PARTE SPECIALE M

REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

Parte speciale M
REATI IN MATERIA
DI VIOLAZIONE DEL DIRITTO DI AUTORE

La “parte speciale M” è dedicata alla trattazione dei reati in materia di violazione del diritto di autore così come individuati nell’art. 24 *novies* d.lgs. n. 231 del 2001.

Di seguito viene riportato l’elenco delle fattispecie criminose prese in considerazione dalle suddette disposizioni, le modalità attraverso le quali queste fattispecie criminose possono essere compiute nonché le “macro aree” sensibili, i ruoli aziendali coinvolti e i “protocolli di prevenzione” attuati all’interno della Società. Infine, vengono riportati anche i c.d. “processi strumentali” e i compiti generali dell’OdV.

Ai fini del presente documento si considera Protocollo di prevenzione “una specifica connotazione di una variabile organizzativa, secondo cui è progettata l’attività sensibile o che agisce sugli output della stessa, con l’effetto di azzerare o ridurre la probabilità o la frequenza con cui può essere compiuto un reato del catalogo di cui al d.lgs. n. 231 del 2001”.

Legge del 22 aprile 1941 n. 633: Protezione del diritto d’autore e di altri diritti connessi al suo esercizio

Art. 171 comma 1, lett. a-bis e comma 3

Testo della norma

1. Salvo quanto previsto dall’art. 171-*bis* e dall’art. 171-*ter*, è punito con la multa da euro 51,00 a euro 2.065,00 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 di ingegno protetta, o parte di essa;

[…]

3. La pena è della reclusione fino ad un anno o della multa non inferiore ad euro 516,00 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.

Autore del reato

L’illecito penale in esame è un reato comune, può essere commesso da “Chiunque”.

Descrizione

La lettera a-*bis*) incrimina la condotta di messa a disposizione del pubblico, tramite immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa, cioè di opere altrui senza averne diritto.

La legge tutela indifferentemente la messa a disposizione di un'opera protetta per intero o in una sua parte, accentuando l'importanza delle modalità di condotta, cioè l'immissione dell'opera in un sistema di reti telematiche.

La condotta in esame rientra tra le forme di riproduzione con tecnologia digitale o, in ogni caso, rileva come una elusione del divieto di realizzare copie dell'opera protetta.

Trattandosi di un reato di mera condotta per la cui realizzazione non è richiesto il verificarsi dell'eventolesivo, l'arrecare offesa all'onore o alla reputazione dell'autore dell'opera costituisce motivo di aggravamentodi pena ai sensi del comma 3.

Nel panorama giurisprudenziale, i casi più frequenti di illecita diffusione attraverso la rete telematica riguardano le composizioni musicali, le opere cinematografiche e le composizioni cartacee o informatiche aventi ad oggetto materie giuridiche, economiche e bancarie.

L'elemento soggettivo è il dolo generico.

In tema di concorso di persone, si segnala un'importante sentenza della Suprema Corte (Cass., sez. III, 10 ottobre 2006, n. 33945), la quale ha ravvisato il «concorso nel reato di abusiva diffusione mediante internet di immagini protette da diritto di esclusiva anche in capo al soggetto che, pur non avendole immesse in rete, abbia inoltrato sul web in epoca antecedente alla loro immissione ad opera di altri, informazioni sui collegamenti e sui programmi necessari alla loro visione, in tal modo agevolando la connessione e la loro indebita diffusione».

La prima ipotesi prevista dal comma 3 fa riferimento ad un'opera altrui, escludendo che il reato possa essere compiuto dall'autore dell'opera. Oggetto dell'illecito è un'opera non destinata alla pubblicazione: vengono, perciò, tutelati gli inediti.

La seconda ipotesi di usurpazione della paternità dell'opera fa riferimento al c.d. plagio, che ricorre quando un'opera viene presentata con una paternità non rispondente al vero. Il plagio è integrato sia dalla riproduzione, totale o parziale, degli elementi creativi di un'opera altrui con usurpazione della paternità, sia dalla contraffazione, intesa quale sfruttamento dei diritti economici nascenti dall'opera protetta senza il consenso dell'autore.

La terza ipotesi fa riferimento a modificazioni dell'opera e prevede, invece, un intervento su un'opera non viziata dalle illiceità di cui sopra, vale a dire un'opera pubblicata o destinata alla pubblicazione e provvista di paternità, usurpando quest'ultima ovvero deformando o modificando la stessa, qualora ne risulti un'offesa all'onore ed alla reputazione.

In quest'ultimo caso la produzione dell'offesa è da qualificarsi come condizione obiettiva di punibilità.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera di ingegno protetta, o parte di essa.

- La Società mette a disposizione del pubblico, immettendola in un sistema di reti telematiche,mediante connessioni di qualsiasi genere, un'opera di ingegno protetta, o parte di essa, quando l'opera è altrui e non destinata alla pubblicazione, offendendo l'onore e la reputazione dell'autore.
- La Società mette a disposizione del pubblico, immettendola in un sistema di reti telematiche,mediante connessioni di qualsiasi genere, un'opera di ingegno protetta, o parte di essa, plagiando un'opera altrui e offendendo l'onore e la reputazione dell'autore.
- La Società mette a disposizione del pubblico, immettendola in un sistema di reti telematiche,mediante connessioni di qualsiasi genere, un'opera di ingegno protetta, o parte di essa, offendendo l'onore e la reputazione dell'autore, con la deformazione, mutilazione o altra modificazione dell'operamedesima.

Art. 171-*bis*

1.1.1 Testo della norma

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 euro 2.582,00 a euro 15.493,00. 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 penanon è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493,00 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 inviolazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582,00 a euro 15.493,00. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493,00 se il fatto è di rilevante gravità.

Autore del reato

L'illecito penale in esame è un reato comune, può essere commesso da "Chiunque".

Descrizione

La norma in questione contempla due distinte ipotesi delittuose.

La fattispecie prevista dal comma 1 consiste nella duplicazione dei programmi per elaboratore o nella distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, o concessione in locazione dei programmi contenuti in supporti sprovvisti del contrassegno SIAE.

I programmi per elaboratore sono stati giuridicamente tutelati dal D. Lgs. 518/1992 – in attuazione della direttiva comunitaria 91/250/CEE – che li ha inseriti tra le opere letterarie protette a norma della Convenzione di Berna.

Nel caso della duplicazione, la condotta deve essere abusiva, cioè posta in essere in violazione delle norme che regolamentano la medesima attività.

Le altre condotte attengono alla commercializzazione di programmi contenuti in supporti privi del contrassegno SIAE.

L'ipotesi di cui al comma 2, invece, prende in considerazione il contenuto di una banca-dati. La condotta può consistere nella riproduzione su supporti non contrassegnati dalla SIAE, nel trasferimento su altro supporto, nella distribuzione, nella comunicazione, nella presentazione o dimostrazione in pubblico del contenuto di una banca-dati, in violazione di quanto previsto dagli artt. 64-*quinquies* e 64-*sexies*. Questi disciplinano le banche-dati prevedendo, nel primo, l'oggetto del diritto esclusivo dell'autore di eseguire o autorizzare la riproduzione, la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica, la riproduzione, distribuzione, presentazione, dimostrazione o comunicazione in pubblico; nel secondo, le attività non soggette ad autorizzazione dell'autore di una banca-dati.

In alternativa, sono incriminate le condotte di estrazione e reimpiego della banca-dati, in violazione delle disposizioni di cui agli artt. 102-*bis* e 102-*ter*, le quali disciplinano, rispettivamente, i diritti del costitutore di una banca-dati e i diritti e gli obblighi dell'utente.

Infine, sono punite le condotte di distribuzione, vendita e concessione in locazione di una banca-dati.

Comune a tutte le condotte è il fine di trarne profitto. L'elemento soggettivo è quindi il dolo specifico.

In relazione ai reati previsti dall'articolo in questione è prevista, a norma dell'art. 171 *sexies*, comma 2, la confisca dei supporti fonografici, audiovisivi, ecc. già duplicati, nonché degli strumenti e dei materiali non ancora utilizzati per commettere i reati stessi, ma destinati a commetterli.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società duplica, per trarne profitto, programmi per elaboratore; sono suscettibili di integrare il reato in questione tutte le duplicazioni di programmi informatici realizzate al di fuori delle forme previste dagli artt. 64 *bis*, 64 *ter* e 64 *quater* della L. n. 633 del 1941.

- La Società, per trarne profitto, realizza programmi ricavati dallo sviluppo o da modifiche del prodotto originale, quando di quest'ultimo sia replicata una parte funzionalmente autonoma e costituente, comunque, il nucleo centrale dell'opera protetta.

- La Società, per trarne profitto, 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). La mancanza del contrassegno SIAE, pur se non comunicato dallo Stato italiano alla Commissione Europea in adempimento della normativa comunitaria relativa alle “regole tecniche”, nel senso affermato dalla Corte di giustizia CE, mantiene valenza indiziaria dell’illecita duplicazione o riproduzione.

- La Società agisce con 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 Società, 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.

- La Società esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter.

- La Società distribuisce, vende o concede in locazione una banca di dati.

Art. 171-*ter*

Testo della norma

1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (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. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-*bis*) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza 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 in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
c) 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.

Autore del reato

L'illecito penale in esame è un reato comune, può essere commesso da "Chiunque".

Descrizione

La norma in esame prevede due diverse fattispecie di reato.

La prima ipotesi delittuosa, di cui al comma 1, è mirata a tutelare i diritti d'autore in relazione alla diffusione di sistemi di produzione di opere create per il circuito televisivo e per quello cinematografico a mezzo di videocassette.

L'elemento oggettivo del reato è rappresentato da una pluralità di condotte che, essenzialmente, si sostanziano nella abusiva duplicazione, riproduzione, trasmissione, diffusione in pubblico, vendita, noleggio e condotte assimilate.

Oggetto materiale del reato sono, principalmente, videocassette, musicassette o altri supporti contenenti fonogrammi o videogrammi di opere cinematografiche o audiovisive o sequenze di immagini in movimento non contrassegnate dalla SIAE.

Si riportano di seguito le condotte delineate dalla norma in esame.

La lett. a) contempla una serie di condotte riconducibili alla duplicazione abusiva.

La lett. b) punisce la abusiva riproduzione, trasmissione o diffusione in pubblico di una serie di opere.

La lett. c) sembra contemplare condotte riconducibili alla categoria della diffusione, ma in realtà pare mirare alla fase della prevenzione.

Le condotte previste dalla lett. d), invece, paiono riconducibili alla categoria della diffusione e commercializzazione di supporti irregolari, rispetto all'apposizione del contrassegno SIAE (che può essere assente, contraffatto o alterato).

Quanto previsto dalla lett. e) viene ricondotto alla categoria della diffusione abusiva di trasmissioni ad accesso condizionato.

Le condotte di cui alla lett. f) sembrano riconducibili alla categoria della diffusione di dispositivi atti ad eludere un servizio criptato.

La lett. f-*bis*) pare contemplare le condotte riconducibili alla categoria della diffusione di strumenti finalizzati ad eludere le misure di cui all'art. 102-*quater*.

La lett. h) contempla le condotte riconducibili alla categoria della diffusione di materiali protetti, nonché alla rimozione o alterazione delle informazioni elettroniche.

Elemento soggettivo del reato è il dolo specifico rappresentato dal fine di lucro.

Il comma 2 prevede ulteriori fattispecie criminose che integrano autonome ipotesi di reato e non sono qualificabili come circostanze aggravanti.

In particolare, si hanno quattro diverse figure delittuose:

1) la riproduzione, duplicazione, trasmissione o diffusione abusiva nonché vendita oimmissione in commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere protette dal diritto d'autore;
2) la comunicazione al pubblico con immissione in un sistema di reti telematiche, a fini di lucro di opere di ingegno protette dal diritto d'autore in violazione dell'art. 16 L. n. 633 del 1941 che sancisce a favore dell'autore stesso il diritto esclusivo di comunicazione al pubblico su filo o senza filo, ricomprendendo quindi l'impiego di tutti i mezzi di diffusione a distanza (es. telegrafo, telefono, radio, televisione, comunicazione via satellite, ritrasmissione via cavo);
3) il compimento di taluno dei fatti previsti nel primo comma del medesimo articolo nell'esercizio in forma imprenditoriale di attività di riproduzione, distribuzione, vendita o commercializzazione ovvero importazione di opere tutelate dal diritto d'autore;
4) la promozione o organizzazione delle attività illecite contemplate nel primo comma.

Al comma 3 è prevista la diminuzione della pena per i fatti di particolare tenuità, applicabile a tutte le fattispecie delittuose contemplate nel medesimo articolo.

Il comma 4, per la condanna per i soli reati contemplati dal comma 1, prevede l'applicazione delle pene accessorie della interdizione da una professione o da un'arte e della interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui rispettivamente agli artt. 30 e 32 *bis* c.p., la pubblicazione della sentenza e la sospensione per un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

In relazione ai reati previsti dall'articolo in questione è prevista, a norma dell'art. 171 *sexies*, comma 2, la confisca dei supporti fonografici, audiovisivi, ecc. già duplicati, nonché degli strumenti e dei materiali non ancora utilizzati per commettere i reati stessi, ma destinati a commetterli.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, per trarre profitto, pone in essere una condotta riconducibile alla duplicazione, alla riproduzione, alla trasmissione, alla diffusione, alla commercializzazione abusive di operevariamente qualificate (a norma dell'articolo in esame), opere dell'ingegno altrui o comunque contrassegnate da parte della SIAE, in violazione del diritto d'autore.

- La Società consente l'uso di una scheda elettronica che permette la ricezione dei programmitelevisivi a pagamento in un locale di pertinenza della stessa società e nell'ambito di attività di un circolo privato, cui accedono più persone dietro pagamento di una quota associativa, ma il contratto posto in essere con la società di trasmissione dei programmi prevede l'uso strettamente personale e familiare di tale strumento, con esclusione di finalità commerciali.
- La Società finanzia consapevolmente, per trarne profitto, un'attività consistente nel porre in vendita o rendere disponibili per il noleggio cassette o supporti abusivamente riprodotti.

Art. 171-septies

Testo della norma

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.

Autore del reato

L'illecito penale in esame è un reato comune, può essere commesso da "Chiunque". La lettera a), però, fa esplicito riferimento ai produttori e importatori dei supporti non soggetti al contrassegno SIAE.

Descrizione

La norma in questione, alla lett. a) estende l'applicazione dell'art. 171-*ter*, comma 1, ai produttori e importatori dei supporti non soggetti al contrassegno SIAE, qualora non comunichino a detto ente, entro trenta giorni dalla data di immissione in commercio o di importazione, i dati necessari alla univoca identificazione dei supporti immessi in commercio o importati.

La lett. b) estende la pena anche a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi derivanti dalla legge sul diritto d'autore e sui diritti connessi, con particolare riferimento alle ipotesi in cui l'apposizione del contrassegno SIAE sia facoltativa. Si tratta degli obblighi di dichiarare produttore e importatore sull'identificazione del prodotto, al fine di consentire un controllo di legittimità sullo stesso.

Le false dichiarazioni concernono le indicazioni, identificative dei prodotti, incombenti su chiunque, in alternativa all'apposizione del contrassegno SIAE, che attesta l'avvenuto controllo di legittimità.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, se produce o importa supporti non soggetti al contrassegno SIAE, non comunica a detto ente, entro trenta giorni dalla data di immissione in commercio o di importazione, i dati necessari alla univoca identificazione dei supporti immessi in commercio o importati.

- La Società dichiara falsamente l'avvenuto assolvimento degli obblighi derivanti dalla legge sul diritto d'autore e sui diritti connessi (obblighi di dichiarare produttore e importatore sull'identificazione del prodotto, al fine di consentire un controllo di legittimità sullo stesso), soprattutto nelle ipotesi in cui l'apposizione del contrassegno SIAE sia facoltativa.

Art. 171-octies

Testo della norma

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 euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

Autore del reato

L'illecito penale in esame è un reato comune, può essere commesso da "Chiunque".

Descrizione

La fattispecie in questione rappresenta un'ipotesi residuale, risultando applicabile solo ai casi in cui il fatto non costituisca più grave reato e, in particolare, qualora la condotta non sia sussumibile nella previsione di cui all'art. 171 *ter*, comma 1.

Le condotte sanzionate dalla norma in esame sono quelle del produrre, porre in vendita, importare, promuovere, installare, modificare, utilizzare per uso pubblico e privato gli apparati elencati, cioè, in buona sostanza, viene incriminata l'utilizzazione di materiale per la decodificazione di trasmissioni audiovisive ad accesso condizionato, che si sostanzia in una abusiva fruizione di tali programmi riservati.

Il fine perseguito è di natura fraudolenta.

Tale fattispecie di reato, rispetto alle altre sopra descritte, incrimina comportamenti prodromici rispetto alla captazione ed eventuale diffusione delle immagini e dei suoni.

Nel primo comma viene anche descritto cosa si intende per trasmissioni ad accesso condizionato, cioè sono 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.

Il comma 2 prevede l'aggravante per la rilevante gravità.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società produce, pone in vendita, importa, promuove, installa, modifica, utilizza, per uso pubblico o 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.

- La Società possiede apparecchiature denominate "splitty" attraverso le quali viene trasferita a più "decoders" la chiave di decodifica per l'accesso a trasmissioni audiovisive ad accesso condizionato.

1 Le “macro aree” di attività sensibili in relazione ai reati in materia di violazione del diritto di autore (art. 25-*novies*, D. Lgs. 231/01): elencazione.

Con riferimento agli illeciti sopra elencati, le aree di attività ritenute più specificamente a rischio risultano essere le seguenti:

1. Gestione dei sistemi informativi aziendali
2. Gestione del sito aziendale e della comunicazione
3. Gestione dei software e/o delle banche dati
4. Utilizzo di strumenti informatici aziendali
5. Impiego, a qualsiasi titolo, di prodotti contrassegnati SIAE, senza il contrassegno o con il contrassegno contraffatto o alterato
6. Impiego illecito di servizi criptati attraverso sistemi di codificazione
7. Impiego di strumenti atti ad eludere le misure tecnologiche di protezione e messa a disposizione delle opere prive della protezione stessa
8. Impiego illecito di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato

2 Le “macro aree” di attività sensibili e i ruoli aziendali coinvolti.

In occasione dell’implementazione dell’attività di *risk mapping*, sono state individuate, nell’ambito della struttura organizzativa ed aziendale di LED CITY s.r.l., delle “macro aree” di attività sensibili, ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati di cui al punto n. 1. Nell’elaborazione, queste “macro aree” – fortemente caratterizzate – sono state tuttavia immediatamente calate all’interno delle fattispecie di reato esaminate. Sono stati inoltre identificati i ruoli aziendali coinvolti nell’esecuzione di tali attività e che, astrattamente, potrebbero commettere i reati qui considerati.

Nell’espletamento delle rispettive attività/funzioni, oltre alle regole stabilite nel Modello di organizzazione, gestione e controllo (di seguito “Modello”), i soggetti aziendali coinvolti nella gestione delle “macro aree” di attività sensibili individuate in relazione ai reati in materia di violazione del diritto di autore di cui all’art. 25-*novies* del Decreto sono tenuti, al fine di prevenire e impedire il verificarsi dei reati qui considerati, al rispetto di una serie di “Protocolli preventivi.

Sono stati individuati, altresì, i “protocolli preventivi” predisposti dalla Società al fine di evitare che tali reati possano essere compiuti nell’interesse o a vantaggio della Società stessa; tali protocolli possono essere “PROTOCOLLI PREVENTIVI DI SISTEMA” o “PROTOCOLLI PREVENTIVI”, a seconda che riguardino, i primi, ad esempio, l’organizzazione della Società o la formazione del personale, ed i secondi, la previsione di prassi aziendali specifiche. Talvolta esistono “PROTOCOLLI PREVENTIVI SPECIFICI” che rappresentano vere e proprie procedure aziendali.

Di seguito è riepilogato il quadro in precedenza esposto.

Art. 171 comma 1, lett. a-*bis* e comma 3

1) GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI

ruoli aziendali coinvolti
Amministratore di sistema
Responsabile del sito web
Società di consulenza esterne

attività sensibili

- **a)** Gestione dell'attività di sviluppo di nuovi sistemi informativi
- **b)** Gestione dell'attività di manutenzione dei sistemi esistenti
- **c)** Gestione dell'attività di elaborazione dei dati
- **d)** Gestione della sicurezza informatica sia a livello fisico che a livello logico:
    1. Configurazione delle security policy dei firewall ai fini della tutela delle intrusioni esterne;
    2. Gestione e protezione dei back up dei dati
    3. Elaborazione di un Disaster Recovery Plan a tutela del patrimonio informativo

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esiste una procedura per il tracciamento e la documentazione della manutenzione dei sistemi, basati su due ambienti segregati (Società di consulenza esterne);
2. i sistemi sono monitorati e gestiti dai vari team di maintanance, sia a livello applicativo che infrastrutturale, secondo schedulazioni predefinite (Società di consulenza esterna);
3. esistono software per il controllo e le verifiche dello stato dei sistemi informatici (Società di consulenza esterne);
4. la rete privata, realizzata mediante collegamenti via cavo, è costituita da un server localizzato nell'area CED; dieci postazioni lavoro; un dispositivo di backup localizzato nell'area CED ad accessocontrollato; un pc portatile collegabile in rete;
5. oltre alle istruzioni generali, vengono fornite esplicite istruzioni ai dipendenti in merito alle modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici; la prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro; procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggerei sistemi informativi; procedure per il salvataggio dei dati; modalità di custodia ed utilizzo dei supportirimuovibili; il dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal Responsabile Sistemi informativi, sulle misure di sicurezza;
6. il DataCenter è protetto ed allarmato e l'accesso è consentito alle sole persone autorizzate; in particolare, al fine di scongiurare il rischio di perdita o danneggiamento dei dati a seguito di eventuali eventi distruttivi, i locali sono protetti da: dispositivi antincendio previsti dalla normativa vigente; gruppo di continuità dell'alimentazione elettrica; impianto di condizionamento. Sono inoltre adottate

le seguenti misure, al fine di impedire accessi non autorizzati: suonerie d'ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;

7. realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'l'identità delle persone che hanno accesso agli strumenti informatici; le postazioni di lavoro munite di videoterminale sono state dotate di password o parola chiave, che consentono l'accesso ai soli soggetti autorizzati a conoscenza di dette parole chiavi; l'accesso alla rete e ai sistemi aziendali è pertanto soggetto ad autenticazione mediante l'uso di UserID e Password personali; le password sono soggette a scadenza (ogni 6 mesi) e criteri di robustezza (Amministratore di sistema);
8. conferimento della qualifica di custode delle password e vice custode delle password a personale dell'azienda individuato, con l'obbligo di stilare un elenco di parole chiave e di mantenerlo aggiornato; obbligo di comunicazione, per i dipendenti, al custode delle password delle parole chiavee di eventuali variazioni, ulteriori rispetto alle modifiche obbligatorie periodiche (ogni 6 mesi);
9. protezione di strumenti e dati da malfunzionamenti e attacchi informatici. Tutta la rete della LED CITY s.r.l. è gestita a livello globale e protetta da firewall; ogni singolo pc ha installato un firewall (le policy sono gestite a livello corporate per le varie tipologie di firewall e non è possibile cambiarle localmente), che si attiva automaticamente quando il pc non è collegato alla rete aziendale, e un programma antivirus; il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione; aggiornamento trimestrale del sistema di protezione;
10. esiste una procedura di Disaster Recovery a tutela del patrimonio informativo della LED CITY s.r.l.;
11. esiste un dispositivo di backup localizzato nell'area CED ed esiste una procedura standardizzata e documentata per la gestione dei backup dei dati del server; previsione di procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema; il salvataggio dei dati avviene con frequenza giornaliera e le copie vengono custodite in luogo protetto;
12. aggiornamento delle misure di sicurezza; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup;
13. LED CITY s.r.l. ha chiaramente informato gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalle Società di consulenza esterne;
14. tutta la posta aziendale in uscita e in ingresso viene mantenuta e salvata ed è soggetta alle stesse regole di autenticazione degli altri sistemi aziendali;
15. il sistema di posta elettronica è protetto da un sistema ANTISPAM che blocca immediatamente l'ingresso della posta indesiderata;
16. il sistema è dotato di un web filtering perimetrale per evitare l'accesso di virus in azienda tramite web e per limitare l'accesso ad alcuni siti internet da parte degli utenti (black list);
17. gestione del sito online da parte di una Società di consulenza esterna e aggiornamento dei contenuti da parte del Responsabile Servizi informativi;
18. tutte le attività devono prevedere un sistema di autorizzazioni, deleghe e/o separazioni dei compiti, per ciascuna delle attività dei singoli processi;
19. la Società deve porre particolare attenzione affinché, nelle procedure riguardanti il processo di gestione dei sistemi informativi e in tutte le attività ad esso collegate, siano ben definite e controllate le responsabilità delle funzioni preposte allo sviluppo delle singole attività e che tali responsabilità siano coerenti con il quadro dei controlli specifici ai fini del D.Lgs. 231/01;
20. la funzione preposta deve informare l'OdV periodicamente – e comunque con frequenza almeno trimestrale – attraverso uno specifico report, sugli aspetti significativi afferenti le diverse attività di propria competenza, in particolare per quando attiene: le attività di salvaguardia delle attrezzature

hardware e dei programmi software; i controlli e le verifiche periodiche sull'efficienza del sistema. La funzione preposta ha l'obbligo di comunicare immediatamente all'OdV ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata (Amministratore di sistema).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

2) GESTIONE DEL SITO AZIENDALE E DELLA COMUNICAZIONE

ruoli aziendali coinvolti
Amministratore Unico/Direzione Generale (DG)
Responsabile Servizi Informativi
Società di consulenza esterna

attività sensibili
- **a)** Inserimento di dati aziendali nel sito della società
- **b)** Immissione di dati aziendali in sistemi di reti telematiche

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. individuazione di una procedura tesa a verificare la conformità ai requisiti di legge del materiale da pubblicare (DG);
2. individuazione di una figura aziendale volta a verificare l'inserimento del materiale sul sito aziendale (Responsabile del sito web);
3. gestione del sito online da parte di una Società di consulenza esterna e aggiornamento dei contenuti da parte del Responsabile Servizi informativi;
4. utilizzo del sito aziendale e delle comunicazioni nel rispetto delle norme di tutela della concorrenza e del mercato;
5. verifica circa l'utilizzo o la diffusione, sul sito, di opere dell'ingegno senza la necessaria autorizzazione e/o il pagamento dei dovuti compensi all'autore (es. produttore) (Società di consulenza esterna/Responsabile Servizi Informativi);
6. eventuale coinvolgimento di qualificati professionisti del settore nella valutazione circa l'esistenza o meno dei requisiti che determinano le caratteristiche tipiche di "opera dell'ingegno" e/o di "opera altrui" (DG);
7. divieto di utilizzare, in favore della società – anche attraverso sistemi informatici –, "opere dell'ingegno" e/o "opere altrui" senza avere seguito le procedure regolamentari previste dalla legge; necessità dell'evidenza di tale percorso (es. campagna pubblicitaria predisposta da società estere o direttamente da LED CITY s.r.l.);
8. evidenza documentale dei vari passaggi sopra richiamati e dei rapporti eventuali posti in essere (Responsabile Servizi Informativi).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare

Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

Art. 171-*bis*

1) GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI

ruoli aziendali coinvolti
Amministratore di sistema
Responsabile del sito web
Società di consulenza esterne

attività sensibili

- **a)** Gestione dell'attività di sviluppo di nuovi sistemi informativi
- **b)** Gestione dell'attività di manutenzione dei sistemi esistenti
- **c)** Gestione dell'attività di elaborazione dei dati
- **d)** Gestione della sicurezza informatica sia a livello fisico che a livello logico:
    1. Configurazione delle security policy dei firewall ai fini della tutela delle intrusioni esterne;
    2. Gestione e protezione dei back up dei dati
    3. Elaborazione di un Disaster Recovery Plan a tutela del patrimonio informativo

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esiste una procedura per il tracciamento e la documentazione della manutenzione dei sistemi, basati su due ambienti segregati (Società di consulenza esterne);
2. i sistemi sono monitorati e gestiti dai vari team di maintanance, sia a livello applicativo che infrastrutturale, secondo schedulazioni predefinite (Società di consulenza esterna);
3. esistono software per il controllo e le verifiche dello stato dei sistemi informatici (Società di consulenza esterne);

4. la rete privata, realizzata mediante collegamenti via cavo, è costituita da un server localizzato nell'area CED; dieci postazioni lavoro; un dispositivo di backup localizzato nell'area CED ad accessocontrollato; un pc portatile collegabile in rete;
5. oltre alle istruzioni generali, vengono fornite esplicite istruzioni ai dipendenti in merito alle modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici; la prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro; procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggerei sistemi informativi; procedure per il salvataggio dei dati; modalità di custodia ed utilizzo dei supportirimuovibili; il dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal Responsabile Sistemi informativi, sulle misure di sicurezza;
6. il DataCenter è protetto ed allarmato e l'accesso è consentito alle sole persone autorizzate; in particolare, al fine di scongiurare il rischio di perdita o danneggiamento dei dati a seguito di eventuali eventi distruttivi, i locali sono protetti da: dispositivi antincendio previsti dalla normativa vigente; gruppo di continuità dell'alimentazione elettrica; impianto di condizionamento. Sono inoltre adottate le seguenti misure, al fine di impedire accessi non autorizzati: suonerie d'ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;
7. realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'l'identità delle persone che hanno accesso agli strumenti informatici; le postazioni di lavoro munite di videoterminale sono state dotate di password o parola chiave, che consentono l'accesso ai soli soggetti autorizzati a conoscenza di dette parole chiavi; l'accesso alla rete e ai sistemi aziendali è pertanto soggetto ad autenticazione mediante l'uso di UserID e Password personali; le password sono soggette a scadenza (ogni 6 mesi) e criteri di robustezza (Amministratore di sistema);
8. conferimento della qualifica di custode delle password e vice custode delle password a personale dell'azienda individuato, con l'obbligo di stilare un elenco di parole chiave e di mantenerlo aggiornato; obbligo di comunicazione, per i dipendenti, al custode delle password delle parole chiavee di eventuali variazioni, ulteriori rispetto alle modifiche obbligatorie periodiche (ogni 6 mesi);
9. protezione di strumenti e dati da malfunzionamenti e attacchi informatici. Tutta la rete della LED CITY s.r.l. è gestita a livello globale e protetta da firewall; ogni singolo pc ha installato un firewall (le policy sono gestite a livello corporate per le varie tipologie di firewall e non è possibile cambiarle localmente), che si attiva automaticamente quando il pc non è collegato alla rete aziendale, e un programma antivirus; il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione; aggiornamento trimestrale del sistema di protezione;
10. esiste una procedura di Disaster Recovery a tutela del patrimonio informativo della LED CITY s.r.l.;
11. esiste un dispositivo di backup localizzato nell'area CED ed esiste una procedura standardizzata e documentata per la gestione dei backup dei dati del server; previsione di procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema; il salvataggio dei dati avviene con frequenza giornaliera e le copie vengono custodite in luogo protetto;
12. aggiornamento delle misure di sicurezza; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup;
13. LED CITY s.r.l. ha chiaramente informato gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalle Società di consulenza esterne;
14. tutta la posta aziendale in uscita e in ingresso viene mantenuta e salvata ed è soggetta alle stesse regole di autenticazione degli altri sistemi aziendali;

15. il sistema di posta elettronica è protetto da un sistema ANTISPAM che blocca immediatamente l'ingresso della posta indesiderata;
16. il sistema è dotato di un web filtering perimetrale per evitare l'accesso di virus in azienda tramite web e per limitare l'accesso ad alcuni siti internet da parte degli utenti (black list);
17. gestione del sito online da parte di una Società di consulenza esterna e aggiornamento dei contenuti da parte del Responsabile Servizi informativi;
18. tutte le attività devono prevedere un sistema di autorizzazioni, deleghe e/o separazioni dei compiti, per ciascuna delle attività dei singoli processi;
19. la Società deve porre particolare attenzione affinché, nelle procedure riguardanti il processo di gestione dei sistemi informativi e in tutte le attività ad esso collegate, siano ben definite e controllate le responsabilità delle funzioni preposte allo sviluppo delle singole attività e che tali responsabilità siano coerenti con il quadro dei controlli specifici ai fini del D.Lgs. 231/01;
20. la funzione preposta deve informare l'OdV periodicamente – e comunque con frequenza almeno trimestrale – attraverso uno specifico report, sugli aspetti significativi afferenti le diverse attività di propria competenza, in particolare per quando attiene: le attività di salvaguardia delle attrezzature hardware e dei programmi software; i controlli e le verifiche periodiche sull'efficienza del sistema. La funzione preposta ha l'obbligo di comunicare immediatamente all'OdV ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata (Amministratore di sistema).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

2) GESTIONE DEI SOFTWARE E/O DELLE BANCHE DATI

ruoli aziendali coinvolti
Amministratore Unico/Direzione Generale (DG)
Amministratore di sistema
Responsabile del sito web
Responsabile Servizi Informativi
Società di consulenza esterne

attività sensibili

- **a)** Riproduzione e duplicazione di software e/o di banche dati su supporti non contrassegnati SIAE;
- **b)** detenzione abusiva, anche a scopi commerciali, di software e/o di banche dati non contrassegnati SIAE;
- **c)** commercializzazione, modificazione e impostazione di software e/o di banche dati non contrassegnati SIAE.

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esistenza di una mappatura dei dispositivi hardware e dei programmi software (Responsabile Sistemi Informativi; Amministratore di sistema);
2. mappatura delle licenze software e delle banche dati (Responsabile Sistemi Informativi; Amministratore di sistema);
3. individuazione di una figura aziendale deputata a gestire l'aggiornamento della mappatura sia dei dispositivi hardware e software, sia delle licenze relative a software e banche dati (Responsabile Sistemi Informativi; Amministratore di sistema; Società di consulenza esterna);
4. individuazione di una diversa figura aziendale deputata a verificare la corrispondenza tra i programmi software e le banche dati lecitamente detenute e quelle "in generale" utilizzate (Responsabile Sistemi Informativi; Amministratore di sistema; Società di consulenza esterna);
5. verifica periodica circa l'utilizzo, la detenzione, la commercializzazione, la duplicazione e la riproduzione di software e banche dati non contrassegnati SIAE (Responsabile Sistemi Informativi; Amministratore di sistema);
6. LED CITY s.r.l. ha chiaramente informato tutti i dipendenti e gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalla Società di consulenza esterna;
7. revisioni periodiche dei contratti di licenza in essere (Società di consulenza esterna).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale

Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

Art. 171-*ter*

1) GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI

ruoli aziendali coinvolti
Amministratore di sistema
Responsabile del sito web
Società di consulenza esterne

attività sensibili

- **a)** Gestione dell'attività di sviluppo di nuovi sistemi informativi
- **b)** Gestione dell'attività di manutenzione dei sistemi esistenti
- **c)** Gestione dell'attività di elaborazione dei dati
- **d)** Gestione della sicurezza informatica sia a livello fisico che a livello logico:
    1. Configurazione delle security policy dei firewall ai fini della tutela delle intrusioni esterne
    2. Gestione e protezione dei back up dei dati
    3. Elaborazione di un Disaster Recovery Plan a tutela del patrimonio informativo

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esiste una procedura per il tracciamento e la documentazione della manutenzione dei sistemi, basati su due ambienti segregati (Società di consulenza esterne);
2. i sistemi sono monitorati e gestiti dai vari team di maintanance, sia a livello applicativo che infrastrutturale, secondo schedulazioni predefinite (Società di consulenza esterna);
3. esistono software per il controllo e le verifiche dello stato dei sistemi informatici (Società di consulenza esterne);
4. la rete privata, realizzata mediante collegamenti via cavo, è costituita da un server localizzato nell'area CED; dieci postazioni lavoro; un dispositivo di backup localizzato nell'area CED ad accessocontrollato; un pc portatile collegabile in rete;
5. oltre alle istruzioni generali, vengono fornite esplicite istruzioni ai dipendenti in merito alle modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici; la prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro; procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggerei sistemi informativi; procedure per il salvataggio dei dati; modalità di custodia ed utilizzo dei supportirimuovibili; il dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal Responsabile Sistemi informativi, sulle misure di sicurezza;
6. il DataCenter è protetto ed allarmato e l'accesso è consentito alle sole persone autorizzate; in particolare, al fine di scongiurare il rischio di perdita o danneggiamento dei dati a seguito di eventuali eventi distruttivi, i locali sono protetti da: dispositivi antincendio previsti dalla normativa vigente; gruppo di continuità dell'alimentazione elettrica; impianto di condizionamento. Sono inoltre adottate le seguenti misure, al fine di impedire accessi non autorizzati: suonerie d'ingresso; attivazione

automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;

7. realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'l'identità delle persone che hanno accesso agli strumenti informatici; le postazioni di lavoro munite di videoterminale sono state dotate di password o parola chiave, che consentono l'accesso ai soli soggetti autorizzati a conoscenza di dette parole chiavi; l'accesso alla rete e ai sistemi aziendali è pertanto soggetto ad autenticazione mediante l'uso di UserID e Password personali; le password sono soggette a scadenza (ogni 6 mesi) e criteri di robustezza (Amministratore di sistema);
8. conferimento della qualifica di custode delle password e vice custode delle password a personale dell'azienda individuato, con l'obbligo di stilare un elenco di parole chiave e di mantenerlo aggiornato; obbligo di comunicazione, per i dipendenti, al custode delle password delle parole chiavee di eventuali variazioni, ulteriori rispetto alle modifiche obbligatorie periodiche (ogni 6 mesi);
9. protezione di strumenti e dati da malfunzionamenti e attacchi informatici. Tutta la rete della LED CITY s.r.l. è gestita a livello globale e protetta da firewall; ogni singolo pc ha installato un firewall (le policy sono gestite a livello corporate per le varie tipologie di firewall e non è possibile cambiarle localmente), che si attiva automaticamente quando il pc non è collegato alla rete aziendale, e un programma antivirus; il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione; aggiornamento trimestrale del sistema di protezione;
10. esiste una procedura di Disaster Recovery a tutela del patrimonio informativo della LED CITY s.r.l.;
11. esiste un dispositivo di backup localizzato nell'area CED ed esiste una procedura standardizzata e documentata per la gestione dei backup dei dati del server; previsione di procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema; il salvataggio dei dati avviene con frequenza giornaliera e le copie vengono custodite in luogo protetto;
12. aggiornamento delle misure di sicurezza; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup;
13. LED CITY s.r.l. ha chiaramente informato gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalle Società di consulenza esterne;
14. tutta la posta aziendale in uscita e in ingresso viene mantenuta e salvata ed è soggetta alle stesse regole di autenticazione degli altri sistemi aziendali;
15. il sistema di posta elettronica è protetto da un sistema ANTISPAM che blocca immediatamente l'ingresso della posta indesiderata;
16. il sistema è dotato di un web filtering perimetrale per evitare l'accesso di virus in azienda tramite web e per limitare l'accesso ad alcuni siti internet da parte degli utenti (black list);
17. gestione del sito online da parte di una Società di consulenza esterna e aggiornamento dei contenuti da parte del Responsabile Servizi informativi;
18. tutte le attività devono prevedere un sistema di autorizzazioni, deleghe e/o separazioni dei compiti, per ciascuna delle attività dei singoli processi;
19. la Società deve porre particolare attenzione affinché, nelle procedure riguardanti il processo di gestione dei sistemi informativi e in tutte le attività ad esso collegate, siano ben definite e controllate le responsabilità delle funzioni preposte allo sviluppo delle singole attività e che tali responsabilità siano coerenti con il quadro dei controlli specifici ai fini del D.Lgs. 231/01;
20. la funzione preposta deve informare l'OdV periodicamente – e comunque con frequenza almeno trimestrale – attraverso uno specifico report, sugli aspetti significativi afferenti le diverse attività di propria competenza, in particolare per quando attiene: le attività di salvaguardia delle attrezzature hardware e dei programmi software; i controlli e le verifiche periodiche sull'efficienza del sistema. La

funzione preposta ha l'obbligo di comunicare immediatamente all'OdV ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata (Amministratore di sistema).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

2) UTILIZZO DI STRUMENTI INFORMATICI AZIENDALI

ruoli aziendali coinvolti
Amministratore Unico/Direzione Generale (DG)
Amministratore di sistema
Responsabile Sistemi Informativi

attività sensibili

- **a)** Abusiva duplicazione, riproduzione, trasmissione, diffusione in pubblico, vendita di prodotti multimediali attraverso il sistema informatico aziendale
- **b)** Abusiva duplicazione, riproduzione, trasmissione, diffusione in pubblico di banche dati attraverso il sistema informatico aziendale

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esistenza di una mappatura dei dispositivi hardware dotati di masterizzatore;
2. LED CITY s.r.l. ha chiaramente informato gli utenti che non è possibile utilizzare ilmasterizzatore per usi diversi da quelli strettamente collegati all'attività aziendale;
3. LED CITY s.r.l. ha chiaramente informato gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalle Società di consulenza esterne.

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

3) IMPIEGO, A QUALSIASI TITOLO, DI PRODOTTI CONTRASSEGNATI SIAE, SENZA IL CONTRASSEGNO O CON IL CONTRASSEGNO CONTRAFFATTO O ALTERATO

ruoli aziendali coinvolti
Impiegati amministrativi
Funzioni aziendali deputate a utilizzare prodotti – anche informatici – contrassegnati SIAE

attività sensibili

a) Detenzione, utilizzo o messa in commercio di supporti o altri strumenti informatici per i quali sia prescritto il contrassegno SIAE.

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esistenza di una mappatura di tutti i supporti o altri strumenti informatici per il quale sia prescritto il contrassegno SIAE (Funzioni aziendali deputate a utilizzare prodotti – anche informatici – contrassegnati SIAE);
2. esistenza di una mappatura di tutti i soggetti che possono avere accesso a supporti o altri sistemi informatici per i quali sia prescritto il contrassegno SIAE (Funzioni aziendali deputate a utilizzare prodotti – anche informatici – contrassegnati SIAE);
3. LED CITY s.r.l. ha chiaramente informato i propri dipendenti e gli utenti che è vietato duplicare, eliminare, contraffare o alterare il contrassegno SIAE in relazione ai prodotti per i qualitale contrassegno sia prescritto (Impiegati amministrativi; Funzioni aziendali deputate a utilizzare prodotti – anche informatici – contrassegnati SIAE);
4. LED CITY s.r.l. ha chiaramente informato i propri dipendenti e gli utenti che è vietato detenere, porre in commercio o cedere a qualsiasi titolo supporti privi del contrassegno SIAEladdove questo contrassegno sia previsto per legge (impiegati amministrativi; Funzioni aziendali deputate a utilizzare prodotti – anche informatici – contrassegnati SIAE).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio

Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

4) IMPIEGO ILLECITO DI SERVIZI CRIPTATI ATTRAVERSO SISTEMI DI CODIFICAZIONE

ruoli aziendali coinvolti
Ogni operatore che ha accesso ad apparati idonei alla ricezione di servizi criptati
Impiegati amministrativi

attività sensibili

a) Impiego di sistemi informatici e audiovisivi criptati.

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esistenza di una mappatura di tutti i sistemi informatici e audiovisivi criptati di decodificazione speciale (Ogni operatore che ha accesso ad apparati idonei alla ricezione di servizi criptati);
2. esistenza di una mappatura di tutti i soggetti che possono avere accesso ai sistemi informatici e audiovisivi criptati (Ogni operatore che ha accesso ad apparati idonei alla ricezione di servizicriptati);
3. LED CITY s.r.l. ha chiaramente informato i propri dipendenti e gli utenti che è vietato detenere elementi di decodificazione speciale senza il pagamento del canone dovuto, nonchétrasmettere o diffondere servizi criptati ad accesso condizionato (impiegati amministrativi).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

5) IMPIEGO DI STRUMENTI ATTI AD ELUDERE LE MISURE TECNOLOGICHE DI PROTEZIONE E MESSA A DISPOSIZIONE DELLE OPERE PRIVE DELLA PROTEZIONE STESSA

ruoli aziendali coinvolti
Ogni operatore che ha accesso ad una postazione informatica
Impiegati amministrativi

attività sensibili
a) Impiego di hardware e software

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. LED CITY s.r.l. ha chiaramente informato i dipendenti e gli utenti che è vietato impiegare strumenti atti ad eludere le misure tecnologiche di protezione relative ad opere e materiale protetti;
2. LED CITY s.r.l. ha chiaramente informato i dipendenti e gli utenti che sono vietate la diffusione e la distribuzione di opere o altri materiali protetti rispetto ai quali siano state rimosse le protezioni.

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

Art. 171-*septies*

Tale disposizione non è applicabile a LED CITY s.r.l. in quanto la società non risulta néproduttrice o importatrice di supporti soggetti all'apposizione del contrassegno SIAE.

Art. 171-*octies*

1) IMPIEGO ILLECITO DI APPARATI ATTI ALLA DECODIFICAZIONE DI TRASMISSIONI AUDIOVISIVE AD ACCESSO CONDIZIONATO

ruoli aziendali coinvolti
Ogni operatore che ha accesso ad apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato
Impiegati amministrativi

attività sensibili
a) Impiego di strumenti idonei alla decodificazione di trasmissioni audiovisive ad accesso condizionato

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area di rischio sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltrea definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esistenza di una mappatura di tutti gli apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato;
2. esistenza di una mappatura di tutti i soggetti che possono avere accesso agli apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato;
3. LED CITY s.r.l. ha chiaramente informato i dipendenti e gli utenti che è vietato utilizzare, per fini differenti rispetto a quelli propri leciti, gli apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi

Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

3 I “ processi strumentali” in relazione ai reati in materia di violazione del diritto di autore (art. 25-*novies*, D. Lgs. 231/01)

Seguendo la stessa metodologia utilizzata per l’individuazione delle attività “a rischio reato”, sono state individuate, nell’ambito della struttura organizzativa ed aziendale di LED CITY s.r.l., i processi considerati strettamente “strumentali”, ovvero quei processi c.d. “di supporto” alle attività che insistono sulle aree “ a rischio reato”.

Nell’ambito di ciascuna attività “strumentale”, sono stati, inoltre, individuati i Ruoli Aziendali coinvolti e le relative attività c.d. “sensibili”. Sono stati, infine, individuati i principali protocolli preventivi che insistono su ciascuna area “strumentale”.

Con riferimento agli illeciti sopra elencati, i “processi strumentali” collegati alle “ m acro aree” sens ib i l i ritenute più specificamente a rischio risultano essere le seguenti:

1. Gestione degli acquisti di beni e servizi
2. Budget e controllo di gestione
3. Selezione, assunzione e formazione del personale
4. Gestione dei contratti
5. Gestione dei sistemi informativi aziendali
6. Gestione degli omaggi, regalie, erogazioni liberali e sponsorizzazioni

1) GESTIONE DEGLI ACQUISTI DI BENI E SERVIZI

ruoli aziendali coinvolti
Direzione Generale (DG)
Commerciale (COM)
Ufficio Acquisti (ACQ)
Responsabile Amministrazione (AMM)
Responsabile Strumenti di Misura (RSM)
Responsabile Cantiere (CANT)
Capo Cantiere (CCA)
Responsabile della Gestione per la Qualità (RGQ)
Ufficio Operativo Gare (OPG)

attività sensibili

- **a)** Selezione e valutazione dei fornitori nuovi/storici
- **b)** Scelta della controparte, definizione delle clausole contrattuali, stipula dei contratti
- **c)** Verifica delle prestazioni/beni acquistati
- **d)** Emissione degli ordini di acquisto
- **e)** Gestione delle importazioni/esportazioni

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali coinvolti nell'area strumentale di acquisto di beni e servizi sono tenuti, al fine di prevenire e impedire il verificarsi dei reati in esame, al rispettodelle procedure aziendali emesse a regolamentazione di tale area a rischio. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio:

1. gestione centralizzata degli acquisti relativi alla produzione, agli impianti e ai cantieri (DG; ACQ);
2. definizione di criteri, modalità operative, responsabilità e modulistica al fine di garantire la qualità degli approvvigionamenti di prodotti/servizi considerati primari, ovverosia tutti i prodotti e gli strumenti utilizzati dalla LED CITY s.r.l. Costruzioni nelle attività di costruzione e tutti i prodotti/servizi (manodopera, tarature, etc.) che hanno un'influenza diretta sulla qualità delle opere fornite (DG; ACQ);
3. verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari (ACQ);
4. definizione dei criteri di scelta dei fornitori fondati su requisiti di carattere qualitativo e quantitativo (DG; ACQ);
5. tutti i fornitori di servizi/prodotti primari, che hanno influenza sulla qualità della fornitura finale devono essere qualificati (ACQ); nell'"Elenco Fornitori Qualificati" vengono riportati tutti i fornitori qualificati (Q) e non qualificati (NQ) presente nell'anagrafica fornitori della contabilità fiscale (ACQ; AMM); durata annuale delle qualifiche riconosciute e riesame delle qualifiche attribuite alla scadenza delle stesse o per altre cause straordinarie (es. richiesta da parte di una funzione aziendale, non conformità gravi, etc.) (ACQ);
6. vengono qualificati come storici i fornitori che storicamente, ovvero per 2 anni, hanno fornito prodotti/servizi di qualità alla LED CITY s.r.l.;

7. vengono considerati qualificati direttamente dalla LED CITY s.r.l. i fornitori che hanno superato con esito positivo la valutazione fatta dal Responsabile Ufficio Acquisti, secondo i criteri previsti e stabiliti all'interno di apposita procedura aziendale, utilizzabili singolarmente o congiuntamente, a seconda dei beni/servizi oggetto di fornitura (es. inerti, materie prime, magazzini edili, subappaltatori, macchine e strumenti, etc.) (ACQ);
8. vengono considerati qualificati altresì i fornitori richiesti esplicitamente dal committente, e con riferimento al solo cliente che lo ha esplicitamente richiesto o al solo cantiere, previadocumentazione giustificativa da parte del committente stesso (ACQ; DG);
9. compilazione di un modello relativo al fornitore qualificato, con indicazione dei requisiti necessari per la determinata tipologia di fornitore (ACQ);
10. richiesta al fornitore di una dichiarazione relativa ad eventuali rapporti in grado di generare conflitti di interesse con esponenti della P.A. (ACQ);
11. necessario ricorso ai fornitori qualificati, inseriti nelle liste aziendali definite per ciascuna tipologia di acquisto (ACQ);
12. approvvigionamento di prodotti/servizi primari, quindi influenti sulla qualità del prodotto offerto dalla LED CITY s.r.l., esclusivamente da fornitori qualificati - e indicati in apposito "Elenco Fornitori Qualificati" (Mod. 74.01) - fatto salvo il caso in cui sia lo stesso committente a specificare nell'ordine il fornitore che deve essere utilizzato (ACQ);
13. avvio del procedimento di valutazione dei fornitori per scegliere il fornitore di un nuovo articolo non approvvigionato prima, per individuare fornitori alternativi a quelli già esistenti, più competitivi per capacità qualitative, tecnologiche e/o economiche, e per convalidare lo stato di qualifica dei fornitori esistenti (ACQ);
14. per la selezione del fornitore di un articolo e/o per la valutazione di nuovi fornitori, vengono definite le caratteristiche del prodotto/servizio da approvvigionare, vengono individuati i probabili fornitori, viene effettuata relativa valutazione commerciale (ACQ);
15. per la selezione del fornitore più idoneo, tra fornitori ritenuti qualificati, il Responsabile UfficioAcquisti valuta eventuali differenze di prezzo e scostamenti rispetto ai requisiti (ACQ);
16. monitoraggio periodico delle prestazioni e dei requisiti dei fornitori ai fini dell'aggiornamento delle liste aziendali (CANT; CCA);
17. per ogni fornitore qualificato, registrazione sulla "Scheda valutazione fornitore" - a cura del Responsabile per la Gestione Qualità - di tutte le non conformità attribuibili al fornitore stesso (RGQ);
18. avvio - annuale - del procedimento di convalida della valutazione dei fornitori già qualificati e riporto dell'esito sulle schede di valutazione dei fornitori (ACQ); avvio del procedimento di convalida della valutazione dei fornitori già qualificati, anche a fronte di fattori oggettivi, come non conformitàripetitive e rilevanti, o su richiesta di una funzione aziendale (ACQ);
19. emissione di ordini esclusivamente nei confronti di fornitori presenti nell'Elenco Fornitori Qualificati;
20. richiesta di preventivi per la selezione del fornitore per acquisti superiori a determinati importi (ACQ);
21. evidenza documentale del processo di selezione del fornitore per acquisti superiori a determinati importi (ACQ);
22. definizione degli ordini sulla base delle esigenze scaturite - di norma - dall'analisi delle commesse, dal controllo delle giacenze di magazzino e dalle necessità relative ai cantieri; all'apertura di un cantiere è responsabilità del Responsabile Ufficio Acquisti procede progressivamente all'ordine di materiali/prodotti/servizi necessari (ACQ; CANT; CCA);
23. registrazione degli acquisti (ACQ); gli ordini possono essere concordati dal Responsabile Ufficio Acquisti anche telefonicamente, ma devono sempre essere registrati su un ordine scritto e firmato da Responsabile Ufficio Acquisti e Direzione Generale per avvenuto esame (ACQ; DG);

24. approvazione degli ordini d'acquisto di servizi e beni in base a definiti livelli autorizzativi; approvazione degli ordini di beni diretti di produzione in base a definiti livelli autorizzativi (ACQ; DG);
25. formalizzazione dei rapporti con i fornitori tramite la stipula di accordi quadro/contratti/lettere di incarico in cui è inserita la clausola di rispetto del Codice Etico adottato dalla LED CITY s.r.l., al fine di sanzionare eventuali comportamenti/condotte contrari ai principi etici (ACQ; DG);
26. per gli acquisti effettuati direttamente da banco presso i fornitori - esclusivamente dal Capo Cantiere e per importi inferiori a 500,00 euro - la firma del documento di accompagnamento contestuale al ricevimento della merce è sostitutiva del riesame (CCA); per gli acquisti superiori a 500,00 euro procede sempre l'Ufficio Acquisti (ACQ);
27. i materiali di modico valore (es. cancelleria) vengono acquistati, tramite cassa, da fornitori con regolare fattura (ACQ);
28. all'avvallo degli acquisti procede la Direzione Generale;
29. aggiornamento dell'elenco dei listini dei fornitori in uso (AMM);
30. le modifiche d'ordine vengono emesse in seguito a variazioni nei dati di acquisto, intervenute dopo l'emissione dell'ordine corrispondente, e seguono l'iter procedurale previsto per la prima emissione;
31. verifica dei termini di consegna dei materiali/servizi da parte del Responsabile Ufficio Acquisti e sollecito delle forniture in ritardo in tempo utile per rispettare il programma di consegna delle opere ai clienti (ACQ);
32. la verifica dei prodotti approvvigionati è responsabilità del Capo cantiere, del Responsabile Cantiere e del Responsabile Amministrazione (CCA; CANT; AMM);
33. per gli acquisti da banco e per gli acquisti con consegna presso i cantieri, sono previsti i seguenti controlli eseguiti da funzioni segregate:
    - controllo tra DDT e materiale da parte del Capo Cantiere (o un suo incaricato), che verifica la rispondenza di quanto indicato sul DDT e quanto caricato nel magazzino del fornitore, oppure tra quanto scaricato in cantiere da parte del fornitore e quanto indicato sul DDT, vista tutte le voci conformi sulla copia del DDT che rimane alla LED CITY s.r.l. S.r.l., con firma e data (CCA) e presenta eventuali non conformità al Responsabile della Gestione per la Qualità (RGQ);
    - controllo tra DDT e fattura, quando la fattura arriva in Ufficio da parte del Responsabile Amministrazione, che vista tutte le voci corrispondenti sulla fattura, appone la data e firma (AMM);
    - controllo tra DDT e ordine, quando il personale riporta il DDT dal cantiere in ufficio, al termine della giornata lavorativa, da parte del Responsabile Amministrazione, che vista tutte le voci corrispondenti sull'ordine, appone la data e firma (AMM);
34. per gli acquisti con consegna presso i cantieri magazzini, i controlli tra DDT e materiale, tra DDT e fattura e tra DDT e ordine vengono effettuati dal Responsabile Amministrazione (AMM);
35. controlli formali e sostanziali sui documenti relativi a tutti i materiali d'importazione (ACQ);
36. predisposizione di controlli di riconciliazione contabile tra le somme pagate a fronte della merce ricevuta e riconciliazione di magazzino tra la merce effettivamente ordinata e la merce acquistata in magazzino (CCA; AMM; ACQ; RGQ);
37. controlli periodici mensili sulle fatture da parte del Responsabile di Gestione della Qualità, diconcerto con la Direzione Generale (RGQ; DG);
38. verificare che fornitori e partner non abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal Gruppo di Azione Finanziaria contro il riciclaggio di denaro (GAFI) (ACQ); qualora fornitori o partner siano collegati in qualche modo a uno di tali Paesi, sarà necessario che le decisioni relative ottengano l'espressa autorizzazione del Direttore Generale.

protocolli preventivi di sistema

Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno, autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
Approvvigionamento (POI 74.01)
Elenco Fornitori Qualificati (Mod. 74.01)
Scheda valutazione fornitore (Mod. 74.02)

2) BUDGET E CONTROLLO DI GESTIONE

ruoli aziendali coinvolti
Direzione Generale (DG)
Responsabile Amministrazione
Amministrazione (AMM)
Commerciale (COM)

attività sensibili

- **a)** Raccolta e consolidamento dei dati provenienti dalle varie aree aziendali
- ***b)*** Analisi del piano strategico aziendale e conseguente elaborazione del *budget:*
  1. Elaborazione dei report consuntivi
  2. Determinazione degli scostamenti preventivo/consuntivo ed analisi delle cause
- ***c)*** Monitoraggio sui risultati delle singole aree di *budget*
- **d)** Riformulazione degli obiettivi sulla base dei dati consuntivati
- ***e)*** Gestione delle spese extra-*budget*

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. concorrenza di più soggetti responsabili delle singole funzioni alla definizione delle risorse disponibili e degli ambiti di spesa, con l'obiettivo di garantire la costante presenza di controlli e verifiche incrociati su un medesimo processo/attività, volta tra l'altro a garantire una adeguata segregazione delle funzioni (DG; Responsabile Amministrazione; AMM; COM);
2. adozione di modalità corrette ed omogenee per la valorizzazione economica delle iniziative, così da assicurare la possibilità di confrontare i valori economici delle differenti funzioni aziendali (DG; AMM);
3. verifica trimestrale degli scostamenti tra i risultati effettivi e quelli fissati nel *budget* (AMM; Responsabile Amministrazione);
4. analisi delle cause degli scostamenti e necessità di autorizzazione delle differenze da parte dell'adeguato livello gerarchico (DG; AMM; Responsabile Amministrazione).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi

Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno, autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
Procedura per la formazione del budget
Procedura per il controllo di gestione

3) SELEZIONE, ASSUNZIONE E FORMAZIONE DEL PERSONALE

ruoli aziendali coinvolti
Datore di lavoro/Direzione Generale (DG)
Responsabile Amministrazione (AMM)
RSPP
Responsabile della Gestione per la Qualità (RGQ)
Responsabili delle Funzioni Aziendali
Capo Cantiere (CCA)

attività sensibili

- **a)** Individuazione delle posizioni da ricoprire mediante nuove assunzioni
- **b)** Definizione formale dei profili di potenziali candidati per le diverse posizioni da ricoprire
- **c)** Raccolta ed archiviazione della documentazione relativa alle candidature pervenute
- **d)** Analisi e valutazione delle candidature e verifica della loro "idoneità" rispetto ai profili definiti
- **e)** Selezione del personale e formalizzazione dell'esito del processo
- **f)** Formulazione dell'offerta retributiva
- **g)** Formazione del personale di nuova assunzione

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. formalizzazione dei requisiti richiesti (ad es. caratteristiche tecniche ed esperienza acquisita) per la posizione da ricoprire e delle valutazioni dei diversi candidati nelle diverse fasi del processo di selezione; il datore di lavoro decide l'assunzione di nuove risorse umane sulla base di valutazioni oggettive in merito alle competenze possedute, ed a quelle potenzialmente esprimibili, in relazione alla funzione da ricoprire all'interno della Società (Datore di lavoro/Direzione Generale; Amministrazione);
2. per ogni funzione rilevante all'interno della LED CITY s.r.l. sono definiti dei requisiti minimi di competenze e formazione, esplicitate nel modulo 62.04;
3. reclutamento del personale tramite agenzie interinali, *curriculum vitae* inviati via e-mail, identificazione attraverso chiamata specifica, su segnalazione di agenzie di ricerca/selezione, di profili elevati provenienti da altre società (Amministrazione);
4. archiviazione della documentazione relativa al processo di selezione, al fine di garantire la tracciabilità dello stesso (Responsabile Amministrazione); gestione delle "Schede personale" su cui vengono registrati dati anagrafici, titoli di studio ed eventuali specializzazioni, esperienze precedenti all'assunzione, incarichi/mansioni ricoperte in azienda, corsi di formazione effettuati e corsi di formazione ritenuti necessari (Responsabile Amministrazione; RGQ); procedura di archiviazione di tutta la documentazione inerente il personale all'interno del raccoglitore contenente i dati del personale (POI 42.01 Gestione dei documenti);
5. richiesta al candidato di una dichiarazione relativa a eventuali rapporti di parentela in grado di generare conflitti di interesse con esponenti della PA;

6. all'assunzione, vengono consegnati i seguenti documenti: lettera del contratto di assunzione, tesserino di riconoscimento, ricevuta DPI, documenti per le detrazioni Irpef, informativa sulla privacy, documentazione per la scelta del TFR, comunicazione del divieto di assunzione di bevande alcoliche;
7. formulazione dell'offerta economica in base a Linee Guida aziendali relative alla retribuzione e necessaria autorizzazione per offerte economiche superiori al limite definito per la posizione; le retribuzioni eccedenti quelle fissate dal CCNL di riferimento sono convenute sulla base delle responsabilità e dei compiti della mansione attribuita al dipendente e comunque in riferimento ai valori medi di mercato (Datore di lavoro/Direzione Generale);
8. individuazione di un piano per la consegna del DPI, di concerto con il RSPP, e relativa documentazione, cui segue la formazione in materia di sicurezza generale, di cui rimane evidenza cartacea (Amministrazione; RSPP; RGQ); in particolare, è prevista l'istruzione del personale sulle prescrizioni relative a salute e sicurezza sul lavoro e quelle derivanti dal rispetto della normativa ambientale, sia in sede che nei cantieri temporanei e mobili (RSPP; Capo Cantiere);
9. individuazione, programmazione e attuazione di attività di formazione e addestramento del personale di nuova assunzione, al fine di fornire elementi necessari e utili a svolgere le attività di competenza e istruzioni sulle procedure che regolano le mansioni affidate; l'addestramento è effettuato sia tramite corsi di formazione strutturati, sia attraverso periodi di affiancamento a dipendenti esperti, trasferendo non solamente le competenze tecniche, specifiche del ruolo, ma anche i principi etici che regolano lo svolgimento delle attività (Codice Etico dell'impresa) (DG; Responsabili delle Funzioni Aziendali; RGQ);
10. predisposizione del protocollo sanitario stipulato, da parte del medico competente contattato, a seconda della tipologia di contratto, dalla LED CITY s.r.l. direttamente o dall'agenzia interinale;
11. previsione di controlli "drugtest" – iniziale (preassuntiva) e annuale – per gli autisti, gli addetti a macchine operatrice (escavatoristi) e lavoratori in quota, con rilascio di attinente documentazione;
12. nel caso in cui occorra assumere un cittadino extracomunitario, la Società è tenuta a verificare: a) la regolarità dell'ingresso tramite i flussi di immigrazione con controllo dell'attribuzione di codice fiscale, mediante lo sportello unico di immigrazione (S.U.I.); b) la residenza anagrafica effettiva dichiarata e l'agibilità della stessa; c) l'apertura di un conto corrente bancario regolare sul quale effettuare obbligatoriamente il pagamento del salario; test di conoscenza dell'italiano, archiviati (Amministrazione);
13. nel caso in cui un dipendente di altra società presti servizio, a qualsiasi titolo, a favore di LED CITY s.r.l. quest'ultima deve ottenere dalla società terza una attestazione relativa al fatto che il dipendente stesso possegga i requisiti di cui ai punti precedenti (attestazioni e idoneità sanitaria).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione

Direttiva aziendale antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno, autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
POI 62.01 Risorse Umane
Manuale di Gestione Qualità
POI 42.01 Gestione dei documenti

4) GESTIONE DEI CONTRATTI

ruoli aziendali coinvolti
Direzione Generale (DG)
Amministrazione (AMM)
Responsabile Commerciale (COM)
Ufficio Operativo Gare (OPG)
Responsabile Cantieri (CANT)
Responsabile della Gestione per la Qualità (RGQ)
Consulente esterno

attività sensibili

- **a)** Revisione dei contratti prima della stipula
- **b)** Formulazione di integrazioni/modifiche da apportare al contratto prima della stipula
- **c)** Approvazione dell'ultima versione del contratto

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. gestione dei contratti anche attraverso il sistema informatico;
2. revisione dei contratti da stipulare, all'interno del suddetto sistema, da parte di diversi soggetti aziendali per approvazioni di diversa natura (tecnico-economica, legale, fiscale) (DG; AMM; COM; CANT);
3. condivisione con la controparte dei commenti e delle proposte di modifiche da apportare alla bozza del contratto sottoposto ad approvazione;
4. approvazione dei contratti da parte della Direzione Generale (DG);
5. richiesta di consulenze civilistiche, nell'eventualità in cui si verifichino problematiche su determinate cause nel privato (Consulente esterno);
6. in particolare, l'Ufficio addetto alla preparazione delle gare (OPG), nella fase successiva all'aggiudicazione definitiva di una gara, prepara la documentazione (Mod. 72.04) in cui specifica le caratteristiche generali del contratto; tra i primi documenti da preparare per l'invio all'ente, vi sono il certificato della camera di commercio con dichiarazione antimafia, fideiussione definitiva, versamento delle spese contrattuali, piano operativo sicurezza (POS);
7. sulla base della documentazione inviata, viene preparato dall'ente appaltante il contratto che viene poi riesaminato e firmato per approvazione dal Responsabile Commerciale (COM);
8. in caso di divergenze, il Responsabile Commerciale può accettare di firmare il contratto o gli atti allegati ad esso con riserva (COM);
9. prima dell'inizio delle attività operative in cantiere, l'Ufficio Operativo Gare (OPG) invia agli enti preposti le comunicazioni di inizio lavori;
10. l'archiviazione dei documenti e della modulistica è a cura del Responsabile della Gestione per la Qualità (RGQ).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno, autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
Procedura per la scelta dei consulenti
Gestione dei contratti commerciali
Gestione dei documenti (POI 42.01)
Processi relativi al cliente (POI 72.01)

5) GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI

ruoli aziendali coinvolti
Amministratore di sistema
Responsabile del sito web
Società di consulenza esterne

attività sensibili

- **a)** Gestione dell'attività di sviluppo di nuovi sistemi informativi
- **b)** Gestione dell'attività di manutenzione dei sistemi esistenti
- **c)** Gestione dell'attività di elaborazione dei dati
- **d)** Gestione della sicurezza informatica sia a livello fisico che a livello logico:
    1. Configurazione delle security policy dei firewall ai fini della tutela delle intrusioni esterne;
    2. Gestione e protezione dei back up dei dati
    3. Elaborazione di un Disaster Recovery Plan a tutela del patrimonio informativo

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esiste una procedura per il tracciamento e la documentazione della manutenzione dei sistemi, basati su due ambienti segregati (Società di consulenza esterne);
2. i sistemi sono monitorati e gestiti dai vari team di maintanance, sia a livello applicativo che infrastrutturale, secondo schedulazioni predefinite (Società di consulenza esterna);
3. esistono software per il controllo e le verifiche dello stato dei sistemi informatici (Società di consulenza esterne);
4. la rete privata, realizzata mediante collegamenti via cavo, è costituita da un server localizzato nell'area CED; dieci postazioni lavoro; un dispositivo di backup localizzato nell'area CED ad accessocontrollato; un pc portatile collegabile in rete;
5. oltre alle istruzioni generali, vengono fornite esplicite istruzioni ai dipendenti in merito alle modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici; la prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro; procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggerei sistemi informativi; procedure per il salvataggio dei dati; modalità di custodia ed utilizzo dei supportirimuovibili; il dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal Responsabile Sistemi informativi, sulle misure di sicurezza;
6. il DataCenter è protetto ed allarmato e l'accesso è consentito alle sole persone autorizzate; in particolare, al fine di scongiurare il rischio di perdita o danneggiamento dei dati a seguito di eventuali eventi distruttivi, i locali sono protetti da: dispositivi antincendio previsti dalla normativa vigente; gruppo di continuità dell'alimentazione elettrica; impianto di condizionamento. Sono inoltre adottate le seguenti misure, al fine di impedire accessi non autorizzati: suonerie d'ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;

7. realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'l'identità delle persone che hanno accesso agli strumenti informatici; le postazioni di lavoro munite di videoterminale sono state dotate di password o parola chiave, che consentono l'accesso ai soli soggetti autorizzati a conoscenza di dette parole chiavi; l'accesso alla rete e ai sistemi aziendali è pertanto soggetto ad autenticazione mediante l'uso di UserID e Password personali; le password sono soggette a scadenza (ogni 6 mesi) e criteri di robustezza (Amministratore di sistema);
8. conferimento della qualifica di custode delle password e vice custode delle password a personale dell'azienda individuato, con l'obbligo di stilare un elenco di parole chiave e di mantenerlo aggiornato; obbligo di comunicazione, per i dipendenti, al custode delle password delle parole chiavee di eventuali variazioni, ulteriori rispetto alle modifiche obbligatorie periodiche (ogni 6 mesi);
9. protezione di strumenti e dati da malfunzionamenti e attacchi informatici. Tutta la rete della LED CITY s.r.l. è gestita a livello globale e protetta da firewall; ogni singolo pc ha installato un firewall (le policy sono gestite a livello corporate per le varie tipologie di firewall e non è possibile cambiarle localmente), che si attiva automaticamente quando il pc non è collegato alla rete aziendale, e un programma antivirus; il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione; aggiornamento trimestrale del sistema di protezione;
10. esiste una procedura di Disaster Recovery a tutela del patrimonio informativo della LED CITY s.r.l.;
11. esiste un dispositivo di backup localizzato nell'area CED ed esiste una procedura standardizzata e documentata per la gestione dei backup dei dati del server; previsione di procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema; il salvataggio dei dati avviene con frequenza giornaliera e le copie vengono custodite in luogo protetto;
12. aggiornamento delle misure di sicurezza; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup;
13. LED CITY s.r.l. ha chiaramente informato gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalle Società di consulenza esterne;
14. tutta la posta aziendale in uscita e in ingresso viene mantenuta e salvata ed è soggetta alle stesse regole di autenticazione degli altri sistemi aziendali;
15. il sistema di posta elettronica è protetto da un sistema ANTISPAM che blocca immediatamente l'ingresso della posta indesiderata;
16. il sistema è dotato di un web filtering perimetrale per evitare l'accesso di virus in azienda tramite web e per limitare l'accesso ad alcuni siti internet da parte degli utenti (black list);
17. gestione del sito online da parte di una Società di consulenza esterna e aggiornamento dei contenuti da parte del Responsabile Servizi informativi;
18. tutte le attività devono prevedere un sistema di autorizzazioni, deleghe e/o separazioni dei compiti, per ciascuna delle attività dei singoli processi;
19. la Società deve porre particolare attenzione affinché, nelle procedure riguardanti il processo di gestione dei sistemi informativi e in tutte le attività ad esso collegate, siano ben definite e controllate le responsabilità delle funzioni preposte allo sviluppo delle singole attività e che tali responsabilità siano coerenti con il quadro dei controlli specifici ai fini del D.Lgs. 231/01;
20. la funzione preposta deve informare l'OdV periodicamente – e comunque con frequenza almeno trimestrale – attraverso uno specifico report, sugli aspetti significativi afferenti le diverse attività di propria competenza, in particolare per quando attiene: le attività di salvaguardia delle attrezzature hardware e dei programmi software; i controlli e le verifiche periodiche sull'efficienza del sistema. La funzione preposta ha l'obbligo di comunicare immediatamente all'OdV ogni deroga alle procedure di

processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata (Amministratore di sistema).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Iscrizione nella *white list* istituita presso la Prefettura
Clausola l. 122/2012 nei contratti di appalto e di fornitura

protocolli preventivi specifici
DPS

6) GESTIONE DEGLI OMAGGI, REGALIE, EROGAZIONI LIBERALI E SPONSORIZZAZIONI

ruoli aziendali coinvolti
Direzione Generale
Amministrazione
Responsabile Amministrazione
Responsabile Commerciale (COM)

attività sensibili
- **a)** Gestione omaggi e regalie
- **b)** Erogazioni liberali
- **c)** Sponsorizzazioni

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. nello svolgimento delle attività di comunicazione e promozione deve essere sempre salvaguardato il principio di separazione delle responsabilità per le fasi di: richiesta/proposta; autorizzazione; monitoraggio e controllo (Amministrazione; COM; DG);
2. nello svolgimento delle attività di comunicazione e promozione deve sempre essere inserito un tetto massimo di spesa; ove si decida di andare oltre il tetto massimo, occorre l'autorizzazione di una funzione diversa da quella che ha deciso di andare oltre (AMM; COM; DG);
3. necessità di stabilire – in caso di sponsorizzazioni continuative nei confronti di enti pubblici o società private – una soluzione basata sul criterio dell'alternanza temporale ovvero sull'obbligo di prevedere periodi di astensione dall'adottare sponsorizzazioni.

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno, autorizzato a trattare con la PA

Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
Gestione degli omaggi, regalie, erogazioni liberali e sponsorizzazioni

4 I compiti dell'Organismo di Vigilanza

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'OdV nel documento approvato dall'Amministratore Unico e denominato "Parte speciale C – Struttura, composizione, regolamento e funzionamento dell'Organismo di Vigilanza", in relazione alla prevenzione dei reati di cui alla presente Parte speciale, l'OdV, tra l'altro, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati in materia di violazione dei diritti d'autore;
- verificare, in particolare, il rispetto delle regole procedurali e del Modello in ordine ai flussi finanziari aziendali, con riferimento ai pagamenti da/verso i terzi;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi di flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi *sub* responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività;
- verificare la correttezza della valutazione della congruità economica degli investimenti effettuati dai soggetti aziendali competenti o dai consulenti all'uopo nominati;
- verificare l'applicazione dei punti di controllo previsti nelle procedure riferibili alla prevenzione dei reati contro la P.A. (parte speciale "E") e ai reati societari (parte speciale "F"), qualora inerenti le medesime attività "sensibili" o "strumentali" rilevanti ai fini della prevenzione dei reati informatici e di trattamento illecito di dati.