto, la WINS ed i suoi utenti sono autorizzati alle riproduzioni in copia, solo per fini personali, avendo riguardo del menzionato limite e per i quali controlli sarà preposto il personale amministrativo interno, che fornirà ciascuno di card in cui vengano tracciate quantità di copie effettuate e dati dell’utente.

La Scuola adotta tutte le misure necessarie per evitare che all’interno della propria struttura vi siano condotte non conformi alla disciplina a tutela del diritto d’autore.

## **Opere protette**

La riproduzione tramite fotocopiatura è soggetta alla disciplina sul diritto d’autore prevista dalla legge n.633/41 e successive modifiche.

Tale norma si applica a tutte le opere protette, dato il loro carattere creativo, di cui di seguito si riporta a titolo esemplificativo un’elencazione:

- le opere letterarie, scientifiche, didattiche e religiose;
- le opere drammatiche;
- le opere musicali;
- le opere liriche;
- le opere coreografiche, pantomimiche;
- le opere della scultura, della pittura, dell’arte del disegno;
- i programmi per elaboratore;
- le elaborazioni di carattere creativo dell’opera originale;
- le opere fotografiche;
- i disegni e le opere dell’architettura;
- le banche di dati;
- il disegno industriale;
- le opere collettive (riviste e giornali).

WINS adotta tutte le misure necessarie affinché nella riproduzione di tali opere siano rispettate le norme vigenti, con l’adozione di protocolli interni che possa essere di volta in volta implementati, laddove necessario, per escludere la responsabilità ex D.lgs. 231/2001.



## **Materiale didattico**

Il materiale didattico distribuito dalla Scuola e nella stessa deve avere le autorizzazioni rilasciate dagli aventi diritto (autori ed editori) e non da altri soggetti privo dello stesso (es. gli insegnanti, la scuola, etc.). Le carte geografiche, se fanno parte di un volume o di un fascicolo di periodico, possono essere riprodotte, anch'esse nel limite del 15%, previo pagamento dei diritti. Quest'ultime non sono liberamente riproducibili, se non fanno parte di un volume o di un periodico.

Milano, 1 settembre 2017

Amministratore Unico

***Dottor Pietro Paolo Formiga***