MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO *EX* D.LGS. 231/2001

PARTE SPECIALE B

REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI E DELITTI IN MATERIA DI DIRITTO D'AUTORE

Approvato in data 19 luglio 2018

INDICE

PARTE 1: FATTISPECIE DI REATO PREVISTE DAL D.LGS. N. 231/2001

1 FATTISPECIE DI REATO PREVISTE DALL'ARTICOLO 24 BIS

L'articolo 24 bis del D.Lgs. n. 231 del 2001, introdotto dalla Legge 18 marzo 2008, n. 48, ha ampliato le fattispecie di reato da cui può sorgere la responsabilità dell'ente relativamente alla criminalità informatica (di seguito i "Reati Informatici e Trattamento Illecito di Dati"). Nello specifico, le fattispecie rilevanti ai fini della presente Parte Speciale sono le seguenti:

- Documenti informatici (art. 491 bis c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.).

2 FATTISPECIE DI REATO PREVISTE DALL'ARTICOLO 25 NOVIES

L'articolo 25 novies del D.Lgs. n. 231 del 2001, introdotto dalla Legge 23 luglio 2009, n. 99, richiama le fattispecie di reato che violino il diritto d'autore (di seguito, "Delitti in materia di Violazione del Diritto d'Autore"). Nello specifico, le fattispecie rilevanti ai fini della presente Parte Speciale sono i delitti previsti dagli articoli 171, primo comma, lettera a bis), e terzo comma, 171-bis, 171 ter, 171 septies e 171 octies e 174 quinquies della legge 22 aprile 1941, n. 633, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio. (di seguito, anche "LdA").

PARTE 2: LE AREE A RISCHIO REATO E I RELATIVI PRINCIPI DI COMPORTAMENTO E DI CONTROLLO SPECIFICI

1 LE AREE A RISCHIO REATO

Con riferimento ai Reati di cui alla presente Parte Speciale, ad esito delle attività di *risk assessment* svolte, è stata individuata la seguente area a "rischio reato":

Area a "rischio"	Fattispecie di reato rilevanti		Principali Organi / Unità Organizzative coinvolti	
	Art. 24 bis	Art.25 novies	DICT / DTA	Tutte le UO coinvolte
Gestione ICT	✔	✔	✔	✔

I reati informatici e quelli relativi alle fattispecie previste in tema di diritti d'autore possono essere commessi, potenzialmente, da tutti i dipendenti/componenti degli Organi Sociali che, a vario titolo, possono utilizzare strumenti informatici.

2 PRINCIPI GENERALI DI COMPORTAMENTO

Al fine di prevenire ed impedire il verificarsi dei reati di cui alla presente Parte Speciale, individuati alla precedente Parte 1 e ritenuti rilevanti per Anas, i Destinatari del Modello, fermo restando quanto indicato nel successivo paragrafo 3 e dalle disposizioni normative interne, sono tenuti al rispetto dei seguenti principi generali di comportamento:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato indicate nella precedente Parte 1;
- astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati indicati nella precedente Parte 1, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi.

Inoltre, in relazione ai Reati Informatici e Trattamento Illecito di Dati, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

- accedere abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;
- introdursi in un sistema informatico o telematico, o in parti di esso, ovvero in banche dati di Anas, o in parti di esse, non possedendo le credenziali di accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;
- distruggere, deteriorare, cancellare, manipolare, eliminare informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di

pubblica utilità;
- inserire o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inutilizzabili, impedire il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- alterare, mediante l'utilizzo di firma elettronica o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o manipolati;
- intercettare fraudolentemente e/o diffondere comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti tecnologici (es. *software*) non autorizzati idonei ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- detenere, procurarsi, riprodurre e o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento.

In particolare, le funzioni aziendali che svolgono servizi di *Information Technology* ovvero *Information Management* devono ispirare la loro azione ai seguenti principi generali:
- Riservatezza - garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- Integrità - garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- Disponibilità - garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Inoltre, in relazione ai Delitti in materia di Violazione del Diritto d'Autore, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:
- accedere abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;
- divulgare, senza autorizzazione, mediante immissione in un sistema di reti telematiche con connessioni di qualsiasi genere, opere dell'ingegno - o parti di esse - protette dal diritto d'autore;
- duplicare, riprodurre, trasmettere e diffondere in pubblico in maniera abusiva, senza cioè avere ottenuto l'opportuno consenso o cessione del diritto da parte del titolare dell'opera o del titolare dei diritti di sfruttamento economico, di opere dell'ingegno;

- caricare, senza autorizzazione, software sugli strumenti informatici forniti dalla Società;
- duplicare, senza autorizzazione, programmi per elaboratore;
- riprodurre, trasferire su altro supporto, diffondere, comunicare, presentare o dimostrare in pubblico il contenuto di una banca dati senza aver in via preventiva ottenuto la necessaria autorizzazione dal legittimo titolare del diritto d'autore e/o del diritto di sfruttamento economico della banca dati medesima.

Con riferimento all'acquisto o all'utilizzo da parte della Società di qualsivoglia bene suscettibile di tutela, è fatto altresì obbligo ai Destinatari di ottenere dai rispettivi titolari e/o licenzianti dei relativi diritti di utilizzo sui beni in questione, specifiche dichiarazioni volte ad attestare di :

- essere i legittimi titolari dei diritti di sfruttamento economico sui beni oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
- garantire che i beni oggetto di cessione o di concessione in uso non violano alcun diritto di proprietà intellettuale in capo a terzi;
- impegnarsi a tenere indenne Anas da qualsivoglia danno o pregiudizio di natura patrimoniale e non, le potesse derivare per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

In aggiunta, è necessario che:

- tutte le attività e le operazioni svolte per conto di Anas siano improntate al massimo rispetto delle leggi vigenti, con particolare riferimento alle norme vigenti in materia di violazione del diritto di autore, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- sia garantita la separazione di ruoli e responsabilità in ciascuna fase dei processi interni della Società;
- sia assicurata la perfetta rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure interne;
- coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi all'espletamento delle attività sensibili, pongano particolare attenzione all'attuazione degli adempimenti stessi e riferiscano immediatamente all'OdV eventuali situazioni di irregolarità.

3 PRINCIPI DI CONTROLLO PER AREA A RISCHIO

Con riferimento all'area a "rischio reato", sono elencate le attività sensibili e le fattispecie di reato considerate rilevanti.

3.1 GESTIONE ICT

ATTIVITÀ SENSIBILI

- Gestione fabbisogni ICT
- Gestione e sviluppo soluzioni informatiche e infrastruttura tecnologica
- Gestione sicurezza informatica e terze parti.

FATTISPECIE DI REATO RILEVANTI

Art. 24 bis "Delitti informatici e trattamento illecito di dati"

- *Documenti informatici (Art. 491-bis c.p.)*

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici".

- *Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.)*

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

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

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

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

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

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

- *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater c.p.)*

"Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato".

- *Installazione di apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies c.p.)*

"Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater".

- *Danneggiamento di informazioni, dati e programmi telematici (Art. 635-bis c.p.)*

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

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

"Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

- *Danneggiamento di sistemi informatici o telematici (Art. 635-quater c.p.)*

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

- *Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.)*

"Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

- *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640-quinquies c.p.)*

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

Art. 25 novies "Delitti in materia di violazione del diritto d'autore"

- *Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o parte di essa (art. 171, comma 1, lettera a) bis e comma 3 Legge del 22 aprile 1941, n. 633)*

"Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

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

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

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

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

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

e) in violazione dell'articolo 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

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

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore".

- *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis legge del 22 aprile 1941, n. 633)*

"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 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.

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

- *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-ter legge del 22 aprile 1941, n. 633)*

"E' punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582,00 a euro 15.493,00 chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.
f bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti

ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale dì 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;

g) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102 quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. E' punito con la reclusione da uno a quattro anni e con la multa da euro 2.582,00 a euro 15.493,00 chiunque:

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

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

La pena è diminuita se il fatto è di particolare tenuità. La condanna per uno dei reati previsti nel comma 1 comporta:

a) applicazione delle pene accessorie di cui agli articoli 30 e 32 bis del codice penale;
b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale. 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."

- *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 septies legge del 22 aprile 1941, n. 633)*

"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".

- *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 octies legge del 22 aprile 1941, n. 633)*

"Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da e 2.582,00 a e 25.822,00 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".

CONTROLLI SPECIFICI

Con riferimento all'area a rischio "Gestione ICT", l'attività della Società si ispira ai seguenti principi di controllo:

- rispetto dei compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo nella gestione del processo;
- esistenza di specifici protocolli aziendali che descrivono ruoli, responsabilità, iter e modalità operative, nonché i controlli relativi alla gestione del processo;
- archiviazione di tutta la documentazione connessa alla gestione del processo, anche al fine di garantirne la tracciabilità;
- chiara identificazione delle modalità di richiesta e relativa autorizzazione riguardanti la rilevazione di nuove esigenze di tipo informatico;
- pianificazione degli approvvigionamenti in ambito ICT, in linea con le esigenze della Società;
- chiara identificazione di ruoli e responsabilità sia per quanto riguarda lo sviluppo di nuove applicazioni software, compreso lo sviluppo di nuove funzionalità e l'adeguamento delle applicazioni a fronte dell'evoluzione del contesto tecnologico, operativo e legislativo (manutenzione evolutiva), sia per quanto riguarda lo sviluppo di nuove soluzioni tecnologiche;
- chiara identificazione dei ruoli e responsabilità, delle modalità di richiesta, dei canali di invio della richiesta e dei livelli di servizio relativi all'erogazione di servizi da parte della Direzione ICT;
- implementazione di ambienti logicamente e fisicamente separati che consentono di controllare e testare le modifiche *software* sino al rilascio in produzione;
- adozione di meccanismi che consentono la tracciabilità nel tempo delle modifiche passate in produzione;
- previsione di controlli volti a monitorare l'istallazione dei software sui sistemi operativi, garantendo altresì la conformità legale (*copyright*).
- formale definizione delle regole per il corretto utilizzo degli strumenti informatici, ivi inclusi i software, da parte dei dipendenti;
- previsione di programmi di informazione e sensibilizzazione rivolti al personale aziendale in materia di corretto utilizzo degli *asset* informativi;

- formale individuazione degli amministratori di sistema;
- chiara individuazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- verifica sulle attività e sull'operato degli amministratori di sistema;
- concessione dei privilegi di accesso, ossia dei profili di autorizzazione per le operazioni sulle risorse informatiche, in funzione del principio del "*need to know*", ovvero commisurati al ruolo associato;
- previsione di apposite *password policy* per le utenze di dominio che impongono specifici requisiti per la creazione e il mantenimento delle password;
- registrazione di tutto il personale con accesso agli *asset* informatici della Società, al fine di garantire l'acquisizione, da parte di ciascun membro del personale, di un'identità digitale univoca;
- definizione formale delle regole per la rimozione dei diritti di accesso al termine del rapporto di lavoro;
- monitoraggio periodico dell'associazione tra utenza censita a sistema e mansione organizzativa al fine di garantire l'allineamento tra privilegi di accesso e ruolo organizzativo;
- tracciabilità, tramite log, degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio;
- esistenza di misure di protezione/restrizione volte a garantire la sicurezza perimetrale fisica del centro di elaborazione dati (CED) e ai nastri di salvataggio dei backup;
- formalizzazione dei rapporti con gli *outsourcer* di servizi informatici, attraverso specifici contratti approvati nel rispetto dei poteri di firma vigenti;
- esistenza di specifiche clausole, nell'ambito dei contratti stipulati con i fornitori, relative alla sicurezza informatica e telematica;
- implementazione di misure di sicurezza volte a garantire l'accesso alle informazioni aziendali da parte di terze parti solo previa autorizzazione formale e nel rispetto degli accordi di riservatezza e confidenzialità stipulati.