



## **CENTRO STUDI CITTÀ DI FOLIGNO**

### **PARTE SPECIALE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D. Lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni**

Approvato dal Consiglio di Amministrazione in data 28/02/2018

Tutti i cambiamenti devono essere sottoposti all'approvazione del Consiglio di Amministrazione (C.d.A.) ed al controllo dell'Organismo di Vigilanza (O.d.V.)

# INDICE

1. PREMESSA ALLA PARTE SPECIALE .....	4
2. FINALITA' .....	5
3. IL SISTEMA DEI CONTROLLI SULLE ATTIVITÀ .....	7
3.1. STANDARD DI CONTROLLO GENERALI .....	7
3.2. STANDARD DI CONTROLLO SPECIFICI .....	8
PARTE SPECIALE – A .....	9
I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE .....	9
E DI CORRUZIONE TRA PRIVATI .....	9
1. AMBITO APPLICATIVO ED OBIETTIVI SPECIFICI .....	9
2. I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE .....	10
2.1. CONCETTO DI PUBBLICA AMMINISTRAZIONE, PUBBLICO UFFICIALE ED INCARICATO DI PUBBLICO SERVIZIO .....	10
2.2. LE FATTISPECIE DI REATO CONTRO LA PUBBLICA AMMINISTRAZIONE PREVISTE DAL D. LGS. 231/2001 .....	12
3. I REATI DI CORRUZIONE TRA PRIVATI (artt. 2635, comma 3, e 2635-bis c.c.) .....	20
4. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI AI FINI DELLA COMMISSIONE DEI REATI ESAMINATI .....	22
5. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE .....	26
5.1. OBBLIGHI .....	27
5.2. DIVIETI PER I REATI CONTRO LA pubblica amministrazione .....	28
5.3. DIVIETI PER I REATI DI CORRUZIONE TRA PRIVATI .....	29
5.4. DOVERI DI CONDOTTA .....	30
6. PRINCIPI PROCEDURALI SPECIFICI .....	31
6.1. IL RESPONSABILE INTERNO .....	31
6.2. RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE .....	32
6.3. IDONEITÀ DEI SOGGETTI CHE INTRATTENGONO RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E PRINCIPI DI INTERAZIONE .....	32
6.4. RAPPORTI CON SOGGETTI PRIVATI .....	33
7. I CONTROLLI DELL'ORGANISMO DI VIGILANZA .....	34
8. MODIFICHE ED AGGIORNAMENTI DELLA PRESENTE PARTE SPECIALE .....	35
PARTE SPECIALE – B .....	35
DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI .....	35



1. PREMESSA.....	35
1.1. LE FATTISPECIE RILEVANTI DEI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI (ART. 24 BIS DEL D. LGS. 231/2001) .....	36
2. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI NELL’AMBITO DEI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI.....	45
3. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE .....	46
3.1. OBBLIGHI.....	46
3.2. DIVIETI .....	47
3.3. DOVERI DI CONDOTTA .....	49
3.4. PRINCIPI PROCEDURALI SPECIFICI .....	50
4. I CONTROLLI DELL’ORGANISMO DI VIGILANZA.....	54
5. MODIFICHE ED AGGIORNAMENTI DELLA PRESENTE PARTE SPECIALE.....	55
PARTE SPECIALE – C.....	56
DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D’AUTORE.....	56
1. LE FATTISPECIE RILEVANTI DEI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D’AUTORE (ART. 25-NONIES DEL D. LGS.231/2001) .....	56
2. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI NELL’AMBITO DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D’AUTORE.....	70
3. PRINCIPI DI COMPORTAMENTO .....	71
3.1. OBBLIGHI.....	71
3.2. DIVIETI .....	72
3.3. DOVERI DI CONDOTTA .....	73
3.4. PRINCIPI PROCEDURALI SPECIFICI .....	74
4. I CONTROLLI DELL’ORGANISMO DI VIGILANZA.....	76
5. MODIFICHE ED AGGIORNAMENTI DELLA PRESENTE PARTE SPECIALE.....	77



## 1. PREMESSA ALLA PARTE SPECIALE

Nella struttura del presente Modello Organizzativo del Centro Studi Città di Foligno si distinguono una “Parte Generale” – attinente all’organizzazione dell’Associazione nel suo complesso, al progetto per la realizzazione del Modello, all’Organismo di Vigilanza, al sistema disciplinare, alle modalità di formazione e di comunicazione – e la “Parte Speciale”, che riguarda l’applicazione nel dettaglio dei principi richiamati nella “Parte Generale” con riferimento alle fattispecie di reato richiamate dal D.Lgs. n. 231/2001 che l’Associazione ha stabilito di prendere in considerazione in ragione delle caratteristiche della propria attività.

Nelle “Parti Speciali” che seguono sono analizzati rispettivamente:

- Parte Speciale “A” – Reati nei rapporti con la Pubblica Amministrazione e di corruzione tra privati
- Parte Speciale “B” – Delitti informatici e di trattamento illecito dei dati
- Parte Speciale “C” – Delitti in materia di violazione del diritto d’autore.

In considerazione dell’analisi del contesto dell’Associazione, dell’attività svolta e delle aree potenzialmente soggette a rischio-reato, sono stati considerati rilevanti e quindi specificamente esaminati nel Modello, solo gli illeciti oggetto di specifica trattazione nella presente Parte Speciale.

Con riferimento agli altri “reati presupposto” della responsabilità amministrativa degli Enti ai sensi del Decreto (ad esempio reati contro la fede pubblica ex art. 25-bis del D. Lgs. 231/2001<sup>1</sup> o delitti contro la vita e l’incolumità individuale ex art. 25-quater.1 del d.lgs. 231/01<sup>2</sup>) è stato valutato dall’Associazione, che il rischio è solo astrattamente e non concretamente ipotizzabile e che, in ogni caso, gli strumenti di controllo approntati per prevenire i reati sopra evidenziati, sulla base

---

<sup>1</sup> Nello specifico si fa riferimento ai seguenti reati: reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.), alterazione di monete (art. 454 c.p.), spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.), spendita di monete falsificate ricevute in buona fede (art. 457 c.p.), falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.), contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.), fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.), uso di valori di bollo contraffatti o alterati (art. 464 c.p.).

<sup>2</sup> Nello specifico si fa riferimento al reato di Pratiche di mutilazione degli organi genitali femminili (art 583-bis c.p.)



dell'analisi effettuata, possono costituire, unitamente al rispetto del Codice Etico e delle disposizioni legislative vigenti, un presidio anche per la prevenzione di tali reati.

Ogni Parte Speciale è composta necessariamente dai seguenti paragrafi:

- il primo è dedicato alla descrizione delle “Fattispecie rilevanti” e contiene l’indicazione e la descrizione dei “reati presupposto” oggetto della Parte Speciale;
- un secondo paragrafo è volto alla “Identificazione delle attività sensibili”. Attraverso l’analisi dei rischi, svolta in conformità a quanto prescritto dall’art. 6, comma 2 lettera a) del D. Lgs. 231/2001, si sono evidenziate le attività dell’Associazione coinvolte in processi astrattamente esposti al rischio di commissione di fatti rilevanti ai sensi del Decreto. Nel paragrafo vengono quindi indicate le attività sensibili, al fine di chiarire quali sono gli ambiti di attività nei quali è più alto il rischio di commissione per il gruppo di reati di riferimento;
- un terzo paragrafo contiene le indicazioni relative ai “Principi di comportamento”. I “Principi di comportamento” sono volti a richiamare l’osservanza del Codice Etico, nonché a specificare le regole di condotta che devono ispirare il comportamento dei destinatari del Modello al fine di prevenire la commissione dei singoli gruppi di reati. Essi comprendono anche obblighi, divieti e doveri di condotta.
- Un quarto paragrafo evidenzia i “Principi procedurali specifici” dando atto degli standard di controllo che dovranno essere applicati.

A tali paragrafi sono stati aggiunti, a seconda delle necessità derivanti dalle fattispecie considerate, ulteriori approfondimenti opportuni per rendere la singola Parte Speciale più comprensibile, efficace e completa.

Ogni parte indica, infine, i controlli dell’organismo di vigilanza e le regole per le modifiche e gli aggiornamenti.

## **2. FINALITA’**

La struttura del Modello con la previsione di una “Parte Speciale” suddivisa in più sezioni consente di individuare, nell’ambito di ciascuna delle macro-aree elaborate con riferimento ai gruppi di illecito previsti dal D. Lgs. 231/2001 e da considerare peculiari rispetto all’Associazione, le attività sensibili alle quali vengono, in seguito, associati gli strumenti di controllo adottati per la prevenzione dei c.d. reati presupposto.



Sarà necessario il tempestivo aggiornamento del Modello, tramite eventuali opportune aggiunte, laddove il Legislatore intenda inserire ulteriori fattispecie penali rilevanti o qualora, in seguito allo svolgimento di nuove attività, vi siano nuovi settori di rischio di commissione dei reati previsti dal D. Lgs. 231/2001.

La “Parte Speciale” va messa in relazione con i principi contenuti nel Codice Etico che indirizzano i comportamenti dei destinatari, allo scopo di prevenire condotte scorrette o non in linea con le direttive dell’Associazione.

Gli strumenti di controllo individuati nel M.O.G. sono vincolanti per i destinatari del Modello e si sostanziano in obblighi di fare (il rispetto delle procedure e le segnalazioni agli Organi di Controllo) e in obblighi di non fare (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, l’Associazione reagirà applicando il sistema disciplinare e sanzionatorio descritto nella “Parte Generale” del M.O.G..

La Parte Speciale del M.O.G. ha lo scopo di:

1. individuare ed illustrare le fattispecie di reato presupposto incluse tra i reati contro la Pubblica Amministrazione e di corruzione tra privati per i quali, ricorrendo le condizioni previste dal Decreto, è prevista la responsabilità amministrativa in capo al Centro Studi Città di Foligno, ai sensi del D.Lgs 231/2001;
2. indicare i principi di comportamento generali e procedurali che gli Amministratori, gli eventuali dirigenti, i direttori ed i dipendenti, nonché i consulenti ed i partner esterni (compresi agenti, rappresentanti e fornitori) del Centro Studi Città di Foligno, nella misura in cui essi operino nell’ambito delle aree di attività sensibili per conto o nell’interesse dell’Associazione, sono chiamati a osservare ai fini della corretta applicazione del Modello;
3. fornire all’Organismo di Vigilanza ed ai responsabili delle funzioni dell’Associazione gli elementi di riferimento e gli strumenti esecutivi per l’esercizio delle attività di controllo, monitoraggio e verifica.

In linea generale, tutti gli interessati dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- M.O.G.;
- Codice Etico;
- Linee guida/procedure/regolamenti;



- Procure, deleghe e disposizioni organizzative;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del D. Lgs. 231/2001.

E' inoltre sempre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

### **3. IL SISTEMA DEI CONTROLLI SULLE ATTIVITÀ**

Il sistema dei controlli, previsto dall'Associazione Centro Studi Città di Foligno, anche sulla base delle indicazioni fornite dalle Linee guida di Confindustria, nonché delle "best practice" prevede, con riferimento alle Aree ed alle Attività Sensibili individuate:

- 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.

#### **3.1. STANDARD DI CONTROLLO GENERALI**

Gli standard di controllo di carattere generale, da considerare e applicare con riferimento a tutte le Attività Sensibili, sono i seguenti:

- segregazione delle funzioni/attività: si richiede il rispetto del principio della separazione delle funzioni tra chi autorizza, chi esegue e chi controlla;
- procedure: devono esistere all'interno dell'Associazione procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento di ogni attività sensibile nonché modalità di archiviazione della documentazione rilevante;
- poteri autorizzativi e di firma: i poteri autorizzativi e di firma, qualora riconosciuti a più di un soggetto all'interno dell'Associazione, dovranno:
  - 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 dell'Associazione.
- tracciabilità: ogni operazione relativa ad attività sensibili deve, ove possibile, essere adeguatamente registrata e archiviata. Il processo di decisione, autorizzazione e svolgimento delle attività sensibili deve essere verificabile ex post, anche tramite appositi supporti documentali. 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.

### **3.2. STANDARD DI CONTROLLO SPECIFICI**

Sulla base degli standard di controllo generali sopra riportati, gli standard di controllo specifici, che ai primi fanno riferimento, sono elaborati affinché:

- a) tutte le operazioni, la formazione e l'attuazione delle decisioni dell'Associazione rispondano ai principi ed alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Codice Etico e delle procedure interne;
- b) siano definite e adeguatamente comunicate le disposizioni interne idonee a fornire i principi di comportamento, le modalità operative per lo svolgimento delle attività sensibili nonché le modalità di archiviazione della documentazione rilevante;
- c) per tutte le operazioni:
  - siano formalizzate le responsabilità di gestione, coordinamento e controllo;
  - siano sempre documentabili e ricostruibili le fasi di formazione e autorizzazione degli atti, a garanzia della trasparenza delle scelte effettuate;
  - siano adeguatamente comunicati dall'Associazione i poteri di firma;
  - l'assegnazione e l'esercizio dei poteri sia coerente con le posizioni di responsabilità e con la rilevanza delle sottostanti operazioni economiche;
  - non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
  - l'accesso e l'intervento sui dati sensibili posseduti dall'Associazione sia consentito esclusivamente alle persone autorizzate in conformità al D. Lgs. 196/2003 e successive modifiche e 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, con modalità tali da non permetterne la modificazione successiva, se non dandone evidenza.



## **PARTE SPECIALE – A**

### **I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E DI CORRUZIONE TRA PRIVATI**

#### **1. AMBITO APPLICATIVO ED OBIETTIVI SPECIFICI**

La presente Parte Speciale è relativa alla prevenzione dei reati contro la Pubblica Amministrazione previsti dagli artt. 24 e 25 del D. Lgs. 231/2001 ed ai reati previsti dall'art. 25-ter del D. Lgs. 231/2001 di "Corruzione tra privati" (di cui all'art. 2635, comma 3, C.C. - così come riformulato



dalla L.190/2012 e dal D. Lgs. 38/2017) e di “Istigazione alla corruzione tra privati” di cui all’art. 2635-bis C.C. -inserito dal d.lgs. 38/2017-).

Si tratta, quindi, conformemente alle previsioni del D. Lgs. 231/2001, di reati compiuti da soggetti che ricoprono posizioni apicali nell’Associazione quali Amministratori, eventuali dirigenti e direttori, nonché dipendenti che, in ragione delle loro cariche o funzioni, sono entrati in contatto con Pubblici Ufficiali o Incaricati di Pubblico Servizio.

Anche i consulenti esterni, gli agenti, i rappresentanti ed in generale tutti coloro che svolgono attività in nome e per conto dell’Associazione che prevedono contatti con le Pubbliche Amministrazioni-intese in senso ampio- e con Enti privati, dovranno conformare il loro operato ai principi ed alle regole indicati nella presente parte speciale.

## **2. I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE**

Per poter esaminare i Reati contro la Pubblica Amministrazione e comprendere le relative fattispecie è necessario effettuare un breve approfondimento in merito a cosa si intenda in diritto penale per Pubblica Amministrazione, Pubblico Ufficiale ed Incaricato di Pubblico Servizio.

### **2.1. CONCETTO DI PUBBLICA AMMINISTRAZIONE, PUBBLICO UFFICIALE ED INCARICATO DI PUBBLICO SERVIZIO**

Il Codice Penale non dà una definizione di Pubblica Amministrazione.

In base a quanto stabilito nella Relazione Ministeriale al Codice Penale ed in relazione ai reati in esso previsti, per Pubblica Amministrazione deve intendersi l’insieme di Enti che “*svolgono tutte le attività dello Stato e gli altri Enti pubblici*” in cui rientrano, oltre a quelli italiani, anche gli Stati esteri e gli Organi Comunitari.

Secondo un’accezione prudenziale, la Pubblica Amministrazione si articola essenzialmente in: Ministeri, Agenzie amministrative, Enti pubblici, Autorità Amministrative Indipendenti, strutture amministrative delle Regioni, delle Province, dei Comuni e delle Città Metropolitane<sup>3</sup>.

Adottando un’accezione estesa, per “Pubblica Amministrazione” si devono intendere anche quei soggetti che, sebbene presentino formalmente una natura privatistica, siano caratterizzati dalla veste pubblicistica dell’attività svolta ovvero dalla rilevante presenza di partecipazione da parte di soggetti pubblici.

---

<sup>3</sup> Così Enciclopedia Treccani alla voce “Pubblica Amministrazione”.



In linea generale, buona parte delle fattispecie incriminatrici richiamate dagli artt. 24 e 25 del Decreto sono configurate come “reati propri”, ovvero come reati che possono essere commessi soltanto da persone fisiche dotate di una determinata qualifica soggettiva. In tal senso, le figure che assumono rilevanza ai fini della commissione delle tipologie di reato in commento sono:

1. i Pubblici Ufficiali;
2. gli Incaricati di Pubblico Servizio.

Agli effetti della legge penale (art. 357, comma 1, del Codice Penale), sono considerati Pubblici Ufficiali coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa.

È funzione pubblica amministrativa quella disciplinata da norme di diritto pubblico e da atti autoritativi, attraverso la quale si forma e si manifesta la volontà della Pubblica Amministrazione, ovvero quella esercitata attraverso poteri autoritativi o certificativi<sup>4</sup>.

Ai sensi dell’art. 358 del Codice Penale, sono Incaricati di un Pubblico Servizio coloro i quali, a qualunque titolo, prestano un Pubblico Servizio, laddove, per “Pubblico Servizio” deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

A riguardo, al fine di segnare una linea di confine tra le due nozioni, la giurisprudenza della Suprema Corte<sup>5</sup> ha precisato che, ai fini del corretto inquadramento della figura del Pubblico

---

<sup>4</sup> Dalla lettura dell’art. 357 C.P. si evince che la qualifica di Pubblico Ufficiale va attribuita a tutti quei soggetti che concorrono a formare la volontà di una Pubblica Amministrazione. Si tratta dei soggetti muniti di poteri decisionali, di certificazione, di attestazione e di coazione. (in tal senso Cass. Pen. sentenza n. 148796/1981), nonché "di collaborazione anche saltuaria" (Cass. Pen. sentenza n. 166013/1984). La giurisprudenza ha avuto modo di chiarire, tuttavia, che è "irrelevante la qualifica formale della persona all'interno dell'Amministrazione" (Cass. Pen. sentenza n. 172198/1985) e che può essere considerato Pubblico Ufficiale anche "chi concorre in modo sussidiario o accessorio all'attuazione dei fini della Pubblica Amministrazione, con azioni che non possano essere isolate dal contesto delle funzioni pubbliche" (Cass. Pen. sentenza n. 172191/1985). Pertanto, "la qualifica di Pubblico Ufficiale, ai sensi dell'art. 357 C.P. (come modificato dalle Leggi 86/1990 e 181/1992), deve esser riconosciuta a quei soggetti che, pubblici dipendenti o semplici privati, possono e debbono - quale che sia la loro posizione soggettiva - formare e manifestare, nell'ambito di una potestà regolata dal diritto pubblico, la volontà della P.A., ovvero esercitare, indipendentemente da formali investiture, poteri autoritativi, deliberativi o certificativi, disgiuntamente e non cumulativamente considerati" (Cass. Pen. sentenza 7.6.2001; Cass. Pen. sentenza n. 191171/1992 e Cass. Pen. sentenza n. 213910/1999).

<sup>5</sup> Si segnalano in proposito alcune pronunce della Corte di Cassazione, la quale ha stabilito che:

➤ sono considerati Pubblici Ufficiali:

- tutti coloro che, nell’ambito di una potestà regolata dal diritto pubblico, possono e debbono formare e manifestare la volontà della Pubblica Amministrazione oppure esercitare, indipendentemente da formali investiture, poteri autorizzativi, deliberativi o certificativi (Cass. Pen., sez. un., 11.7.1992, n. 7598);
- gli operatori di istituti di credito - normalmente esclusi dall’ambito pubblico – per le attività svolte dai medesimi istituti nelle vesti di banche agenti o delegate dall’amministrazione finanziaria (Cass. Pen., sez. VI, 24.4.1997, n. 3882);
- gli organi amministrativi e il presidente di società privata concessionaria di autostrade, ovvero concessionaria dell’ANAS, in quanto dette società assolvono la funzione di protezione dell’interesse pubblico affidata originariamente all’Ente concedente (Cass. Pen., sez. III, 13.9.1993, n. 1806).



Ufficiale o dell'Incaricato di Pubblico Servizio, occorre verificare se la relativa attività svolta sia disciplinata da norme di diritto pubblico e sia volta al perseguimento di interessi pubblici o al soddisfacimento di bisogni di interesse generale, risultando, invece, irrilevanti sia la qualifica rivestita dal soggetto, che l'assetto formale dell'Ente presso il quale il soggetto presta la propria attività.

Peraltro, ai fini della realizzazione delle diverse fattispecie di reato, come tipizzate dal Legislatore, le figure di Pubblico Ufficiale e di Incaricato di Pubblico Servizio finiscono sostanzialmente per coincidere.

Posto quanto sopra, i destinatari del Modello devono prestare la massima attenzione nei rapporti, di qualsiasi tipo ed a qualsiasi livello, intrattenuti con Pubblici Ufficiali ed Incaricati di Pubblico Servizio.

## **2.2. LE FATTISPECIE DI REATO CONTRO LA PUBBLICA AMMINISTRAZIONE PREVISTE DAL D. LGS. 231/2001**

---

Ai fini della nozione di pubblico ufficiale, non rileva il rapporto di dipendenza del soggetto rispetto allo Stato o ad altro Ente Pubblico, ma è richiesto soltanto l'esercizio effettivo di una pubblica funzione. Tale deve essere considerata l'attività consistente nella acquisizione della prova di un fatto, imposta dall'ordinamento, come condizione necessaria per l'erogazione di un pubblico servizio (Cass. pen., sez. V, 16 gennaio 1997, n. 2036).

In materia di responsabilità degli amministratori (in senso lato) degli enti pubblici economici, occorre accertare, di volta in volta, se gli atti sono stati posti in essere nell'ambito della gestione privatistica dell'attività imprenditoriale ovvero quali indicazione di esercizio di poteri autoritativi, di autorganizzazione ovvero di funzioni pubbliche svolte in sostituzione dell'Amministrazione dello Stato o di pubbliche potestà (Cass. pen., sez. V, 14 maggio 1997, n. 7295).

➤ Sono considerati Incaricati di un Pubblico Servizio:

- il dipendente di una società concessionaria di opere pubbliche che abbia la disponibilità di denaro vincolato al conseguimento di scopi pubblicistici (Cass. pen., sez. VI, 27 gennaio 2005, n. 11902);
- gli impiegati postali addetti alla selezione e allo smaltimento della corrispondenza, anche dopo che l'Ente Poste è stato trasformato in società per azioni, poiché i servizi postali e quelli di telecomunicazione appartengono al novero dei servizi pubblici (Cass. Pen., sez. VI, 25.9.1998, n. 10138).

Non può ritenersi investito della qualifica di Incaricato di Pubblico Servizio chi non operi nell'ambito di un'attività che sia obiettivamente di natura pubblicistica, in quanto diretta a realizzare in via immediata le finalità dell'Ente Pubblico, concretandosi in un servizio rivolto alla generalità dei cittadini (Cass. pen., sez. VI, 02 dicembre 2003, n. 2549).

Al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, ai sensi e per gli effetti di cui agli artt. 357 e 358 C.P., ha rilievo esclusivo la natura delle funzioni esercitate, che devono essere inquadrabili tra quelle della P.A.. Non rilevano, invece, la forma giuridica dell'Ente e la sua costituzione secondo le norme del diritto pubblico, né lo svolgimento della sua attività in regime di monopolio, né tanto meno il rapporto di lavoro subordinato dell'agente con l'organismo datore di lavoro.

Nell'ambito dei soggetti che svolgono pubbliche funzioni, la qualifica di Pubblico Ufficiale è poi riservata a coloro che formano o concorrono a formare la volontà della Pubblica Amministrazione o che svolgono tale attività per mezzo di poteri autoritativi o certificativi, mentre quella di Incaricato di Pubblico Servizio è assegnata dalla legge in via residuale a coloro che non svolgono pubbliche funzioni, ma che non curino neppure mansioni di ordine o non prestino opera semplicemente materiale (Cass. pen., sez. VI, 21 febbraio 2003, n. 11417).



In tema di reati contro la Pubblica Amministrazione il D. Lgs. 231/2001 prevede due articoli che individuano i seguenti reati presupposto:

1. l'art. 24: Indebita percezione di erogazioni, truffa in danno dello Stato o di un Ente Pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un Ente Pubblico;
2. l'art. 25: Concussione, induzione indebita a dare o promettere utilità e corruzione.

Nello specifico, i reati considerati nei due citati articoli del D. Lgs. 231/2001 sono:

### **Malversazione a danno dello Stato (art. 316 bis C.P.)**

*“Chiunque, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato o da altro Ente Pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni”.*

Il reato si concretizza nel caso in cui l'Ente ottenga correttamente contributi o finanziamenti da parte dello Stato o di un altro Ente Pubblico o dalla Comunità Europea ma non li destini alle finalità per cui sono stati erogati.

A titolo esemplificativo e non esaustivo, è considerata area a rischio di reato di malversazione a danno dello Stato la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego ma anche, stando all'interpretazione estensiva che si è voluta dare alle norme, qualsiasi attività collegata all'ottenimento di eventuali agevolazioni fiscali.

L'oggetto giuridico della norma è costituito dall'interesse pubblico all'effettiva realizzazione da parte del beneficiario dello scopo assegnato al singolo finanziamento.

Lo spazio applicativo della norma si estende dal settore economico a quello sociale, così da comprendere, ad esempio, anche i finanziamenti a sostegno di attività culturali o di ricerca scientifica, con il solo limite che si verta in tema di erogazione di risorse pubbliche con vincolo di scopo.

### **Indebita percezione di erogazioni a danno dello Stato (art. 316 ter C.P.)**

*“1. Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi,*



*finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni.*

*2. Quando la somma indebitamente percepita è pari o inferiore a 3.999,96 euro si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5.164 euro a 25.822 euro. Tale sanzione non può comunque superare il triplo del beneficio conseguito.”*

Il reato si caratterizza per il fatto di aver ottenuto l'erogazione di un contributo, di un finanziamento o di un prestito in modo fraudolento. In particolare si tratta dell'utilizzo di documenti falsi (non prodotti dall'utilizzatore) oppure dell'omissione di informazioni dovute.

A titolo esemplificativo e non esaustivo, è considerata attività a rischio di reato di malversazione a danno dello Stato la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da organismi pubblici italiani o comunitari e il loro concreto impiego ma anche, stando l'interpretazione estensiva che si è voluta dare alle norme, qualsiasi attività collegata all'ottenimento di eventuali agevolazioni fiscali.

### **Truffa in danno dello Stato o di un Ente Pubblico (art. 640, comma 2, n. 1 C.P.)**

*“1. Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

*2. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:*

*1. se il fatto è commesso a danno dello Stato o di un altro Ente Pubblico o col pretesto di far esonerare taluno dal servizio militare;”*

Il reato si caratterizza per il fatto di aver conseguito un ingiusto profitto di natura patrimoniale, mediante una condotta fraudolenta che ha ingannato un terzo, con correlativo danno alla Pubblica Amministrazione.

Gli elementi del reato sono dunque la condotta fraudolenta (con “artifici e raggiri”), l'induzione in errore di un terzo, il danno ed il profitto ingiusto. Il reo è elemento attivo del reato.

Per comprendere la differenza con l'art. 316 ter C.P. va rilevato che il reato di cui all'art. 316 ter C.P. si configura nell'ipotesi di indebita percezione di erogazioni pubbliche conseguita dal mero utilizzatore o presentatore di documenti o dichiarazioni falsi o contenenti attestazioni *contra verum* circa la presenza dei presupposti per la pubblica sovvenzione, dovendo, invece, l'agente rispondere



del più grave reato di cui all'art. 640 bis C.P. laddove egli stesso sia anche l'artefice delle suddette falsità.

### **Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis C.P.)**

*“1. La pena è della reclusione da uno a sei anni e si procede d’ufficio se il fatto di cui all’art. 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee”.*

Tale ipotesi di reato si configura nel caso in cui il reato di truffa di cui all’art. 640 C.P. sia posto in essere per conseguire in modo indebito erogazioni pubbliche. L’elemento qualificante è costituito dall’oggetto materiale della frode in quanto “per erogazione pubblica” va intesa ogni attribuzione economica agevolata (contributi, finanziamenti, mutui ecc.) erogata da parte dello Stato, di Enti Pubblici o dalle Comunità europee.

### **Frode informatica (art. 640 ter C.P.)**

*“ 1. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.*

*2. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.*

*3. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.*

*4. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante”.*

Tale fattispecie di reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, un soggetto ottenga per sé o altri un ingiusto profitto arrecando anche un danno a terzi.



### **Concussione (art. 317 C.P.)**

*“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 altra utilità è punito con la reclusione da sei a dodici anni.”*

Gli elementi essenziali del reato di concussione sono:

1. abuso dell'ufficio, da intendere come abuso della qualità di Pubblico Ufficiale ovvero dei poteri del Pubblico Ufficiale. Solo nel secondo caso è necessario che l'abuso concerna atti dell'Ufficio;
2. costringimento della vittima a dare o promettere denaro al Pubblico Ufficiale. Nel reato la condotta assume i caratteri dell'abuso e della prevaricazione essendo diretta a strumentalizzare l'Ufficio pubblico per coartare la volontà altrui al fine di ottenere, indebitamente, la dazione o promessa di denaro o altra utilità;
3. dazione o promessa di denaro o altra utilità. Deve trattarsi di una utilità indebita, nel senso che non è dovuta al Pubblico Ufficiale in quanto tale.

Va specificato che, essendo il Centro Studi Città di Foligno un'Associazione volontaria, senza scopo di lucro e non riconosciuta, i suoi dipendenti ed Amministratori non rivestono, di norma, la qualifica né di Pubblico Ufficiale, né di Incaricato di Pubblico Servizio. I delitti di cui agli artt. 317, 318, 319, aggravato ai sensi dell'art. 319-bis, quando dal fatto l'Ente ha conseguito un profitto di rilevante entità, 319-ter, e 320 C.P., rilevano, tuttavia, ai fini dell'art. 321 del C.P. “Pene per il corruttore” che è applicabile al personale ed agli organi apicali dell'Associazione.

### **Corruzione per l'esercizio della funzione (art. 318 C.P.)**

*“Il Pubblico Ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da uno a cinque anni”.*

Tale ipotesi di reato si configura nel caso in cui il Pubblico Ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere, ritardare o rilasciare atti (determinando un vantaggio in favore dell'offerente) da intendersi ricompresi nei suoi doveri di ufficio.

Il reato di “corruzione” si differenzia da quello di “concussione”, in quanto, nella corruzione, tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio.



### **Corruzione per un atto contrario ai doveri d'ufficio (art. 319 C.P.)**

*“Il Pubblico Ufficiale che, 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 altra utilità, o ne accetta la promessa, è punito con la reclusione da quattro a otto anni”.*

Tale ipotesi di reato si configura nel caso in cui un Pubblico Ufficiale riceva, per sé o per altri, denaro o altri vantaggi, o ne accetti la promessa per omettere o ritardare un atto d'ufficio o per aver compiuto un atto contrario ai suoi doveri d'ufficio.

### **Circostanze aggravanti (art. 319-bis C.P.)**

*“La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'Amministrazione alla quale il Pubblico Ufficiale appartiene”.*

La circostanza aggravante di cui all'art. 319-bis C.P. è relativa all'ipotesi in cui la corruzione abbia ad oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'Amministrazione alla quale il Pubblico Ufficiale appartiene.

### **Corruzione in atti giudiziari (art. 319 ter C.P.)**

*“1. Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da quattro a dieci anni.*

*2. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da cinque a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni”.*

Il reato si caratterizza per il particolare oggetto e la particolare finalità della corruzione. Questa deve essere commessa per favorire una parte in un processo penale, civile o amministrativo. Il reato è una forma speciale di corruzione. Non è necessario che derivi effettivamente un danno ad una parte per la consumazione del reato; infatti il danno (l'ingiusta condanna) è prevista come circostanza aggravante. In ogni caso è necessario che il danno o il favore che consegue alla parte siano ingiusti.

### **Induzione indebita a dare o promettere utilità (art. 319-quater C.P.)**



*“Salvo che il fatto costituisca più grave reato, il Pubblico Ufficiale o l’Incaricato di Pubblico Servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da tre a otto anni. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni”.*

Il reato è stato introdotto a seguito dell’entrata in vigore della Legge 190/2012 c.d. *“Legge Anti corruzione”*, a seguito della riforma del reato di concussione (art. 317 C.P.) ora ristretto al solo caso di costrizione.

Il concetto di induzione esprime l’idea della pressione su un terzo affinché tenga un determinato comportamento.

Al secondo comma viene prevista la punibilità del soggetto privato che è indotto alla dazione o alla promessa di denaro o altra utilità. Questo rappresenta una novità rispetto alla previgente disciplina. In precedenza, infatti, al pari del "concusso mediante costrizione", il "concusso mediante induzione" non era punibile, mentre ora invece è considerato concorrente necessario del reato.

### **Corruzione di persona incaricata di un pubblico servizio (Art. 320 C.P.)**

*“Le disposizioni degli articoli 318 e 319 si applicano anche all’Incaricato di un Pubblico Servizio. In ogni caso, le pene sono ridotte in misura non superiore a un terzo”.*

La norma estende agli Incaricati di Pubblico Servizio i reati di *“Corruzione per l’esercizio della funzione”* (art. 318 C.P.) e di *“Corruzione per un atto contrario ai doveri d’ufficio”* (art. 319 C.P.) prevedendo una riduzione della pena in misura non superiore ad un terzo.

### **Pene per il corruttore (art. 321 C.P.)**

*“Le pene stabilite nel primo comma dell’articolo 318, nell’articolo 319, nell’articolo 319-bis, nell’art. 319-ter, e nell’articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al Pubblico Ufficiale o all’Incaricato di un Pubblico Servizio il denaro od altra utilità”.*

La presente norma, che estende al soggetto che corrompe un Pubblico Ufficiale o un Incaricato di Pubblico Servizio le pene stabilite per i reati compiuti da questi ultimi negli articoli espressamente indicati, risulta applicabile ai soggetti privati e quindi anche ai soggetti apicali ed ai dipendenti del Centro Studi Città di Foligno.



### **Istigazione alla corruzione (art. 322 C.P.)**

*“1. Chiunque offre o promette denaro od altra utilità non dovuti ad un Pubblico Ufficiale o ad un Incaricato di un Pubblico Servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo.*

*2. Se l'offerta o la promessa è fatta per indurre un Pubblico Ufficiale o un Incaricato di un Pubblico Servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.*

*3. La pena di cui al primo comma si applica al Pubblico Ufficiale o all'Incaricato di un Pubblico Servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.*

*4. La pena di cui al secondo comma si applica al Pubblico Ufficiale o all'Incaricato di un Pubblico Servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319”.*

Il Codice Penale punisce anche l'istigazione alla corruzione. L'istigazione alla corruzione è il reato del privato che tenta di corrompere (senza riuscirvi) il Pubblico Ufficiale affinché questi ometta o ritardi un atto del proprio ufficio o affinché compia un atto contrario ai suoi doveri di ufficio.

Tale reato può essere commesso anche dal Pubblico Ufficiale che “sollecita” la corruzione.

Di fatto la norma punisce il tentativo unilaterale di corruzione non riuscita.

### **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 esteri (art. 322 bis C.P.)**

*“ 1. Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:*

*1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;*

*2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;*



3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale.

2. Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente articolo;

2) 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 ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria..

3. Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.”.

Si tratta dei medesimi reati sopra descritti in cui la peculiarità sta nel coinvolgimento dei membri degli organi della Comunità europea e di funzionari della Comunità europea e di Stati esteri.

### **3. I REATI DI CORRUZIONE TRA PRIVATI (ARTT. 2635, COMMA 3, E 2635-BIS C.C.)**

Oltre ai reati contro la Pubblica Amministrazione, la presente parte speciale si occupa anche del reato di “Corruzione tra privati” previsto dal Codice Civile (art. 2635, comma 3, C.C.) così come riformulato dalla L.190/2012 e dal D. Lgs. 38/2017, e del reato di “Istigazione alla corruzione tra privati” di cui all’art. 2635-bis C.C. -inserito dal D. Lgs. 38/2017-.

Tali reati sono previsti dall’art. 25-ter, comma 1, lettera s-bis, del D. Lgs. 231/2001.



La peculiarità delle fattispecie è data dal fatto che il reato corruttivo si compie fra soggetti privati e non riguarda un Pubblico Ufficiale o un Incaricato di un Pubblico Servizio.

### **Corruzione tra privati (art. 2635, comma 3 C.C.)**

*“Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per se' o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.*

*Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.*

*Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.”.*

Per quanto concerne la corruzione tra privati, per espressa previsione del D. Lgs. 231/2001, art. 25-ter, comma 1, lettera s-bis), è reato presupposto la sola fattispecie di cui al comma 3 dell'art. 2635 C.C., cioè il delitto commesso dal soggetto corruttore per avvantaggiare il suo Ente di appartenenza (corruzione attiva).

Potrà dunque configurarsi la responsabilità dell'Ente nell'ipotesi in cui il corruttore (soggetto apicale o “sottoposto”) anche per interposta persona, dia o prometta denaro o altra utilità, nell'interesse o a vantaggio del proprio Ente di appartenenza, alle persone indicate nel primo e nel secondo comma dell'articolo 2635 C.C. appartenenti ad altra Società o Ente privato.

### **Istigazione alla corruzione tra privati (art. 2635-bis C.C.)<sup>6</sup>**

*“Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al*

---

<sup>6</sup> Articolo inserito dall'art. 4, comma 1, del D. Lgs. 38/2017.



*proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.*

*La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.”*

Il reato è procedibile a querela della persona offesa.

Con l'ultima recente riforma diventa reato presupposto anche l'istigazione alla corruzione tra privati (nuovo art. 2635-bis, comma 1, C.C.): anche in questo caso il reato è solo a carico dell'Ente a cui appartiene il soggetto che istiga alla corruzione gli esponenti aziendali altrui, per avvantaggiare l'Ente di appartenenza.

L'inserimento nel catalogo dei reati di cui al D. Lgs. 231/2001 del comma 3 dell'articolo 2635 e dell'art. 2635-bis C.C. indica che tale reato, anche nella forma del tentativo, può comportare responsabilità per l'Ente solo nei casi di condotte attive da parte di un soggetto apicale/dipendente dell'Ente che agisce come corruttore.

Da segnalare come novità assoluta è il fatto che si applicano alla corruzione tra privati le sanzioni interdittive ex art 9, comma 2, del D. Lgs. 231/2001 da 3 mesi a 2 anni (non essendo specificata durata diversa); lo stesso dicasi per l'istigazione (punita, invece, con sanzione pecuniaria più contenuta).

Si tratta degli unici reati societari per i quali è prevista la possibilità di applicare a carico dell'Ente le sanzioni interdittive (anche in sede cautelare).

#### **4. IDENTIFICAZIONE DELLE ATTIVITA' SENSIBILI AI FINI DELLA COMMISSIONE DEI REATI ESAMINATI**

Come già specificato nella Parte generale del M.O.G., poiché il Centro Studi Città di Foligno è un'Associazione governata da un Consiglio di Amministrazione che occupa un solo dipendente, per organizzare l'attività lavorativa non c'è una suddivisione interna in uffici, mentre le aree di attività si suddividono in organizzativa e di formazione.

Nelle presente Parte Speciale si considerano, quindi, le sole attività svolte.



Relativamente ai reati contro la Pubblica Amministrazione e di corruzione fra privati, l'analisi dei processi, effettuata conformemente a quanto prescritto dall'art. 6, comma 2, lettera a), del D. Lgs. 231/2001, ha consentito di individuare come potenzialmente a rischio tutte quelle attività tipiche dell'Associazione che implicano rapporti con la Pubblica Amministrazione o con Società ed Enti Privati (c.d. rischio diretto).

Allo stesso modo sono da considerarsi a rischio le attività dell'Associazione che, pur non implicando direttamente l'instaurazione di rapporti con la Pubblica Amministrazione o con Società ed Enti Privati, gestiscono strumenti di tipo finanziario o utilità di altro genere che potrebbero essere impiegati per attribuire vantaggi e utilità a Pubblici Ufficiali, Incaricati di un Pubblico Servizio o ai soggetti indicati negli artt. 2635 e 2635-bis C.C. (c.d. rischio indiretto).

In particolare si fa riferimento ad omaggi, liberalità, sponsorizzazioni, organizzazione di eventi ed attività sociali.

Dalle analisi dei rischi effettuate, le attività a rischio possono essere così precisate:

#### ATTIVITÀ A RISCHIO DIRETTO:

1. ogni attività che coinvolga o che sia in rapporto con la P.A. (per tutti i reati contro la Pubblica Amministrazione previsti dal D. Lgs. 231/2001) e con Società ed Enti Privati (per i reati consumati e tentati di corruzione fra privati);
2. richiesta, percezione, utilizzazione e rendicontazione di finanziamenti, sovvenzioni, fondi e contributi pubblici compresi quelli europei. E' compresa la richiesta, l'utilizzo e la rendicontazione intermedia e finale relativa all'utilizzo di fondi europei e di finanziamenti pubblici.

In relazione a questo processo, i reati ipotizzabili, in linea di principio, potrebbero essere la corruzione e la truffa a danno dello Stato, dei membri degli organi delle Comunità Europee, di funzionari delle Comunità Europee e di Stati esteri, l'indebita percezione di erogazioni e la malversazione. Il reato di corruzione potrebbe essere consumato attraverso il contatto con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore dell'Associazione. Il reato di truffa a danno dello Stato potrebbe configurarsi in una rappresentazione non trasparente dei fatti, tramite l'emissione di documenti o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno allo Stato. Il reato di indebita percezione di erogazioni potrebbe essere commesso al momento della richiesta di stanziamento del finanziamento concesso e dell'acquisizione del finanziamento, mediante la presentazione di richieste di finanziamento che contengano dichiarazioni o documenti falsi che attestino dati o fatti non veri o omettano informazioni dovute. Il



reato di malversazione potrebbe essere commesso nel caso in cui i fondi agevolati ottenuti vengano destinati, in tutto o in parte, a scopi diversi da quelli dichiarati.

3. rapporti con Pubblici Ufficiali in occasione di verifiche ed ispezioni (si considerano in tale area qualsiasi ispezione, accertamento, verifica tecnica, giudiziaria, tributaria, amministrativa, relativa alla normativa sulla sicurezza e salute del lavoro o della normativa ambientale, condotta, a titolo non esaustivo, da ASL, ispettorato del lavoro, INPS, INAIL, Agenzia delle Entrate, Guardia di Finanza, Polizia Municipale o Provinciale, Vigili del Fuoco, Polizia Giudiziaria ecc.) o per favorire una parte in un processo.

In relazione a queste attività, i reati ipotizzabili, in linea di principio, potrebbero essere la corruzione, anche in atti processuali, e la truffa a danno dello Stato. Il reato di corruzione potrebbe essere consumato attraverso il contatto con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore (o a minor sfavore) per l'Associazione comprese le sentenze in eventuali giudizi civili, penali, tributari o amministrativi.

Il reato di truffa a danno dello Stato potrebbe configurarsi in una rappresentazione non trasparente dei fatti, tramite l'emissione di documenti o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno all'Ente pubblico ed un vantaggio ingiusto per l'Associazione.

4. rapporti con soggetti pubblici per l'ottenimento, il mantenimento ed il rinnovo di autorizzazioni, concessioni, licenze, servitù, necessarie o utili per l'esercizio delle attività dell'Ente. Si comprendono in tali attività le richieste di autorizzazioni ai Comuni, alla Provincia, alla Regione ed altri Enti Pubblici. Sono altresì comprese le concessioni rilasciate dai Comuni per lo svolgimento delle attività proprie dell'Associazione.

In relazione a queste attività, i reati ipotizzabili, in linea di principio, potrebbero essere la corruzione e la truffa a danno dello Stato, secondo le fattispecie sopra rappresentate.

5. rapporti con gli Amministratori e con soggetti in posizione apicale di Società ed Enti Privati per i reati consumati o tentati di corruzione fra privati. Sono compresi i rapporti contrattuali e la scelta e selezione dei fornitori. A titolo esemplificativo, il reato, tentato o consumato, potrebbe essere realizzato nel caso in cui un esponente dell'Associazione, offra e/o prometta denaro o altra utilità:

(i) ad un amministratore di una Società o Ente privato al fine di concludere accordi commerciali con tale Società o Ente a condizioni svantaggiose per quest'ultima;

(ii) nell'ambito di un contenzioso, ad un amministratore della Società o Ente privato controparte per ottenere un accordo transattivo sfavorevole per questi ultimi;



(iii) con riferimento alla cessione di beni o servizi, a un amministratore della Società o Ente privato controparte affinché acquisti un bene o un servizio dall'Associazione a condizioni sfavorevoli per l'acquirente.

L'utilità data, promessa od offerta all'amministratore corrotto, potrebbe anche consistere ad esempio:

- nell'assunzione di persone legate all'amministratore corrotto da vincoli di parentela o simili;
- in regali od omaggi che non siano di modico valore (come individuati nel Codice Etico del Centro Studi Città di Foligno) e non direttamente ascrivibili a normali relazioni di cortesia (anche in connessione a ricorrenze socialmente riconosciute);
- nella conclusione di contratti per la fornitura di beni e servizi con controparti segnalate dall'amministratore corrotto;
- nella conclusione di contratti di consulenza o sponsorizzazione con controparti segnalate dall'amministratore corrotto.

6. stipula di contratti, convenzioni e atti in genere con la Pubblica Amministrazione.

#### ATTIVITÀ A RISCHIO INDIRETTO:

1. le attività di amministrazione e contabilità, in cui il rischio principale riguarda l'ipotesi di accantonamento di somme di denaro ("fondi occulti") a scopi corruttivi;
2. le consulenze e la gestione degli approvvigionamenti di beni e servizi, su cui grava il rischio che gli incarichi dissimolino illecite attribuzioni di utilità a soggetti legati direttamente o indirettamente a Pubblici Ufficiali o Incaricati di Pubblico Servizio che hanno rapporti diretti con l'Associazione allo scopo esclusivo di alterarne l'indipendenza di giudizio e di procurare all'Ente un vantaggio ingiusto (ad esempio, con l'assegnazione di consulenze a persone o società "gradite" ai soggetti della Pubblica Amministrazione, per ottenere in cambio favori nell'ambito dello svolgimento di altre attività dell'Associazione), ovvero la distrazione di liquidità dalla contabilità ufficiale per alimentare i "fondi occulti", tramite la sovrapproduzione dei beni e servizi acquistati dal fornitore;
3. la gestione dei sistemi informativi, che potrebbe essere utilizzata illecitamente per il compimento dei reati di truffa in danno dello Stato o di altra Pubblica Amministrazione o di frode informatica;
4. i contenziosi giudiziari, in cui il rischio concerne le ipotesi di reato di corruzione in atti giudiziari;
5. gli accordi transattivi, in cui il rischio riguarda la simulazione di transazioni per determinare distrazione di liquidità dalla contabilità ufficiale per alimentare i fondi occulti;
6. gli omaggi, le spese di rappresentanza e le sponsorizzazioni, su cui grava il rischio che le elargizioni siano direttamente o indirettamente rivolte a Pubblici Ufficiali o Incaricati di Pubblico



Servizio che hanno rapporti diretti con l'Associazione, allo scopo esclusivo di alterarne significativamente l'indipendenza di giudizio e di procurare all'Ente un vantaggio ingiusto;

7. le assunzioni del personale, su cui grava il rischio che siano favoriti in modo non equo soggetti legati direttamente o indirettamente a Pubblici Ufficiali o Incaricati di Pubblico Servizio che hanno rapporti diretti con l'Associazione, allo scopo esclusivo di alterarne significativamente l'indipendenza di giudizio e di procurare all'Ente un vantaggio ingiusto;

8. l'emissione di note di credito, storni di fatture e scritture contabili. La gestione del processo riguarda tutte le attività inerenti le scritture contabili in genere che determinano un credito o un debito, ivi comprese le emissioni di note di credito e gli storni di fatture. In relazione a questo processo, si può ipotizzare, in linea di principio, il reato di corruzione e di truffa a danni dello Stato. Il reato di corruzione si potrebbe commettere, ad esempio, tramite l'emissione di note di credito o storni di fatture a persone o società "gradite" alla Pubblica Amministrazione per ottenere in cambio favori nell'ambito dello svolgimento di altre attività dell'Associazione. Il reato di truffa a danno dello Stato si potrebbe configurare a seguito di una registrazione in contabilità non giustificata a debito per un cliente pubblico, con conseguente danno patrimoniale alla Pubblica Amministrazione e vantaggio ingiusto per l'Associazione;

9. gli adempimenti normativi gestiti da soggetti esterni. Riguarda tutte quelle attività svolte, per conto o a favore dell'Associazione, da soggetti terzi, ed, in particolare, tutti gli adempimenti svolti da consulenti esterni (ad esempio pratiche con INAIL, INPS, Agenzia delle Entrate, pratiche su finanziamenti e contributi ricevuti da Amministrazioni Pubbliche, ecc.). In relazione ai suddetti processi, i reati ipotizzabili, in linea di principio, potrebbero essere la corruzione e la truffa ai danni dello Stato. Il reato di corruzione potrebbe essere consumato attraverso il contatto dei soggetti terzi con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore (o a minor sfavore) per l'Associazione. Il reato di truffa a danno dello Stato potrebbe configurarsi in una rappresentazione non veritiera dei fatti da parte dei soggetti terzi incaricati dall'Associazione, tramite l'emissione di documenti, o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno allo Stato.

## **5. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE**

Nell'ambito della presente sezione della Parte Speciale vengono riportati i principi di comportamento che si richiede vengano adottati da parte degli organi apicali, del personale e dei



collaboratori dell'Associazione nella gestione dei rapporti con la Pubblica Amministrazione e con Società ed Enti privati.

Tali regole di condotta sono finalizzate a limitare il più possibile il verificarsi dei reati presupposto indicati nel D. Lgs. 231/2001 ai danni della Pubblica Amministrazione e le ipotesi di corruzione, tentata o consumata, tra privati.

I principi di comportamento si applicano in modo diretto agli Amministratori, al Direttore (se nominato) ed ai dipendenti del Centro Studi Città di Foligno, mentre si applicano ai consulenti ed in generale ai partner in forza di specifiche clausole contrattuali.

I processi descritti in questo paragrafo devono risultare adeguatamente formalizzati ed aggiornati e dovranno essere sottoposti a continuo monitoraggio e verifica da parte dell'Organismo di Vigilanza.

## **5.1. OBBLIGHI**

E' fatto obbligo a tutti i destinatari del Modello di:

1. Osservare tutte le disposizioni legislative e regolamentari applicabili alle attività indicate nella presente Sezione;
2. Osservare lo Statuto dell'Associazione, il M.O.G. compresi i relativi allegati, il Codice Etico, le decisioni del Consiglio di Amministrazione e degli altri Organi sociali, le disposizioni dei superiori gerarchici e tutte le politiche e procedure interne che disciplinano l'attività dell'Associazione, con particolare riferimento alla gestione dei rapporti con la Pubblica Amministrazione;
3. Impostare e mantenere i rapporti con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza, a garanzia dell'autonomia e della correttezza delle decisioni di quest'ultima;
4. Garantire che ogni operazione e/o transazione, intesa nel senso più ampio del termine, sia legittima, autorizzata, coerente, congrua, documentata, registrata ed in ogni tempo tracciabile e verificabile;
5. Garantire che le informazioni rese alla Pubblica Amministrazione e la documentazione prodotta rispondano ai principi di veridicità, completezza, correttezza;
6. Inviare comunicazioni con la Pubblica Amministrazione preferibilmente per iscritto e solo dietro specifica autorizzazione da parte degli organi di governo dell'Associazione per i dipendenti e per i collaboratori, gli agenti e i rappresentanti, i consulenti e, in generale, per i soggetti che svolgono



attività di lavoro autonomo, nella misura in cui essi operino nell'ambito delle aree di attività sensibili per conto o nell'interesse dell'Associazione stessa;

7. In caso di tentata concussione da parte di un pubblico impiegato nei confronti di un dipendente (o di altri collaboratori) devono essere adottati i seguenti comportamenti:

- non dare seguito alla richiesta;
- informare tempestivamente il superiore;
- attivare una formale informativa, da parte del superiore, all'Organismo di Vigilanza.

8. Impostare e mantenere i rapporti con Società ed Enti privati sulla base di criteri di massima correttezza e trasparenza, a garanzia dell'autonomia e della correttezza delle loro decisioni;

9. Seguire i criteri di selezione di fornitori e consulenti, predeterminati dall'Associazione, per assicurare parità di trattamento e trasparenza.

## **5.2. DIVIETI PER I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE**

La presente Parte Speciale prevede l'espresso divieto di:

1. Porre in essere comportamenti tali da configurare le fattispecie di reato individuate dagli artt. 24 e 25 del D. Lgs. 231/2001;

2. Porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente divenirlo;

3. Porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti è fatto divieto di:

- effettuare elargizioni in denaro a Pubblici impiegati;
- accettare, da chiunque interessato all'attività dell'Associazione, denaro o altre utilità oltre i limiti previsti dal Codice Etico, al fine di acquisire un vantaggio personale;
- distribuire omaggi e regali al di fuori di quanto previsto dal Codice Etico. In particolare, è vietata qualsiasi forma di regalo ad impiegati pubblici, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'Associazione. I regali offerti devono essere documentati in modo adeguato per consentire le prescritte verifiche in termini di opportunità e di valore;
- accordare, in modo consapevole, altri vantaggi di qualsiasi natura (es. promesse di assunzione, assegnazione di incarichi di consulenza, ecc.) in favore di rappresentanti della Pubblica



Amministrazione, o di loro familiari, che possano indurli a trattamenti di favore nei confronti dell'Associazione;

- riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli a cui erano destinati;
- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione in errore nella valutazione tecnico-economica dei prodotti e dei servizi offerti e/o forniti;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione;
- intrattenere rapporti con la Pubblica Amministrazione in rappresentanza dell'Associazione per ragioni non riconducibili alle competenze ed alle funzioni assegnate;
- accedere in maniera non autorizzata ai sistemi informatici della Pubblica Amministrazione per ottenere e/o modificare informazioni a proprio vantaggio;
- accedere in maniera non autorizzata ai sistemi informatici utilizzati dalla Pubblica Amministrazione od alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi modalità a cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare indebitamente informazioni a vantaggio dell'Associazione o di terzi, o comunque al fine di procurare un indebito vantaggio all'Associazione o a terzi;
- per gli amministratori, direttori, dirigenti preposti alla redazione dei documenti contabili e sindaci dell'Associazione, nonché a chi svolge nell'Ente attività lavorativa con l'esercizio di funzioni direttive, accettare o sollecitare per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

### **5.3. DIVIETI PER I REATI DI CORRUZIONE TRA PRIVATI**

Per tutte le operazioni che concernono attività sensibili nei reati di corruzione tra privati è fatto assoluto divieto di:



- porre in essere condotte tali da integrare la commissione del reato di corruzione tra privati;
- porre in essere qualsiasi comportamento che, pur non integrando in concreto il reato di corruzione tra privati, possa in astratto, diventarlo;
- porre in essere comportamenti in violazione del M.O.G. e delle norme del Codice Etico;
- anche per interposta persona, offrire, promettere o dare denaro o altra utilità non dovuti ad amministratori, direttori generali, dirigenti preposti alla redazione di documenti contabili, sindaci e liquidatori di Società o Enti privati, a chi esercita funzioni direttive in Società ed Enti privati o a chi è sottoposto alla direzione e vigilanza dei soggetti sopra elencati, per fargli compiere od omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà;
- adempiere la richiesta di denaro o altra utilità non dovuti da parte di amministratori, direttori generali, dirigenti preposti alla redazione di documenti contabili, sindaci e liquidatori di Società o Enti privati, o comunque da chi esercita funzioni direttive in Società ed Enti privati o da chi è sottoposto alla direzione e vigilanza dei soggetti sopra elencati, per fargli compiere od omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà;
- porre in essere o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con privati, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse dell'Associazione e nel pieno rispetto;
- elargire o promettere indebitamente denaro a un privato;
- distribuire o promettere omaggi e regali che non siano di modico valore a terzi, in violazione di quanto previsto dal Codice Etico;
- accordare o promettere altri vantaggi, di qualsiasi natura essi siano, in favore di privati nonché a beneficio di altri individui o entità giuridiche riconducibili alla sfera di interesse di questi ultimi;
- effettuare prestazioni in favore dei fornitori e/o clienti che non trovino adeguata giustificazione nel contesto del rapporto con essi costituito;
- riconoscere compensi in favore di consulenti e di collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti nell'Associazione o distribuire regalie od omaggi al di fuori di quanto previsto dal Codice Etico;
- presentare dichiarazioni e/o documenti e/o dati e/o informazioni non rispondenti al vero, errati, falsi o incompleti a soggetti ed Enti privati.

## 5.4. DOVERI DI CONDOTTA



Ai fini dell'attuazione dei comportamenti di cui sopra:

- a) deve essere garantito il rispetto dei principi di correttezza, trasparenza e buona fede;
- b) i soggetti che intrattengono rapporti con la Pubblica Amministrazione e con Società ed Enti privati per conto del Centro Studi Città di Foligno devono essere preventivamente autorizzati;
- c) solo il personale preventivamente autorizzato può accedere alle aree riservate di siti di Enti Pubblici o privati;
- d) gli incarichi conferiti ai collaboratori esterni devono essere redatti per iscritto, con l'indicazione delle attività da svolgere e del compenso pattuito. Tali incarichi devono essere proposti o verificati o approvati dal Presidente del Consiglio di Amministrazione;
- d) i pagamenti in contanti possono essere eseguiti nei limiti degli importi unitari massimi di € 250,00 definiti dalle prassi interne. Tali pagamenti devono inoltre essere adeguatamente giustificati, documentati e monitorati;
- e) i pagamenti in contanti ricevuti possono essere accettati nei limiti degli importi unitari massimi definiti nell'apposita normativa vigente;
- f) le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi, fondi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
- g) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.), devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

## **6. PRINCIPI PROCEDURALI SPECIFICI**

### **6.1. IL RESPONSABILE INTERNO**

I rapporti nei confronti della Pubblica Amministrazione e con Società ed Enti privati, per le attività a rischio, devono essere gestiti in modo unitario, da un responsabile (c.d. Responsabile interno).

Vista l'esiguità del personale dell'Associazione, il ruolo di Responsabile interno sarà svolto, salva diversa decisione del C.d.A., dal Presidente del Consiglio di Amministrazione.

Nel caso in cui venga nominato un Direttore Tecnico il ruolo di Responsabile interno potrà essere affidato a quest'ultimo, per tutte o parte delle attività, previa decisione del Consiglio di Amministrazione.



Ogni variazione nei ruoli dovrà comunque essere posta a conoscenza del personale e dei soggetti interessati con comunicazione scritta.

Il Responsabile Interno, garantisce il rispetto dei comportamenti ammessi, delle politiche e delle procedure dell'Associazione e riferisce periodicamente all'Organismo di Vigilanza - secondo le tempistiche da questo definite - sulla gestione delle attività a rischio.

Il Responsabile Interno interpella l'Organismo di Vigilanza per la soluzione di questioni, anche interpretative, riferite agli obiettivi di prevenzione del presente Modello

Il Responsabile Interno può affidare lo svolgimento di talune specifiche funzioni a dipendenti dell'Associazione, avendo cura di verificare il rispetto, da parte di questi ultimi, dei principi e degli obiettivi previsti dal M.O.G. e dai suoi allegati.

## **6.2. RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE**

Le operazioni nei confronti della Pubblica Amministrazione, per le attività a rischio, devono essere poste in evidenza (ad esempio tramite la predisposizione di appositi “verbali” contenenti tutte le informazioni rilevanti relative ad ogni operazione con la Pubblica Amministrazione, ecc.).

Il Responsabile interno deve identificare, per le attività a rischio svolte, gli strumenti più adeguati per garantire che i rapporti tenuti con la Pubblica Amministrazione siano sempre documentati e verificabili.

Per garantire la verificabilità, le operazioni che comportano l'impiego di risorse economiche o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza contabile.

Nel caso in cui la comunicazione alla Pubblica Amministrazione avvenga attraverso supporti informatici, l'identità dell'operatore che immette dati e dichiarazioni deve essere sempre individuabile.

## **6.3. IDONEITÀ DEI SOGGETTI CHE INTRATTENGONO RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E PRINCIPI DI INTERAZIONE**

I rapporti di tipo istituzionale nei confronti della Pubblica Amministrazione, per le attività a rischio in qualunque forma, devono essere gestiti e firmati solo da coloro che sono dotati di idonei poteri.

Alle eventuali ispezioni presso l'Associazione (es. giudiziarie, tributarie, amministrative, sulla sicurezza e igiene sul lavoro, ecc.) partecipa il Responsabile interno o altro soggetto da lui incaricato.



L'inizio di ogni attività ispettiva è prontamente segnalata dal personale presente al Responsabile interno ed all'Organismo di Vigilanza.

In caso di procedimento ispettivo deve essere richiesta copia del verbale redatto dall'Autorità Pubblica, ove disponibile, che andrà trasmessa al Consiglio di Amministrazione ed all'Organismo di Vigilanza.

Devono essere immediatamente segnalati all'Autorità Giudiziaria ed all'O.d.V. eventuali comportamenti della controparte pubblica volti ad ottenere favori, elargizioni illecite di denaro o altre utilità.

Il soggetto che si trovi in una situazione di conflitto di interessi, si astiene dal partecipare a decisioni in relazione alle quali possa determinarsi il predetto conflitto, dichiarandolo.

#### **6.4. RAPPORTI CON SOGGETTI PRIVATI**

Tutti i consulenti, fornitori e chiunque operi in nome e per conto del Centro Studi Città di Foligno, sono impegnati al rispetto dei principi etico-comportamentali adottati dall'Associazione.

A questo scopo l'incarico, a tali soggetti, di operare in rappresentanza e/o nell'interesse dell'Ente (nei confronti della Pubblica Amministrazione o verso terzi) deve essere assegnato in forma scritta e deve prevedere una specifica clausola che vincoli all'osservanza dei principi etico-comportamentali adottati dall'Associazione.

Nell'ottica di favorire una più efficace prevenzione dei reati contro la Pubblica Amministrazione e di corruzione tra privati, si prevede, inoltre, l'inserimento nei contratti stipulati dal Centro Studi Città di Foligno con detti soggetti, di apposita dichiarazione attestante:

- di essere a conoscenza del D.Lgs. 231/2001 e delle sue implicazioni per l'Associazione;
- non essere stato condannato con sentenza passata in giudicato per uno dei reati previsti dal D. Lgs 231/2001;
- di impegnarsi al rispetto del D. Lgs. 231/2001;
- di essere a conoscenza del m.o.g. e del codice etico del centro studi città di foligno e di impegnarsi a rispettarli nella propria attività;
- di non porre in essere, nell'ambito dell'espletamento delle proprie attività, comportamenti tali da integrare le fattispecie di reato di cui all'art. 24 e 25 del D. Lgs. 231/01 a carico del Centro Studi Città di Foligno e comportamenti che, sebbene non intenzionalmente rivolti a commettere un illecito, siano tali da costituire potenzialmente gli eventi delittuosi di



“Corruzione tra privati” e di “Istigazione alla corruzione tra privati” di cui all’art. 25-ter del D. Lgs. 231/2001.

Infine, nei predetti contratti deve essere inserita una specifica clausola risolutiva espressa come conseguenza della violazione da parte dei consulenti, dei fornitori ed in generale di chiunque operi in nome e per conto del Centro Studi Città di Foligno, delle norme di cui al D. Lgs. 231/2001, oltre alla richiesta di risarcimento dei danni eventualmente prodotti.

## **7. I CONTROLLI DELL’ORGANISMO DI VIGILANZA**

I compiti dell’Organismo di Vigilanza, concernenti la valutazione dell’efficacia delle procedure e dell’osservanza delle prescrizioni del Modello in materia di prevenzione dei reati contro la Pubblica Amministrazione e dei reati di “Corruzione tra privati” e di “Istigazione alla corruzione tra privati”, sono i seguenti:

- verifica periodica, con il supporto del personale, del rispetto dei divieti e dei principi procedurali previsti dalla Parte Generale del M.O.G e dalla presente Parte Speciale a presidio delle attività individuate come a rischio;
- raccolta ed esame di eventuali segnalazioni riguardanti irregolarità riscontrate o situazioni di particolare criticità ricevute dal Responsabile interno, da un dipendente, o da terzi;
- raccolta dei documenti di rendicontazione e verifica che siano documentati e registrati in conformità ai principi di correttezza contabile;
- effettuazione delle attività di controllo periodico e disposizione degli accertamenti ritenuti necessari e opportuni a seguito delle segnalazioni ricevute;
- effettuazione periodica di controlli a campione, diretti a verificare la corretta esplicazione delle attività connesse ai processi sensibili relativi ai reati contro la Pubblica Amministrazione ed ai reati di “Corruzione tra privati” e di “Istigazione alla corruzione tra privati”, anche in relazione ai principi espressi nel presente documento ed, in particolare, alle procedure interne in essere;
- monitoraggio sull’efficacia dei presidi organizzativi e di controllo e proposta di eventuali modifiche/integrazioni;
- valutazione delle esigenze formative del personale in materia di legalità e sul D. Lgs. 231/2001 da proporre all’approvazione del Consiglio di Amministrazione, individuandone i destinatari.



Qualora, nell'espletamento dei compiti di cui sopra, l'Organismo di Vigilanza riscontri violazioni delle regole e dei principi contenuti nella presente parte speciale del Modello ne deve dare immediata informazione al Presidente del Consiglio di Amministrazione. Qualora le violazioni fossero imputabili al Presidente del Consiglio di Amministrazione, l'Organismo, secondo opportunità, riferirà agli altri membri del Consiglio di Amministrazione o all'Assemblea dei Soci, tramite il Collegio Sindacale.

Allo stesso modo il Presidente del Consiglio di Amministrazione dovrà informare l'Organismo di Vigilanza circa le procedure di accertamento delle violazioni, l'irrogazione di sanzioni o l'archiviazione di un provvedimento disciplinare qualora le violazioni riguardino norme di comportamento disciplinate nel "Modello Organizzativo".

## **8. MODIFICHE ED AGGIORNAMENTI DELLA PRESENTE PARTE SPECIALE**

Le attività individuate come "a rischio" potranno essere modificate e/o integrate a seguito degli aggiornamenti delle attività di *risk mapping* e *risk assessment* effettuate di volta in volta dall'Associazione -anche su richiesta dell'O.d.V.- a seguito del verificarsi di situazioni quali, a titolo esemplificativo, cambiamenti organizzativi, aggiornamenti legislativi, realizzazione di reati presupposto nell'ambito dell'Associazione, piani di miglioramento del Modello ecc.

L'Organismo di Vigilanza proporrà le modifiche e/o integrazioni del Modello al Consiglio di Amministrazione dell'Associazione, che delibererà sulle stesse ai fini della loro approvazione.

## **PARTE SPECIALE – B**

### **DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI**

#### **1. PREMESSA**

Si riporta qui di seguito una breve descrizione delle singole fattispecie contemplate all'art. 24-bis del D. Lgs. 231/2001 (delitti informatici e di trattamento illecito dei dati).

I "*Delitti informatici e di trattamento illecito di dati*" sono stati introdotti fra le fattispecie di reato originariamente previste dal D. Lgs. 231/2001 dalla Legge 18 marzo 2008, n. 48 "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero*".



Oggetto di tutela per la disciplina in esame sono i sistemi informatici (da intendersi come “qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l’elaborazione automatica di dati” - art. 1 della Convenzione di Budapest del 23 novembre 2001) e i dati informatici (da intendersi come “qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l’elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione” –sempre all’art. 1 della Convenzione di Budapest del 23 novembre 2001).

Per completezza si riporteranno tutte le fattispecie previste dalla normativa, anche se, non tutte sono applicabili al Centro Studi Città di Foligno.

Va evidenziato, infatti, che l’Associazione è un Ente di diritto privato ed i suoi Amministratori e Dipendenti non sono Pubblici Ufficiali né Incaricati di Pubblico Servizio, che l’attività svolta dall’Associazione non è sanitaria, né forense e che presso il Centro Studi non vengono svolti servizi di pubblica necessità. Ciò determina l’inapplicabilità di tutte le fattispecie di reato che prevedono quale autore un Pubblico Ufficiale o un Incaricato di Pubblico Servizio (c.d. reati propri, cioè quei reati che richiedono il possesso di specifiche qualità personali in capo all'autore).

## **1.1. LE FATTISPECIE RILEVANTI DEI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI (ART. 24 BIS DEL D. LGS. 231/2001)**

Come anticipato, l’art. 7 della Legge 48/2008 ha introdotto nel Decreto 231/2001 l’art. 24-bis “*Delitti informatici e trattamento illecito di dati*”, che introduce la responsabilità amministrativa degli Enti per i reati di seguito individuati:

### **Documenti informatici (art. 491 bis C.P.)**

*“Se alcune 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”.*

La norma conferisce valenza penale alla commissione di reati di falso attraverso l’utilizzo di documenti informatici. I reati di falso richiamati dall’articolo in esame sono i seguenti:

**- Falsità materiale commessa dal Pubblico Ufficiale in atti pubblici (art. 476 C.P.)**



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

**- Falsità materiale commessa dal Pubblico Ufficiale in certificati o autorizzazioni amministrative (art. 477 C.P.)**

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

**- Falsità materiale commessa dal Pubblico Ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 C.P.)**

*“Il Pubblico Ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.*

*Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.*

*Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni”.*

**- Falsità ideologica commessa dal Pubblico Ufficiale in atti pubblici (art. 479 C.P.)**

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

**- Falsità ideologica commessa dal Pubblico Ufficiale in certificati o autorizzazioni amministrative (art. 480 C.P.)**

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



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

*“Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00.*

*Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro”.*

**- Falsità materiale commessa da privato (art. 482 C.P.)**

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

**- Falsità ideologica commessa dal privato in atto pubblico (art. 483 C.P.)**

*“Chiunque attesta falsamente al Pubblico Ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.*

*Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi”.*

**- Falsità in registri e notificazioni (art. 484 C.P.)**

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

**- Falsità in scrittura privata (art. 485 C.P.)**

*“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.*

*Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata”.*

**- Falsità in foglio firmato in bianco. Atto privato (art. 486 C.P.)**

*“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.*



*Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito”.*

**- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 C.P.)**

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

**- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 C.P.)**

*“Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private”.*

**- Uso di atto falso (art. 489 C.P.)**

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

*Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno”.*

**- Soppressione, distruzione e occultamento di atti veri (art. 490 C.P.)**

*“Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente”.*

**- Copie autentiche che tengono luogo degli originali mancanti (art. 492 C.P.)**

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

**- Falsità commesse da pubblici impiegati Incaricati di un Pubblico Servizio (art. 493 C.P.)**

*“Le disposizioni degli articoli precedenti sulle falsità commesse da Pubblici Ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, Incaricati di un Pubblico Servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni”.*

**Accesso abusivo a un sistema informatico o telematico (art. 615 ter C.P.)**



*“1. 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.*

*2. 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.*

*3. 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.*

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

Commette il delitto 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 prevista la pena della reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni, 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 che ineriscono alla funzione o al servizio, da chi esercita la professione di investigatore privato o da un operatore del sistema che abusi della sua qualità; se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui descritti riguardino sistemi informatici o telematici di interesse militare o di interesse pubblico (sicurezza pubblica, sanità, protezione civile), la pena è aumentata.



## **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater C.P.)**

*“Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.*

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

Il delitto è commesso da chiunque, per procurare a sé o ad altri un guadagno o arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

## **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies C.P.)**

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

Commette il delitto chiunque, per danneggiare in modo illecito un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero per 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.

## **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater C.P.)**



*“1. 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.*

*2. 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.*

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

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

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

*2) da un Pubblico Ufficiale o da un Incaricato di un Pubblico Servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;*

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

Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Salvo che il fatto costituisca più grave reato, la norma punisce con la stessa pena chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

La pena è aumentata se il reato è commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, da un Pubblico Ufficiale o da un Incaricato di un Pubblico Servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, con abuso della qualità di operatore del sistema, e da chi esercita, anche abusivamente, la professione di investigatore privato.

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

*“1. 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.*



2. *La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater”.*

Compie tale delitto chiunque, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

### **Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis C.P.)**

*“1. 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.*

*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 della reclusione da uno a quattro anni.”*

Il delitto, salvo che il fatto costituisca più grave reato, consiste nella distruzione, nel deterioramento, nella cancellazione, nell’alterazione o nella soppressione di informazioni, dati o programmi informatici altrui, da chiunque posta in essere. Il reato è aggravato se commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

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

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

*2. 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.*

*3. 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”.*

Il delitto, che può essere commesso da chiunque, consiste, salvo che il fatto costituisca più grave reato, nella commissione di 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. La pena è maggiore se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l’alterazione o la soppressione delle informazioni,



dei dati o dei programmi informatici o se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

### **Danneggiamento di sistemi informatici e telematici (art. 635 quater C.P.)**

*“1. 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.*

*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”*

Il delitto, salvo che il fatto costituisca più grave reato, è commesso da chiunque, mediante le condotte di cui all'articolo 635-bis C.P., 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. 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.

### **Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 quinquies C.P.)**

*“1. Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*

*2. 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.*

*3. 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.”*

Il delitto è commesso 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. 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 aumentata. 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.

### **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies C.P.)**

*“1. Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.”*

Commette il delitto il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

## **2. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI NELL'AMBITO DEI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI**

Come già specificato, poiché il Centro Studi Città di Foligno è un'Associazione governata da un Consiglio di Amministrazione che occupa un solo dipendente, per organizzare l'attività lavorativa non c'è una suddivisione interna in uffici, mentre le aree di attività si suddividono in organizzativa e formazione.

Nelle presente Parte Speciale si considerano, quindi, le sole attività svolte e non le aree.

L'analisi dei processi, effettuata conformemente a quanto prescritto dall'art. 6, comma 2, lettera a), del D. Lgs. 231/2001, ha consentito di individuare le attività dell'Associazione coinvolte in processi astrattamente esposti al rischio di commissione delle fattispecie di reato richiamate dall'art. 24-bis del D. Lgs. 231/2001.

Le fattispecie di reato indicate si applicano, in via potenziale, a tutte le attività ed a tutti i destinatari del M.O.G. (siano essi dipendenti o collaboratori) che, nell'espletamento delle attività di propria competenza, siano coinvolti, a qualsiasi titolo, nella gestione e nell'utilizzo dei sistemi informatici dell'Associazione.

Tutti i processi e le attività dell'Associazione risultano, infatti, potenzialmente coinvolti, data la pervasività nell'uso dei sistemi informatici e tutti coloro che, dipendenti e non, nell'espletamento delle attività di propria competenza, siano coinvolti a qualsiasi titolo nella gestione e nell'utilizzo dei sistemi informativi dell'Associazione sono interessati.



In particolare, le attività sensibili sono:

1. Gestione degli accessi a dati e sistemi, dei profili utente e del processo di autenticazione informatici;
2. Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio;
3. Gestione e protezione della postazione di lavoro;
4. Gestione degli accessi da e verso l'esterno;
5. Gestione e protezione delle reti;
6. Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD);
7. Gestione e protezione dei dispositivi di firma elettronica e delle relative password di utilizzo.

### **3. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE**

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, dai dipendenti, nonché da agenti, rappresentanti e consulenti, come meglio definiti nella parte generale, coinvolti nelle attività sensibili.

Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati presupposto in materia di delitti informatici e di trattamento illecito dei dati.

I processi descritti in questo paragrafo devono risultare adeguatamente formalizzati ed aggiornati e dovranno essere sottoposti a continuo monitoraggio e verifica da parte dell'Organismo di Vigilanza.

#### **3.1. OBBLIGHI**

E' fatto obbligo a tutti i destinatari del Modello di:

1. Osservare tutte le disposizioni legislative e regolamentari applicabili alle attività indicate nella presente Sezione;
2. Osservare lo Statuto dell'Associazione, il M.O.G. compresi i relativi allegati, il Codice Etico, le decisioni del Consiglio di Amministrazione e degli altri Organi sociali, le disposizioni dei superiori gerarchici e tutte le politiche e procedure interne che disciplinano l'attività dell'Associazione;
3. Impostare e mantenere i rapporti con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza, a garanzia dell'autonomia e della correttezza delle decisioni di quest'ultima;



4. Garantire che ogni operazione e/o transazione, intesa nel senso più ampio del termine, sia legittima, autorizzata, coerente, congrua, documentata, registrata ed in ogni tempo tracciabile e verificabile;

5. Garantire che le informazioni rese alla Pubblica Amministrazione e la documentazione prodotta rispondano ai principi di veridicità, completezza, correttezza;

Sulla base degli standard di riferimento internazionali, per sistema di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che il Centro Studi Città di Foligno si pone sono i seguenti:

- Integrità: garanzia che ogni dato dell'Associazione sia realmente e completamente rappresentativo, in maniera oggettiva e senza interpretazioni, dei contenuti a cui si riferisce. Tale obiettivo si persegue tramite l'adozione di opportune contromisure che impediscano alterazioni incidentali o intenzionali che ne possono mutare il significato originale o, in alternativa, forniscano la possibilità di rilevare la suddetta alterazione del dato e di recuperare il dato integro;
- Riservatezza: garanzia che un dato trattato dall'Associazione venga reso disponibile solamente alle applicazioni ed agli utenti incaricati e autorizzati al suo utilizzo;
- Disponibilità: garanzia di reperibilità dei dati in funzione delle esigenze di continuità dei processi e di rispetto delle norme (di legge e non) che impongono la conservazione storica.

### **3.2. DIVIETI**

La presente Parte Speciale prevede l'espreso divieto per i destinatari del M.O.G., compresi i collaboratori esterni, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o combinatamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (24-bis del D. Lgs. 231/2001);
- violare i principi e le procedure previste nella presente Parte Speciale.

In particolare, la presente Parte Speciale prevede, conseguentemente, le seguenti norme di comportamento con riferimento ai soggetti sopra indicati:

- a) divieto di alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;



- b) divieto di accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) divieto di accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;
- d) divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di altri soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- e) divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico, al fine di acquisire informazioni riservate;
- f) divieto di svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- g) divieto di svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- h) divieto di installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- i) divieto di svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- j) divieto di svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- k) divieto di distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- l) divieto di utilizzare, sfruttare, diffondere o riprodurre indebitamente a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali, opere dell'ingegno di qualsiasi natura coperte dal diritto d'autore (in proposito si rinvia alla sezione della parte speciale dedicata alla tutela del Diritto d'autore);
- m) divieto di accedere in maniera non autorizzata ai sistemi informatici della Pubblica Amministrazione;
- accedere in maniera non autorizzata ai sistemi informatici utilizzati dalla Pubblica Amministrazione e/o di alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi



modalità a cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare indebitamente informazioni a vantaggio dell'Associazione o di terzi, o comunque al fine di procurare un indebito vantaggio all'Associazione o a terzi.

### **3.3. DOVERI DI CONDOTTA**

I destinatari del M.O.G. devono:

1. Osservare tutte le disposizioni legislative e regolamentari applicabili alle attività indicate nella presente Sezione;
2. Osservare lo Statuto dell'Associazione, il M.O.G. compresi i relativi allegati, il Codice Etico, le decisioni del Consiglio di Amministrazione e degli altri Organi sociali, le disposizioni dei superiori gerarchici e tutte le politiche e procedure interne che disciplinano l'attività dell'Associazione, con particolare riferimento alle fattispecie di reato rientranti tra quelle sopra considerate (24-bis del d.lgs. 231/2001);
3. Utilizzare le informazioni, le applicazioni e le apparecchiature informatiche fornite dall'Associazione esclusivamente per motivi di ufficio;
4. Non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile interno;
5. Segnalare al Responsabile interno il furto, il danneggiamento o lo smarrimento di tali strumenti; Qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire al Responsabile interno l'originale della denuncia all'Autorità di Pubblica Sicurezza;
6. Evitare di introdurre e/o conservare (in forma cartacea, informatica e mediante utilizzo di strumenti dell'Ente), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo che siano acquisiti con il loro espresso consenso, possibilmente fornito per iscritto;
7. Evitare di trasferire all'esterno dell'Associazione e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Associazione stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del Responsabile interno;
8. Evitare di lasciare incustodito e/o accessibile ad altri il proprio PC;



9. Custodire accuratamente le proprie credenziali d'accesso ai sistemi informatici del Centro Studi e aggiornare periodicamente le password, evitando che terzi soggetti possano venirne a conoscenza;
10. Evitare l'utilizzo di password di altri utenti e non accedere ad aree protette in nome e per conto di questi;
11. Evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
12. Utilizzare la connessione a Internet e la posta elettronica per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative che hanno reso necessario il collegamento e mai per motivi personali;
13. Rispettare le procedure e gli standard previsti, segnalando senza ritardo eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
14. Impiegare sulle apparecchiature del Centro Studi solo prodotti ufficialmente acquistati dall'Associazione stessa;
15. Astenersi dall'effettuare copie, non specificamente autorizzate, di dati e di software;
16. Astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
17. Osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Associazione;
18. Osservare scrupolosamente quanto previsto dalle politiche di sicurezza dell'Associazione per la protezione ed il controllo dei sistemi informatici.

Inoltre, le attività svolte da parte di fornitori terzi in materia di:

- Networking
- Gestione applicativi
- Gestione sistemi hardware

devono rispettare i principi e le regole dell'Associazione, al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed infrastrutturali.

### **3.4. PRINCIPI PROCEDURALI SPECIFICI**

Qui di seguito sono elencati gli standard di controllo individuati per le singole Attività Sensibili rilevate.



-Disposizioni sulla Sicurezza Informatica: lo standard richiede l'esistenza di una politica in materia di sicurezza del sistema informatico che preveda, fra l'altro:

a) le modalità di comunicazione anche a terzi;

b) le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi.

-Organizzazione della sicurezza informatica per gli utenti interni: lo standard richiede la definizione dei ruoli e delle responsabilità nella gestione delle modalità di accesso e di identificazione di utenti interni e degli obblighi dei medesimi nell'utilizzo dei sistemi informatici.

-Organizzazione della sicurezza informatica per gli utenti esterni: lo standard richiede la definizione dei ruoli e delle responsabilità nella gestione delle modalità di accesso di utenti esterni all'Associazione e degli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

-Sicurezza fisica e ambientale: lo standard richiede l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

-Gestione delle comunicazioni e dell'operatività: lo standard richiede che si assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi. In particolare, andrà assicurato:

a) il corretto e sicuro funzionamento degli elaboratori;

b) la protezione da software pericoloso;

c) il backup di informazioni e software;

d) la protezione dello scambio di informazioni anche con terzi;

e) gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;

f) una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;

g) la gestione di dispositivi rimovibili.

-Controllo degli accessi: lo standard richiede di disciplinare gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni.

In particolare, si prevede:

a) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password od altro sistema di autenticazione sicura;



- b) le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
- c) una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
- d) la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
- e) la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
- h) la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
- i) la custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.);
- j) l'adozione di regole di clear screen per gli elaboratori utilizzati.

-Gestione degli incidenti e dei problemi di sicurezza informatica: lo standard richiede di prevedere adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, si dovrà:

- a) comunicare immediatamente al Responsabile interno l'esistenza di eventuali problemi;
- b) far effettuare da tecnici specializzati l'analisi periodica di tutti gli incidenti singoli e ricorrenti con l'individuazione della root cause e l'analisi di report e trend sugli incidenti e sui problemi individuando idonee azioni preventive;
- c) l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
- d) verificare i problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva.

-Risorse umane e sicurezza: lo standard richiede di prevedere:

- a) specifiche attività di formazione e aggiornamenti periodici sulle procedure di sicurezza informatica per i dipendenti e, dove rilevante, per i collaboratori;
- b) l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- c) la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

-Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi: lo standard richiede l'adozione di uno strumento normativo che definisca:



- a) l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
- b) la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- c) la confidenzialità, autenticità e integrità delle informazioni;
- d) la sicurezza nel processo di sviluppo dei sistemi informativi.

I principi di controllo volti a prevenire i comportamenti illeciti previsti dagli artt. 24-bis del D. Lgs. 231/2001 sono:

- svolgimento periodico di attività di valutazione dei rischi nell'ambito della gestione dei sistemi informatici;
- autorizzazione del Responsabile interno per l'attivazione, la modifica o la cessazione di un profilo utente;
- verifica periodica delle credenziali utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;
- comunicazione della prima password di accesso ai sistemi informativi in modalità confidenziale. Sarà cura di ogni dipendente provvedere alla successiva sostituzione e curarne la custodia e la non divulgazione;
- gestione delle credenziali di autenticazione ai sistemi informativi con criteri equipollenti a quanto previsto dal D. Lgs. 196/2003 e s.m.i. (tra cui la previsione di vincoli di sicurezza alfanumerici della password, politiche di rinnovo periodico delle password, ecc.);
- accesso ai sistemi informativi tramite autenticazione univoca dell'utente;
- gli indirizzi di posta elettronica di cui sono dotati i dipendenti sono nominativi e ad esclusivo uso lavorativo;
- garantire la protezione contro potenziali attacchi esterni attraverso l'utilizzo di software antivirus (aggiornato in modo automatico, che effettua controlli in entrata e in uscita);
- effettuare tutti gli aggiornamenti dei sistemi operativi e degli applicativi suggeriti dai produttori al fine di limitare i possibili rischi legati a vulnerabilità riscontrate negli stessi;
- installazione da parte di personale specializzato dei software sulle postazioni di lavoro dei dipendenti;
- tutti i programmi installati sulle postazioni di lavoro devono essere dotati di licenza;



- personale specializzato effettuerà una verifica annuale dei software presenti sulle postazioni dei vari utenti, rimuovendo i software vietati o privi di licenza;
- effettuazione di controlli periodici dei software installati sui server;
- definizione di piani di backup periodici dei dati, file, programmi e sistemi operativi, al fine di garantire la salvaguardia del patrimonio informativo. I backup sono opportunamente conservati e sono eseguiti i relativi test di restore allo scopo di verificare l'integrità dei dati archiviati;
- aggiornamenti hardware e software rilasciati solo da persone autorizzate;
- esecuzione di attività di monitoraggio sugli apparati di rete;
- solo il personale preventivamente autorizzato può accedere alle aree riservate di siti di enti pubblici o privati;
- accesso ad internet regolamentato e filtrato da un sistema di web filtering;
- esecuzione periodica di attività di vulnerability assessment.

#### **4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA**

I compiti dell'Organismo di Vigilanza, concernenti la valutazione sull'efficacia delle procedure e l'osservanza delle prescrizioni del Modello in materia di prevenzione dei Delitti Informatici e di trattamento illecito dei dati, sono i seguenti:

- verifica periodica, con il supporto del personale, del rispetto dei divieti e dei principi procedurali previsti dalla Parte Generale del M.O.G e dalla presente Parte Speciale a presidio delle attività individuate come a rischio;
- raccolta ed esame di eventuali segnalazioni riguardanti irregolarità riscontrate o situazioni di particolare criticità ricevute dal Responsabile interno, da un dipendente, o da terzi;
- effettuazione delle attività di controllo periodico e disposizione degli accertamenti ritenuti necessari e opportuni a seguito delle segnalazioni ricevute;
- effettuazione periodica di controlli a campione, diretti a verificare la corretta esplicazione delle attività connesse ai processi sensibili relativi ai Delitti Informatici e di trattamento illecito dei dati, anche in relazione ai principi espressi nel presente documento ed, in particolare, alle procedure interne in essere;
- monitoraggio sull'efficacia dei presidi organizzativi e di controllo e proposta di eventuali modifiche/integrazioni;



□ valutazione delle esigenze formative del personale in materia da proporre all'approvazione del Consiglio di Amministrazione, individuandone i destinatari.

Qualora, nell'espletamento dei compiti di cui sopra, l'Organismo di Vigilanza riscontri violazioni delle regole e dei principi contenuti nella presente parte speciale del Modello ne deve dare immediata informazione al Presidente del Consiglio di Amministrazione.

Qualora le violazioni siano imputabili al Presidente del Consiglio di Amministrazione, l'Organismo, secondo opportunità, riferirà agli altri membri del Consiglio di Amministrazione o all'Assemblea dei Soci, tramite il Collegio Sindacale.

Allo stesso modo il Presidente del Consiglio di Amministrazione dovrà informare l'Organismo di Vigilanza circa le procedure di accertamento delle violazioni, l'irrogazione di sanzioni o l'archiviazione di un provvedimento disciplinare qualora le violazioni riguardino norme di comportamento disciplinate nel "Modello Organizzativo".

## **5. MODIFICHE ED AGGIORNAMENTI DELLA PRESENTE PARTE SPECIALE**

Le attività individuate come "a rischio" potranno essere modificate e/o integrate a seguito degli aggiornamenti delle attività di risk mapping e risk assessment effettuate di volta in volta dall'Associazione -anche su richiesta dell'O.d.V.- a seguito del verificarsi di situazioni quali, a titolo esemplificativo, cambiamenti organizzativi, aggiornamenti legislativi, realizzazione di reati presupposto nell'ambito dell'Associazione, piani di miglioramento del Modello ecc.

L'Organismo di Vigilanza proporrà le modifiche e/o integrazioni del Modello al Consiglio di Amministrazione dell'Associazione, che delibererà sulle stesse ai fini della loro approvazione.



**PARTE SPECIALE – C**  
**DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D’AUTORE**

**1. LE FATTISPECIE RILEVANTI DEI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D’AUTORE (ART. 25-NONIES DEL D. LGS.231/2001)**

L’articolo 25-nonies del D. Lgs. 231/2001, introdotto dall’art. 15, comma 7, lett. c), della Legge 23 luglio 2009, n. 39 e rubricato “*Delitti in materia di violazione del diritto d’autore*”, così recita:

*“1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633 (di seguito indicata anche come “Legge sul diritto d’autore”), si applica all’Ente la sanzione pecuniaria fino a cinquecento quote.*

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

In particolare gli articoli e commi indicati della Legge 633/1941 prevedono:

**- art. 171 comma 1**

*“Salvo quanto previsto dall’art. 171- bis e dall’articolo 171-ter, è punito con la multa da lire 100.000 a lire 4.000.000 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un’opera dell’ingegno protetta, o parte di essa;”*

e comma 3 *“La pena è della reclusione fino ad un anno o della multa non inferiore a lire 1.000.000 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.”*

**- art. 171-bis:**



*“1. 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 lire cinque milioni a lire trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.*

*2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da 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.”;*

**- art. 171-ter:**

*“1. E' punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da cinque a trenta milioni di lire 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, 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 (S.I.A.E.), 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) 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.

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 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.

2. E' punito con la reclusione da uno a quattro anni e con la multa da cinque a trenta milioni di lire 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'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante concessioni 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 le attività illecite di cui al comma 1.*

*3. La pena è diminuita se il fatto è di particolare tenuità.*

*4. 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;*

*e) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.*

*5. 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.”;*

**- art. 171-septies:**

*“1. 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.”;*

**- art. 171-octies:**

*“1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da lire cinque milioni a lire cinquanta milioni 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.*

*2. La pena non è inferiore a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.”;*

**- art. 174-quinquies:**

*“1. Quando esercita l'azione penale per tal uno dei reati non colposi previsti dalla presente sezione commessi nell'ambito di un esercizio commerciale o di un'attività soggetta ad autorizzazione, il pubblico ministero ne dà comunicazione al questore, indicando gli elementi utili per l'adozione del provvedimento di cui al comma 2.*

*2. Valutati gli elementi indicati nella comunicazione di cui al comma 1, il questore, sentiti gli interessati, può disporre, con provvedimento motivato, la sospensione dell'esercizio o dell'attività per un periodo non inferiore a quindici giorni e non superiore a tre mesi, senza pregiudizio del sequestro penale eventualmente adottato.*

*3. In caso di condanna per taluno dei reati di cui al comma 1, è sempre disposta, a titolo di sanzione amministrativa accessoria, la cessazione temporanea dell'esercizio o dell'attività per un periodo da tre mesi ad un anno, computata la durata della sospensione disposta a norma del comma 2. Si applica l'articolo 24 della legge 24 novembre 1981, n. 689. In caso di recidiva specifica è disposta la revoca della licenza di esercizio o dell'autorizzazione allo svolgimento dell'attività.*

*4. Le disposizioni di cui al presente articolo si applicano anche nei confronti degli stabilimenti di sviluppo e di stampa, di sincronizzazione e postproduzione, nonché di masterizzazione, tipografia e che comunque esercitino attività di produzione industriale connesse alla realizzazione dei supporti contraffatti e nei confronti dei centri di emissione o ricezione di programmi televisivi. Le agevolazioni di cui all' art. 45 della legge 4 novembre 1965, n. 1213, e successive modificazioni, sono sospese in caso di esercizio dell'azione penale; se vi è condanna, sono revocate e non possono essere nuovamente concesse per almeno un biennio.”.*

Le norme in esame tutelano il diritto morale e di utilizzo economico da parte del loro autore:

- delle opere dell'ingegno aventi carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione;

- dei programmi per elaboratore, come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con la Legge 20 giugno



1978, n. 399, nonché delle banche di dati che, per la scelta o la disposizione del materiale, costituiscono una creazione intellettuale dell'autore.

In particolare, sono comprese nella protezione:

- 1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto in forma scritta quanto orale;
- 2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale;
- 3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti;
- 4) le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia;
- 5) i disegni e le opere dell'architettura;
- 6) le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del capo quinto del titolo secondo;
- 7) le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia;
- 8) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore;
- 9) le banche di dati intese come *“raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo”*. La tutela delle banche di dati non si estende peraltro al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto;
- 10) le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico.

Sono inoltre protette, come creazioni originali, le opere collettive, che racchiudono in sé più opere dell'ingegno o parti di esse, e le elaborazioni creative di opere dell'ingegno preesistenti, quali le traduzioni in un'altra lingua (es. il doppiaggio cinematografico), i rifacimenti e gli adattamenti.

I diritti d'autore scaturiscono da un fatto creativo che deve essere percepibile all'esterno e che acquista, quindi, una forma espressiva.

Non è necessario che la creazione sia fermata su un supporto, potendosi avere una forma espressiva, ad esempio, anche nella comunicazione orale, ma viene escluso che la mera idea, proprio perché inespressa, sia protetta dal diritto d'autore.

La creazione costituisce opera dell'ingegno quando, come espressione della personalità dell'autore, è caratterizzata dalla novità e dall'originalità. Due requisiti questi che possono sussistere, come si è visto, anche nelle opere collettive, per lo più opere letterarie come le enciclopedie e i giornali –



riguardo alle quali, l'attività creativa consiste più propriamente nell'apporto di colui che organizza e dirige l'assemblamento di opere preesistenti – e nelle elaborazioni di carattere creativo di un'opera dell'ingegno altrui.

I diritti morali sorgono in capo all'autore dell'opera dell'ingegno per il mero fatto della creazione. A differenza dei diritti di utilizzazione economica, sono inalienabili e possono essere fatti valere in qualunque tempo, anche quando si sia privi della possibilità di disporre economicamente del bene oggetto di tutela.

Anche i diritti di utilizzazione economica, come i diritti morali, sorgono generalmente dal solo fatto della creazione; fanno però eccezione la creazione di banche dati, di programmi per elaboratore e di opere di disegno industriale da parte del lavoratore dipendente. In questi casi, mentre restano intransferibili i diritti morali dell'autore-dipendente, i diritti di utilizzazione vengono invece acquisiti a titolo originario dal datore di lavoro.

Diverso è il caso del produttore di un'opera cinematografica, che sarà titolare esclusivo dei diritti di utilizzazione che hanno ad oggetto lo sfruttamento cinematografico dell'opera, salvi comunque i diritti morali ed economici dei quattro coautori (autore del soggetto, autore della sceneggiatura, autore della musica e regista), rispetto all'opera cinematografica (cfr. art. 46 della Legge 633/1941 - *“Legge sul diritto d'autore”*) e salvi i loro diritti esclusivi di utilizzazione sui singoli contributi (il soggetto, la sceneggiatura e la musica, non invece la regia), che non pregiudichino i diritti del produttore.

Il significato di questa previsione si chiarisce quando si consideri che, senza i mezzi produttivi e l'attività di organizzazione del film, diviene impensabile che i contributi creativi dei singoli coautori possano trovare una realizzazione cinematografica e che, quindi, l'apporto conferito dal produttore cinematografico è imprescindibile. I diritti di utilizzazione del film sono comunque limitati allo sfruttamento dell'opera ed è previsto che il produttore non possa modificare o trasformare l'opera, se non nei limiti delle modifiche necessarie all'adattamento cinematografico.

Si distinguono, dai diritti di utilizzazione, i diritti connessi del produttore cinematografico. Essi non sono qualificabili come diritti d'autore, neppure in senso economico, perché attengono ad una serie di situazioni ritenute dalla legge meritevoli di tutela indipendentemente dalla creazione di un'opera dell'ingegno<sup>7</sup>.

---

<sup>7</sup> La previsione dei diritti connessi ha risposto all'esigenza di prevenire la pirateria fonografica e videografica, come fenomeno contrastante con le legittime aspettative di guadagno del produttore fonografico o cinematografico, il quale – indipendentemente dal contenuto del supporto prodotto – ha il diritto di godere dello sfruttamento economico di esso o



Le fattispecie, alle quali fa riferimento l'articolo 25-nonies del D. Lgs. 231/2001, in materia di violazione del diritto d'autore, sono:

- *Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, e senza averne diritto, di un'opera o di parte di un'opera dell'ingegno protetta* (art. 171, co. 1, lett a-bis), L. 633/1941).

- *Reato di cui al punto precedente commesso su un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, qualora ne risulti offeso l'onore o la reputazione dell'autore* (art. 171, co. 3, L. 633/1941).

In base all'art. 171, comma 1, lett. a-bis) "*chiunque 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 è punito con la multa da euro 51 a euro 2.065*".

A questa previsione corrisponde ad esempio l'uploading (il "caricamento" in rete) di un'opera dell'ingegno protetta, compresi file musicali o audiovisivi. Sebbene tale operazione sia generalmente funzionale al cosiddetto file sharing, e quindi alla condivisione e allo scambio di musica o film con altri fruitori, si deve sottolineare che la condotta di messa a disposizione del pubblico in reti telematiche di materiale protetto assume rilevanza penale a prescindere dalla sua finalità e può quindi ben essere realizzata all'interno, ad esempio, di un sito web, attraverso l'immissione di materiale "non autorizzato".

Il delitto in oggetto si consuma con la sola "messa a disposizione" del pubblico e, quindi, in questo caso, con l'uploading dell'opera dell'ingegno.

Occorre precisare che quando lo stesso fatto ora descritto sia diretto a fine di lucro, si ricadrà nelle previsioni di cui all'art. 171-ter, secondo comma, lett. a-bis.

---

delle copie che ne derivino e quindi il diritto esclusivo di autorizzarne operazioni come la riproduzione, la distribuzione, la messa a disposizione del pubblico o il noleggio.

Anche coloro che esercitano l'attività di emissione radiofonica o televisiva sono titolari di diritti connessi, tra i quali il diritto esclusivo di autorizzare la fissazione, la riproduzione, la distribuzione o la messa a disposizione del pubblico delle proprie emissioni.

Vi sono poi i diritti connessi spettanti agli artisti interpreti ed esecutori, come i musicisti, i ballerini e i cantanti, i quali hanno il diritto esclusivo non soltanto di autorizzare la fissazione delle proprie prestazioni artistiche, ma altresì di autorizzare e di trarre un guadagno, ad esempio, dalla riproduzione, dalla distribuzione o dal noleggio di tali fissazioni. Indipendentemente dai diritti connessi, i produttori di fonogrammi, gli interpreti e gli esecutori, hanno inoltre il diritto di ricevere un compenso per l'utilizzazione a scopo di lucro dei fonogrammi (da essi prodotti o sui quali è stata autorizzata la fissazione delle prestazioni artistiche) a mezzo della cinematografia, della diffusione radiofonica e televisiva, ivi compresa la comunicazione al pubblico via satellite.



Una seconda ipotesi di messa a disposizione del pubblico in un sistema di reti telematiche di opere dell'ingegno, si può configurare attraverso l' "offerta" di un flusso di dati audio o video (streaming), che possono essere visti o uditi nel corso della "emissione" e quindi anche quando non siano salvati sul computer. Anche lo streaming "non autorizzato" sembra possa ricorrere ogniqualvolta tra i contenuti dei programmi immessi in rete constino delle immagini o dei suoni protetti dal diritto d'autore, sui quali non si abbiano i diritti di utilizzazione.

In base all'art. 171, comma 3, se il descritto reato di cui alla lettera a-bis è commesso su un'opera altrui non destinata alla pubblicità ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti un'offesa all'onore o alla reputazione dell'autore si applica la pena della reclusione fino ad un anno o della multa non inferiore a euro 516.

- art. 171-bis, co. 1, L. 633/1941:

*"1. 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 lire cinque milioni a lire trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità."*

Tale comma descrive la condotta illecita per il tramite di una pluralità di espressioni ("abusivamente duplica [...] programmi per elaboratore o [...] importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione"), tutte richiamanti particolari modalità di utilizzo del software per elaboratore ed idonee ad arrecare un pregiudizio agli interessi patrimoniali che fanno capo al titolare dei relativi diritti di sfruttamento.

In sostanza, l'indicazione del comportamento vietato viene operata dall'art. 171-bis facendo riferimento al contenuto dei vari diritti di utilizzazione economica dell'opera dell'ingegno.

Relativamente alla nozione di duplicazione, tale condotta, con riferimento al software, consiste, in primo luogo, una copiatura dei files da un supporto materiale - che può essere l'hard disk di un personal computer, un floppy disk, un compact-disc - ad un altro supporto - di tipologia analoga a quella ora indicata - di modo che l'autore della duplicazione viene in possesso dei dati "senza che la precedente situazione di fatto venga modificata a danno del soggetto già possessore originario.



Tuttavia le attività indicate dalla norma non presuppongono necessariamente la sussistenza di un supporto materiale e potrebbero quindi essere commesse anche attraverso il downloading non autorizzato di un programma.

Si ritengono comprese nella previsione in esame le violazioni della licenza d'uso di un programma, per cui si risponderà di abusiva riproduzione anche quando non si ottemperi alle condizioni contrattuali che regolano i rapporti tra il titolare dei corrispondenti diritti e il fruitore del programma.

Peraltro, per essere penalmente rilevante, la duplicazione deve determinare la produzione di una copia identica del programma, non invece la rielaborazione o la creazione di un nuovo software, anche se simile, a condizione che per tale operazione non sia stato indebitamente utilizzato o modificato il programma cui ci si "ispira".

È invece esclusa dallo spettro della norma la copia "di back up", quella copia di riserva che l'utente produce per evitare la perdita del programma.

Inoltre, si rileva che la duplicazione o distribuzione non autorizzata del programma deve essere diretta ad un fine di profitto. Un obiettivo che va oltre il fine di lucro, non esaurendosi in una finalità di guadagno, bensì caratterizzando anche le condotte ispirate da una finalità di risparmio, nel senso di una mancata diminuzione patrimoniale (es. l'utilizzazione dello stesso programma su più postazioni).

Per quanto concerne lo scopo commerciale o imprenditoriale che deve connotare la detenzione del programma, si tratta di finalità che attengono al contesto dell'azione, per cui tale attività (statica) rileverà non soltanto quando sia destinata alla vendita, ma anche quando sia diretta ad un uso meramente interno del programma in un'azienda, o nel caso in cui esso risulti utile o necessario nello svolgimento dell'attività imprenditoriale.

La medesima norma punisce, inoltre, la locazione di programmi non contrassegnati dalla SIAE, in quelle ipotesi in cui sia previsto il contrassegno (non lo è, ad esempio, per i programmi come i sistemi operativi, i driver e quei software acquisibili esclusivamente attraverso download da internet). La ragione è chiara se si considera che i diritti di utilizzazione economica sono fra loro indipendenti, potendo essere ceduti singolarmente.

La Società italiana degli autori ed editori (SIAE) appone un contrassegno su ogni supporto contenente programmi per elaboratore o multimediali, nonché su ogni supporto contenente suoni, voci o immagini in movimento, che reca la fissazione di opere o di parti di opere, destinati ad essere posti comunque in commercio o ceduti in uso a qualunque titolo a fine di lucro.



Tale contrassegno deve avere, comunque, caratteristiche tali da non poter essere trasferito su altro supporto; deve contenere elementi tali da permettere l'identificazione del titolo dell'opera per la quale è stato richiesto, del nome dell'autore, del produttore o del titolare del diritto d'autore; deve, infine, indicare un numero progressivo per ogni singola opera riprodotta o registrata nonché la sua destinazione alla vendita, al noleggio e a qualsiasi altra forma di distribuzione.

Soltanto il supporto che sia passato per l'intermediazione (pressoché) necessaria della SIAE, anche quando esso non sia soggetto a contrassegno, garantisce che siano stati rispettati i diritti di utilizzazione economica sull'opera dell'ingegno in esso racchiusa.

La seconda parte del primo comma dell'art. 171-bis punisce le condotte di duplicazione, distribuzione, vendita, detenzione, locazione riferite (non ai supporti contenenti il programma informatico, bensì) a *“qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratore”*. In relazione a tale fattispecie è prevista la pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493.

La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 (lire trenta milioni) se il fatto è di rilevante gravità.

La norma in parola realizza una forma di anticipazione della tutela degli interessi patrimoniali aggrediti, volta a prevenire l'accesso e l'abusiva duplicazione del software mediante, appunto, l'uso di mezzi idonei a rimuovere o eludere i sistemi di protezione, come dimostrato dal fatto che la norma richiede *“che il mezzo al quale si fa riferimento abbia come finalità unica quella di superare le protezioni poste a salvaguardia del software”*.

- art. 171-bis, co. 2, L. 633/1941

*“2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da 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.”*



Relativamente alla condotta di cui all'art. 171-bis, 2 comma, si rileva che l'illiceità della condotta non è ascrivibile all'esercizio ordinario delle attività di interrogazione per uso privato compiute da parte degli utenti a ciò autorizzati e sul presupposto di una gestione normale della banca dati; essa scatta solo a condizione che si travalichino i limiti gestionali della raccolta o si determini un danno al costituente, come accade ad esempio in ipotesi di estrazione e reimpiego per uso commerciale e finalizzati a concorrere slealmente con il prodotto del costituente.

La fattispecie è punita con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493. 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.

- Reati commessi a fini di lucro, per uso non personale, e caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 1, L. 633/1941: - abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, di dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento (lett. a);

- abusiva riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati (lett. b);

- introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, messa in commercio, concessione in noleggio o cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo televisione con qualsiasi procedimento, trasmissione a mezzo radio, delle duplicazioni o riproduzioni abusive di cui alle lettere a) e b) senza aver concorso nella duplicazione o riproduzione (lett. c);

- detenzione per la vendita o la distribuzione, messa in commercio, vendita, noleggio, cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo radio o televisione con qualsiasi procedimento, di videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o altro supporto per il quale è prescritta l'apposizione del contrassegno SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato (lett. d);



- ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato, in assenza di accordo con il legittimo distributore (lett. e);
- introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, vendita, concessione in noleggio, cessione a qualsiasi titolo, promozione commerciale, installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso a un servizio criptato senza il pagamento del canone dovuto (lett. f);
- fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per la vendita o il noleggio, o detenzione per scopi commerciali, di attrezzature, prodotti o componenti ovvero prestazione di servizi aventi impiego commerciale o prevalente finalità di eludere efficaci misure tecnologiche di protezione ovvero progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di tali misure (lett. f-bis);
- abusiva rimozione o alterazione di informazioni elettroniche sul regime dei diritti di cui all'articolo 102-quinquies, ovvero distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, comunicazione o messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (lett. h).

Tali casi sono puniti con la pena della reclusione da sei mesi a tre anni e con la multa da euro 2.582 ad euro 15.493.

- Reati caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 2, della L. 633/1941: - riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi (lett. a);
- immissione a fini di lucro in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera o parte di un'opera dell'ingegno protetta dal diritto d'autore, in violazione del diritto esclusivo di comunicazione al pubblico spettante all'autore (lett. a-bis);
- realizzazione delle condotte previste dall'art. 171-ter, co. 1, della L. 633/1941, da parte di chiunque eserciti in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, ovvero importazione di opere tutelate dal diritto d'autore e da diritti connessi (lett. b);
- promozione od organizzazione delle attività illecite di cui all'art. 171-ter, co. 1, della L. 633/1941 (lett. c).



Tali casi sono puniti con la pena della reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493.

Le previsioni dell'art.171 ter commi 1 e 2 sono poste a tutela dei diritti dei produttori fonografici e videografici e sono tese a sanzionare la cosiddetta "pirateria" fono e videografica.

Devono essere autorizzate dall'avente diritto la riproduzione e la diffusione in pubblico di quelle opere dell'ingegno che siano destinate alla vendita e al mercato televisivo e cinematografico, così come devono essere autorizzate la riproduzione e la diffusione di supporti che contengano fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive.

Alla medesima autorizzazione sono soggette la riproduzione o la diffusione di opere letterarie, drammatiche, musicali etc., o di parti di esse, poiché tali diritti appartengono esclusivamente al titolare dei diritti di utilizzazione economica dell'opera: quando tali attività vengano eseguite abusivamente e siano destinate al commercio (in ciò ritenendosi integrato il fine di lucro), configureranno il delitto in esame.

I diritti dei produttori o comunque dei titolari dei diritti di sfruttamento dell'opera dell'ingegno si riterranno altresì violati anche da coloro che, pur non avendo materialmente riprodotto o diffuso le opere protette o i supporti videografici o fonografici contenenti un'opera dell'ingegno, li detengano per la vendita o per la distribuzione, li proiettino in pubblico o li trasmettano per radio o per televisione o li facciano ascoltare in pubblico.

Se è il produttore ad avere il diritto esclusivo di sfruttare economicamente l'opera prodotta, ciascuna delle operazioni indicate, che sia quindi diretta a conseguire un lucro indebito, raffigura infatti un illecito sfruttamento economico dell'opera.

Alla medesima ragione si ispira la previsione penale dei casi in cui le operazioni sopra indicate abbiano ad oggetto supporti non contrassegnati dalla SIAE (nei casi in cui il contrassegno sia obbligatorio): la mancanza del contrassegno, secondo la norma, fa, infatti, presumere l'illiceità del supporto.

Una seconda ipotesi di reato si configura quando colui che abbia fruito di un'opera "ad accesso condizionato", la ritrasmetta o diffonda, senza averne l'autorizzazione.

Nella stessa ottica di tutela sono punite la fabbricazione, la distribuzione e la pubblicizzazione a scopo di vendita o di noleggio, o la detenzione a scopo commerciale di dispositivi che consentano l'accesso illecito a servizi ad accesso condizionato (al pagamento di un canone); così come la rimozione (non consentita) dei dispositivi antipirateria e la diffusione di materiale protetto da cui tali dispositivi siano stati rimossi. La tutela penale dei diritti di utilizzazione economica dell'opera



protetta, se da un lato si estende a quelle attività che minaccino la violazione del diritto d'autore, dall'altro conduce a punire anche chi si sia avvantaggiato del materiale in tal modo "alterato".

- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno, da parte di produttori o importatori di tali supporti, ovvero falsa dichiarazione circa l'assolvimento degli obblighi sul contrassegno (art. 171-septies, L. 633/1941).

Anche i supporti per i quali non sia previsto il contrassegno non si sottraggono alla intermediazione della SIAE, per cui il produttore o l'importatore, che intenda metterli in commercio sul territorio nazionale, avrà l'obbligo di comunicare tempestivamente alla SIAE i dati identificativi dell'opera.

- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies, L. 633/1941).

La norma punisce non soltanto chi installi e utilizzi (per uso pubblico o privato) per fini fraudolenti i decodificatori di trasmissioni televisive criptate ("ad accesso condizionato" "indipendentemente dall'imposizione di un canone"), ma anche chi produca o distribuisca gli stessi apparecchi. È prevista la pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 25.822.

La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 (lire trenta milioni) se il fatto è di rilevante gravità.

## **2. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI NELL'AMBITO DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE**

Come già specificato, poiché il Centro Studi Città di Foligno è un'Associazione governata da un Consiglio di Amministrazione che occupa un solo dipendente, per organizzare l'attività lavorativa non c'è una suddivisione interna in uffici, mentre le aree di attività si suddividono in organizzativa e formazione.

Nelle presente Parte Speciale si considerano, quindi, le sole attività svolte e non le aree.

L'analisi dei processi, effettuata conformemente a quanto prescritto dall'art. 6, comma 2, lettera a), del D. Lgs. 231/2001, ha consentito di individuare ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-nonies del D. Lgs. 231/2001. Esse sono:

1. Attività di formazione;
2. Acquisto di copie o esemplari di opere;



3. Installazione di programmi informatici protetti (es. software e banche dati).

### **3. PRINCIPI DI COMPORTAMENTO**

La presente Parte Speciale prevede l'espreso divieto a carico degli Organi dell'Associazione, dei Dipendenti e dei Collaboratori Esterni, in particolar modo dei Docenti e Formatori, ma anche dei Consulenti informatici di:

- 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 (art. 25-nonies del d.lgs. 231/2001);
- violare i principi e le procedure previste nella presente Parte Speciale.

Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati presupposto in materia di delitti informatici e di trattamento illecito dei dati.

I processi descritti in questo paragrafo devono risultare adeguatamente formalizzati ed aggiornati e dovranno essere sottoposti a continuo monitoraggio e verifica da parte dell'Organismo di Vigilanza.

#### **3.1. OBBLIGHI**

I destinatari della presente parte speciale devono:

1. Osservare tutte le disposizioni legislative e regolamentari applicabili alle attività indicate nella presente Sezione;
2. Osservare lo Statuto dell'Associazione, il M.O.G. compresi i relativi allegati, il Codice Etico, le decisioni del Consiglio di Amministrazione e degli altri Organi sociali, le disposizioni dei superiori gerarchici e tutte le politiche e procedure interne che disciplinano l'attività dell'Associazione, con particolare riferimento alle fattispecie di reato rientranti tra quelle sopra considerate
3. Acquistare, realizzare, mettere in rete o comunque a disposizione di un pubblico unicamente contenuti (fotografie, sequenze video, poesie, commenti, recensioni, articoli e altri contenuti scritti, files di musica di qualsiasi formato) con licenza d'uso o comunque in regola con la normativa in materia di diritto d'autore e degli altri diritti connessi al loro utilizzo;
4. Evitare ogni abusiva riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati;



5. Verificare preventivamente, con il massimo rigore e tempestività, che i contenuti diffusi siano conformi alle normative vigenti in materia di diritto d'autore e diritti connessi all'utilizzo delle opere dell'ingegno protette;
6. Verificare che per tutti i contenuti di cui sopra acquistati dall'Associazione, rispettino le norme in materia di diritto d'autore e gli altri diritti connessi all'utilizzo delle opere dell'ingegno;
7. Utilizzare solo software con licenza d'uso e nei limiti ed alle condizioni previste dalla normativa vigente e dalla licenza medesima, ad eccezione di quei programmi per elaboratore disponibili per il download e utilizzo libero, sempre alle condizioni e nei limiti previsti dalla legge o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo;
8. Utilizzare solo banche dati con licenza d'uso e nei limiti ed alle condizioni previste dalla normativa vigente e dalla licenza medesima ad eccezione di quelle liberamente consultabili, sempre alle condizioni e nei limiti previsti dalla legge o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo, anche per quanto attiene alla ricerca, estrazione, elaborazione, rielaborazione e pubblicazione dei dati ivi contenuti.

### **3.2. DIVIETI**

La presente Parte Speciale prevede l'espreso divieto per i destinatari del M.O.G., compresi i collaboratori esterni, di:

- mettere illegittimamente a disposizione del pubblico un'opera dell'ingegno protetta, o parte di essa, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere;
- duplicare abusivamente, importare, distribuire, vendere, detenere, installare, concedere in locazione programmi per elaboratore contenuti in supporti non contrassegnati SIAE;
- utilizzare mezzi atti a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione dei programmi di cui sopra;
- riprodurre, trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico illegittimamente il contenuto di una banca dati, ovvero estrarre o reimpiegare illegittimamente distribuire, installare, vendere, concedere in locazione la stessa o i dati ivi contenuti;
- duplicare, riprodurre, trasmettere o diffondere in pubblico illegittimamente un'opera dell'ingegno destinata al circuito televisivo, cinematografico o a quello della vendita o del noleggio, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di



immagini in movimento su qualsiasi supporto, opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali;

- introdurre nel territorio dello Stato, detenere per la vendita, vendere, o comunque cedere a qualsiasi titolo, o trasmettere con qualsiasi mezzo le duplicazioni o riproduzioni abusive di cui sopra;

- detenere per la vendita, vendere, cedere a qualsiasi titolo, trasmettere con qualsiasi mezzo fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento su qualsiasi supporto, per il quale sia obbligatorio il contrassegno SIAE, privo di tale contrassegno o dotato di contrassegno contraffatto o alterato;

- ritrasmettere o diffondere con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato, in assenza di accordo con il legittimo distributore;

- introdurre nel territorio dello Stato, detenere per la vendita, vendere, cedere a qualsiasi titolo, promuovere commercialmente, installare dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

- fabbricare, importare, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per vendita o noleggio, detenere per scopi commerciali o utilizzare a scopo commerciale attrezzature, prodotti o componenti atti ad eludere le "misure tecnologiche di protezione" poste a tutela del diritto d'autore e degli altri diritti connessi al suo esercizio;

- rimuovere abusivamente o alterare "informazioni elettroniche" poste a tutela del diritto d'autore e degli altri diritti connessi al suo esercizio, ovvero distribuire, importare a fini di distribuzione, diffondere, comunicare con qualsiasi mezzo o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse;

- produrre, porre in vendita, importare, promuovere, installare, modificare, utilizzare per uso pubblico e privato, a fini fraudolenti, apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

### 3.3. DOVERI DI CONDOTTA

I destinatari del M.O.G. devono:



1. Osservare tutte le disposizioni legislative e regolamentari applicabili alle attività indicate nella presente Sezione;
2. Osservare lo Statuto dell'Associazione, il M.O.G. compresi i relativi allegati, il Codice Etico, le decisioni del Consiglio di Amministrazione e degli altri Organi sociali, le disposizioni dei superiori gerarchici e tutte le politiche e procedure interne che disciplinano l'attività dell'Associazione, con particolare riferimento alle fattispecie di reato rientranti tra quelle sopra considerate (25-nonies del D. Lgs. 231/2001);
3. rispettare le previsioni di legge a tutela della paternità delle opere nonché le limitazioni previste al diritto di duplicazione di programmi per elaboratore e di riproduzione, trasferimento, distribuzione e/o comunicazione del contenuto di banche dati e di opere protette dal diritto d'autore;
4. verificare - in fase di ricezione di supporti contenenti programmi per elaboratore, banche di dati, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive e/o sequenze di immagini in movimento - della presenza sugli stessi del contrassegno da parte delle autorità preposte alla vigilanza in materia di diritto d'autore, ovvero dell'esenzione dei supporti in questione da tale obbligo;
5. non lasciare incustodita, non prestare o cedere a terzi qualsiasi opera dell'ingegno acquistata dall'Associazione, senza la preventiva autorizzazione del Responsabile interno;
6. segnalare al Responsabile interno il furto, il danneggiamento o lo smarrimento di tali opere;
7. vigilare che i docenti rispettino le previsioni di legge a tutela della paternità delle opere nonché le limitazioni previste al diritto di duplicazione.

### **3.4. PRINCIPI PROCEDURALI SPECIFICI**

Qui di seguito sono elencati gli standard di controllo individuati per le singole Attività Sensibili rilevate.

- Attività Editoriale e di Docenza

Lo svolgimento delle attività tanto editoriali, quanto di docenza prevede l'obbligo di rispettare le prescrizioni dettate dalla normativa in materia di tutela del diritto morale e patrimoniale d'autore, con specifico riferimento all'utilizzo, conservazione e distribuzione di testi, musiche, disegni, immagini, fotografie, programmi per elaboratore e banche di dati protetti dal diritto d'autore (di seguito indicate anche come "opere").



In particolare, devono essere rispettate, non solo dal personale del Centro Studi Città di Foligno, ma anche dai soggetti esterni -compresi i professionisti esterni che svolgono attività di docenza-:

1. le disposizioni di legge applicabili con riferimento all'acquisizione, conservazione, utilizzo, riproduzione, duplicazione, elaborazione, diffusione e distribuzione (anche attraverso reti telematiche) delle opere o di loro parti;
2. le previsioni di legge a tutela della paternità delle opere;
3. le previsioni di legge nell'installazione di programmi informatici (es. software e banche dati) che dovranno essere originali e protetti. L'attività verrà svolta nel rispetto degli standard di controllo riportati nella Parte Speciale – B, dedicata ai “Delitti informatici e trattamento illecito dei dati”, alla quale si rimanda.
4. le previsioni di legge a tutela della paternità delle opere nonché le limitazioni previste al diritto di duplicazione di programmi per elaboratore e di riproduzione, trasferimento, distribuzione e/o comunicazione del contenuto di banche dati.

-Attività d'ufficio.

Devono essere rispettate, non solo dal personale del Centro Studi Città di Foligno, ma anche dai soggetti esterni che prestano la loro opera nell'Associazione:

1. le disposizioni di legge applicabili con riferimento all'acquisizione, conservazione, utilizzo, riproduzione, duplicazione, elaborazione, diffusione e distribuzione (anche attraverso reti telematiche) delle opere o di loro parti;
2. le previsioni di legge a tutela della paternità delle opere;
3. le previsioni di legge nell'installazione di programmi informatici (es. software e banche dati) che dovranno essere originali e protetti. L'attività verrà svolta nel rispetto degli standard di controllo riportati nella Parte Speciale – B, dedicata ai “Delitti informatici e trattamento illecito dei dati”, alla quale si rimanda.
4. le previsioni di legge a tutela della paternità delle opere nonché le limitazioni previste al diritto di duplicazione di programmi per elaboratore e di riproduzione, trasferimento, distribuzione e/o comunicazione del contenuto di banche dati;
5. la verifica - in fase di ricezione di supporti contenenti programmi per elaboratore, banche di dati, fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive e/o sequenze di immagini in movimento - della presenza sugli stessi del contrassegno da parte delle autorità preposte alla vigilanza in materia di diritto d'autore, ovvero dell'esenzione dei supporti in questione da tale obbligo.



#### **4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA**

I compiti dell'Organismo di Vigilanza, concernenti la valutazione sull'efficacia delle procedure e l'osservanza delle prescrizioni del Modello in materia di prevenzione dei Delitti in materia di violazione del diritto d'autore, sono i seguenti:

- verifica periodica, con il supporto del personale, del rispetto dei divieti e dei principi procedurali previsti dalla Parte Generale del M.O.G e dalla presente Parte Speciale a presidio delle attività individuate come a rischio;
- raccolta ed esame di eventuali segnalazioni riguardanti irregolarità riscontrate o situazioni di particolare criticità ricevute dal Responsabile interno, da un dipendente, o da terzi;
- effettuazione delle attività di controllo periodico e disposizione degli accertamenti ritenuti necessari e opportuni a seguito delle segnalazioni ricevute;
- effettuazione periodica di controlli a campione, diretti a verificare la corretta esplicazione delle attività connesse ai processi sensibili relativi ai delitti in materia di violazione del diritto d'autore, anche in relazione ai principi espressi nel presente documento ed, in particolare, alle procedure interne in essere;
- monitoraggio sull'efficacia dei presidi organizzativi e di controllo e proposta di eventuali modifiche/integrazioni;
- valutazione delle esigenze formative del personale da proporre all'approvazione del Consiglio di Amministrazione, individuandone i destinatari.

Qualora, nell'espletamento dei compiti di cui sopra, l'Organismo di Vigilanza riscontri violazioni delle regole e dei principi contenuti nella presente parte speciale del Modello ne deve dare immediata informazione al Presidente del Consiglio di Amministrazione.

Qualora le violazioni siano imputabili al Presidente del Consiglio di Amministrazione, l'Organismo, secondo opportunità, riferirà agli altri membri del Consiglio di Amministrazione o all'Assemblea dei Soci, tramite il Collegio Sindacale.

Allo stesso modo il Presidente del Consiglio di Amministrazione dovrà informare l'Organismo di Vigilanza circa le procedure di accertamento delle violazioni, l'irrogazione di sanzioni o l'archiviazione di un provvedimento disciplinare qualora le violazioni riguardino norme di comportamento disciplinate nel "Modello Organizzativo".



## **5. MODIFICHE ED AGGIORNAMENTI DELLA PRESENTE PARTE SPECIALE**

Le attività individuate come “a rischio” potranno essere modificate e/o integrate a seguito degli aggiornamenti delle attività di risk mapping e risk assessment effettuate di volta in volta dall’Associazione -anche su richiesta dell’O.d.V.- a seguito del verificarsi di situazioni quali, a titolo esemplificativo, cambiamenti organizzativi, aggiornamenti legislativi, realizzazione di reati presupposto nell’ambito dell’Associazione, piani di miglioramento del Modello ecc.

L’Organismo di Vigilanza proporrà le modifiche e/o integrazioni del Modello al Consiglio di Amministrazione dell’Associazione, che delibererà sulle stesse ai fini della loro approvazione.

