FONDAZIONE ITS MAKER

Sede Legale in Bologna, Via Bassanelli n. 9/11

MODELLO

DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

sulla “Responsabilità Amministrativa delle Imprese”

Parte Speciale

Violazione del diritto d’autore

Art. 25-novies del D.Lgs. n. 231/2001

Sommario

Premessa

La Legge 23 luglio 2009, n. 99, recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia e contenente modifiche al D. Lgs. n. 231/2001 (d'ora in poi 'Decreto'), ha esteso la responsabilità amministrativa degli Enti ai reati in materia di proprietà intellettuale, introducendo nel Decreto, tra i reati presupposto, i *'Delitti in materia di violazione del diritto di autore'* (art. 25 novies D. Lgs. 231/2001).

Si tratta di alcune delle fattispecie delittuose previste dalla L. 22 aprile 1941, n. 633 (Protezione del diritto di autore e di altri diritti connessi al suo esercizio) ed, in particolare, dei delitti di:

- messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, primo comma, lettera a-bis);
- reati di cui all'art. 171, commessi su opere altrui non destinate alla pubblicazione, qualora ne risulti offeso l'onore o la reputazione (art. 171, terzo comma);
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis, primo comma);
- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171 bis, secondo comma);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171 ter);
- mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171 septies);
- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 octies).

TIPOLOGIA DEI REATI RELATIVI AL DIRITTO D'AUTORE

Si riporta di seguito una breve descrizione dei reati contemplati nell'art. 25 *novies* del Decreto 231/01 la cui commissione possa comunque comportare un interesse e/o un vantaggio per ITSMAKER.

a. Art. 171, primo comma, lettera a-bis, e terzo comma, L. 633/1941

Il delitto di cui all'art. 171 primo comma, lettera a-bis, punisce (con la multa) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa.

L'inserimento della previsione nel Decreto mira a responsabilizzare tutte quelle aziende che gestiscono server attraverso cui si mettono a disposizione del pubblico opere protette da diritto d'autore.

La norma tutela l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.

Dal punto di vista soggettivo, basta a configurare il reato, il dolo generico, ovvero la coscienza e la volontà di porre in essere la condotta descritta dalla norma.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui l'Ente si appropri di ricerche/analisi e/o altri documenti contenenti i risultati delle attività portate avanti da ricercatori in modo da utilizzarne i contenuti o pubblicarli sul suo sito internet o su altre reti telematiche come se fossero propri.

Il delitto di cui al comma 3 dell'art. 171 è configurabile qualora sia integrata alternativamente una delle condotte menzionate dall'art. 171 (quindi sia l'ipotesi prevista dall'art. 171 lett. a bis, sopra descritta, sia le altre ipotesi indicate dalla norma, ovvero riproduzione, trascrizione, diffusione, messa in vendita, di un 'opera altrui o rivelazione del contenuto, prima che sia reso pubblico; o anche rappresentazione o diffusione di un'opera altrui) ove commesse su una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, o con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Il bene giuridico protetto dalla norma di cui al terzo comma consiste nella protezione dei diritti personali del titolare dell'opera, ovvero il suo onore e la sua reputazione, a differenza della ipotesi criminosa precedente che mira a tutelare l'aspettativa di guadagno del titolare dell'opera.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui ITSMAKER riproduca su documenti aziendali (giornali, materiali promozionali, comunicazione via internet, ecc.) opere altrui, prima che sia reso pubblico il contenuto, usurpandone la paternità o modificandone il contenuto, con la conseguenza dell'offesa all'onore od alla reputazione dell'autore.

b. Art. 171 bis, 1 e 2 comma, L. 633/1941

Il primo comma dell'art. 171 bis è volto a tutelare penalmente il c.d. software, punendo l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore; ma anche l'importazione, la distribuzione, la vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; è altresì punita la predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

La condotta può consistere anzitutto nella abusiva duplicazione, essendo prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro.

Il riferimento all'abusività della riproduzione indica che, sul piano soggettivo, il dolo dell'agente debba ricomprendere anche la conoscenza delle norme extra-penali che regolano la materia.

La seconda parte del comma indica le altre condotte che possono integrare il reato *de quo*: importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi "*piratati*". Si tratta di condotte caratterizzate dall'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale.

Infine, nell'ultima parte del comma, il legislatore ha inteso inserire una norma volta ad anticipare la tutela penale del software, punendo condotte aventi ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Sul piano soggettivo, tutte le condotte sono caratterizzate dal dolo specifico di profitto.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui l'Ente acquisti una singola licenza per un programma e provveda alla sua duplicazione, in modo da distribuire tali programmi al proprio interno e/o commercializzare tali programmi all'esterno.

Il comma 2 dell'art. 171 bis mira alla protezione delle banche dati; la condotta, invero, si concretizza nella riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; nell'estrazione o reimpiego della banca dati; nella distribuzione, vendita o concessione in locazione di banche di dati.

Per banche dati si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo, con esclusione dei contenuti e dei diritti sugli stessi esistenti.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui ITSMAKER, attraverso l'accesso a banche dati online (organismi di farmacovigilanza, enti di ricerca, ecc.), riproduca in tutto o in parte opere, testi e/o risultati di tipo scientifico al fine di trarne un vantaggio in termini di pubblicità.

c. Art. 171 ter, L. 633/1941

La norma punisce l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; la riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Perché sia integrato il reato *de quo*, oltre alla realizzazione di una delle condotte descritte dalla norma, devono ricorrere due requisiti: il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, che costituisce il fine ulteriore che l'agente deve avere di mira perché sia integrato il fatto tipico previsto dalla norma.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui ITSMAKER filmi/registri le discussioni e tutte le attività svolte nel corso di meeting/convegni/congressi organizzati da società competitor o da altri enti al fine di riutilizzare quanto emerso nel corso di tali occasioni per erogare formazione all'interno al suo interno o formazione a pagamento presso terzi.

d. Art. 171 septies, L. 633/1941

Il reato si configura allorquando i produttori ed importatori dei supporti non soggetti a contrassegno SIAE non comunichino alla SIAE stessa, entro 30 giorni dalla commercializzazione o dall'importazione, i dati necessari per l'univoca identificazione dei supporti medesimi nonché qualora si dichiari falsamente l'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi.

La disposizione, pertanto, è posta a tutela delle funzioni di controllo della SIAE, in un'ottica di tutela anticipata del diritto di autore. La fattispecie, di conseguenza, è un reato di ostacolo che si configura con la mera violazione dell'obbligo.

e. Art. 171 octies, L. 633/1941

La diposizione punisce chi, a fini fraudolenti, produce, pone in vendita, promuove, installa, modifica, utilizza per uso pubblico o privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

Ai fini della caratterizzazione della condotta, 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 dall'imposizione di un canone per la fruizione del servizio.

Dal punto di vista soggettivo oltre alla consapevolezza e volontà della condotta tipica è richiesto il perseguimento di fini fraudolenti.

PRINCIPALI ATTIVITA' A RISCHIO AI SENSI DEL DECRETO 231/2001.

In occasione dell'implementazione dell'attività di risk mapping, sono state individuate, nell'ambito della struttura organizzativa ed aziendale di ITSMAKER:

- le **aree** considerate "**a rischio reato**", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei delitti in materia di violazione dei diritti di autore;

- nell'ambito di ciascuna area "a rischio reato", sono state individuate le relative **attività c.d. "sensibili"**, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in considerazione;

- **i ruoli aziendali coinvolti nell'esecuzione di tali attività "sensibili"** e che, astrattamente, potrebbero commettere i delitti in materia di violazione dei diritti di autore; sebbene tale individuazione dei ruoli/funzioni non debba considerarsi, in ogni caso, tassativa atteso che ciascun soggetto individuato nelle procedure potrebbe in linea teorica essere coinvolto a titolo di concorso; in particolare, nell'ambito dei ruoli coinvolti, sono eventualmente riportate anche gli Enti/Aziende che, in virtù di contratto di servizi stipulato con ITSMAKER, svolgono le attività sensibili nell'interesse di ITSMAKER;

- in via esemplificativa, **i principali controlli procedurali previsti** con riferimento alle attività che sono poste in essere nelle aree "*a rischio reato*", oltre alle regole definite nel Modello di organizzazione, gestione e controllo e nelle sue procedure o regolamenti interni - dirette ad assicurare la chiara definizione dei ruoli e delle responsabilità degli attori coinvolti nel processo e l'individuazione dei principi di comportamento.

Di seguito è riepilogato il quadro in precedenza esposto per ogni area a rischio reato.

Area a rischio n. 1: ACQUISTI DI BENI E SERVIZI	
Funzioni aziendali coinvolte	- Personale di segreteria e amministrazione - Referente di Sede - Direttore Operativo - Presidente - Responsabile Amministrativo
Attività sensibili	- Raccolta e controllo delle proposte di acquisto - Richieste di offerte, valutazione delle offerte, negoziazione e gestione degli acquistiurgenti - Gestione del sistema di qualificazione e selezione dei fornitori - Emissione degli ordini di acquisto - Stipula e gestione dei contratti - Verifica delle prestazioni/beni acquistati - Gestione dei conferimenti di incarichi a consulenti / professionisti esterni
Reati astrattamente ipotizzabili	- *Art. 171, terzo comma, L. 633/1941* - *Art. 171 bis, primo e secondo comma, L. 633/19413)* - *Art. 171 ter, L. 633/1941*

Principali controlli esistenti	- adozione di specifiche procedure volte a disciplinare il processo di acquisto di beni e servizi nonché il processo di selezione e qualifica dei fornitori; in dettaglio, sono adottate le seguenti procedure: Procedura Acquisti, Procedura di Gestione incarichi; Regolamento contabile-amministrativo - chiara definizione dei ruoli e delle responsabilità delle funzioni coinvolte nel processo, nonché dei reciproci flussi informativi; - diffusione, tramite sistema aziendale interno, delle procedure a tutte le risorse/funzioni coinvolte nel processo; - ambito di applicazione delle procedure chiaramente dettagliato; - il processo di selezione, approvazione e inserimento dei fornitori nell'elenco fornitori prevede la selezione del/i fornitore/i da parte del coordinatore o referente di Sede; - il processo di selezione, approvazione e utilizzo dei fornitori nell'elenco dei fornitori, che possono avere rapporti con la PA, prevede l'approvazione definitiva da parte della Direzione; - presenza di una prassi operativa che prevede, prima di scegliere uno specifico fornitore, l'effettuazione di contatti con due o più fornitori, a seconda delle spese di importo, presenti o da inserire all'interno dell'albo fornitori, al fine dell'ottenimento delle offerte;

Principali controlli esistenti	- predisposizione nelle procedure di autorizzazione delle proposte di acquisto e di criteri e modalità di assegnazione del contratto; ITSMAKER prevede per qualsiasi tipologia di acquisto la formalizzazione di un contratto validato, salvo piccoli acquisti di materiale di consumo per cassa; - previsione dello svolgimento di una gara tra i fornitori per specifiche soglie importi di acquisto; - definizione di criteri di valutazione delle offerte ricevute al fine di individuare la migliore offerta in termini di economicità e di qualità dei beni e servizi offerti; - previsione di un eventuale controllo ex post sull'eventuale utilizzo di fornitori (in funzione dell'importo del contratto) ; - predisposizione di specifico strumento organizzativo che definisca le modalità di qualifica, valutazione e classificazione di fornitori e contrattisti; - svolgimento di adeguate attività di Due Diligence, prima della definizione degli accordi con terze parti; predisposizione di specifiche verifiche in relazione ad eventuali conflitti di interesse dei fornitori; - processo di qualifica, per ogni nuovo fornitore, con il quale questi viene sottoposto ad una analisi volta a valutare l'affidabilità economico-finanziaria, la professionalità e il possesso dei requisiti etici e tecnico-qualitativi; - gestione di specifiche liste di fornitori nelle quali iscrivere i soggetti in possesso dei requisiti richiesti; in dettaglio ITSMAKER dispone di un elenco dei fornitori pubblicato su *Sharepoint*. L'elenco viene aggiornato costantemente man mano che vengono effettuati o rinnovati i singoli processi di utilizzo di un nuovo fornitore o al riutilizzo di un fornitore già esistente; - garanzia che per acquisti (singoli o cumulati) al di sopra di un valore soglia definito sia richiesto, per la qualifica del fornitore (e degli eventuali subappaltatori utilizzati), la richiesta di un'autocertificazione sul casellario giudiziale e sui carichi pendenti, effettuata nel processo di Due Diligence, oltre che l'adesione ai principi che regolamentano il modello 231/01 dell'Ente; - Eventuale predisposizione di una black list per i fornitori; - svolgimento di una sistematica attività di analisi dei fornitori registrati al fine di disattivare fornitori non più utilizzati da un determinato lasso di tempo o doppi e di verifica delle anagrafiche - svolgimento di specifici audit al fine di verificare l'adeguatezza dei sistemi utilizzati; - monitoraggio degli ordini fino alla conclusione del processo di acquisto al fine di evitare il rischio di registrazione di transazioni improprie; - gestione delle approvazioni per eventuali modifiche/integrazioni dei PO;

	- gestioni contrattuali standardizzate in relazione a natura e tipologie di contratto, (es. docenti) contemplando clausole contrattuali finalizzate all'osservanza di principi di controllo nella gestione delle attività da parte del terzo (registri e timesheet) - previsione, negli schemi contrattuali/ordini utilizzati, di una clausola risolutiva del contratto in caso di mancato rispetto di quanto previsto dal modello ex D.Lgs. 231/01; - adozione di un Codice di Comportamento rivolto ai fornitori che contenga regole etico-sociali atte a disciplinare i rapporti con ITSMAKER, da allegarsi ai contratti; - predisposizione di una clausola risolutiva espressa per il caso in cui l'impresa fornitrice non rispetti le norme di qualificazione etica, di autoregolamentazione o l'obbligo di denunciare i reati subiti direttamente o dai propri familiari e/o collaboratori; - controlli sui collaboratori esterni e sulla congruità dei costi rispetto a quelli praticati normalmente nell'area geografica di riferimento;

Area a rischio n. 2: GESTIONE SISTEMI INFORMATIVI/INFORMATION TECHNOLOGY	
Funzioni aziendali coinvolte	- Sistemista (esterno) - Referente sistemi integrati - Referenti tecnici di sede
Attività sensibili	Gestione della sicurezza informatica sia a livello fisico che a livello logico Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici Gestione dell'attività di manutenzione dei sistemi esistenti e gestione dell'attività di elaborazione dei dati Gestione e protezione delle reti Attività di back-up dei dati e degli applicativi Gestione banche dati e software
Reati astrattamente ipotizzabili	*Art. 171, primo comma, lettera a-bis, L. 633/1941* *Art. 171, terzo comma, L. 633/1941* *Art. 171- bis, primo comma, L. 633/1941* *Art. 171- bis, secondo comma, L. 633/1941* *Art. 171 ter, L. 633/1941*

Principali controlli esistenti	Adozione di apposite procedure che regolamentano: • le attività di gestione attraverso l'uso di sistemi informativi; • la gestione del sito internet; • la gestione/archiviazione delle informazioni aziendali; – diffusione delle procedure aziendali attraverso un sistema aziendale interno (Sharepoint/Office 365-Teams); – chiara segregazione di funzioni e responsabilità nelle attività relative alla gestione della rete, all'amministrazione dei sistemi e allo sviluppo/manutenzione degli applicativi; tutti i server di ITSMAKER sono su cloud; – adozione di procedure, emanate e gestite a livello centralizzato, per la gestione delle credenziali di accesso ai sistemi ed il loro monitoraggio periodico; – criteri per le attribuzioni degli accessi ai dati e identificazione dei i soggetti ammessi al processo di richiesta, verifica ed autorizzazione degli accessi; regolamentazione della rimozione dei diritti di accesso al termine del rapporto di lavoro; – svolgimento a livello centralizzato della gestione delle configurazioni dei PC e del loro monitoraggio; – predisposizione di operazioni di intervento e ripristino delle configurazioni dei sistemi in caso di anomalia; – identificazione di tutti gli utenti attraverso una user ID personale tramite il quale accedono ai vari applicativi; – definizione centralizzata di criteri minimi di robustezza per la scelta delle password (ogni password è alfanumerica e contiene almeno un carattere maiuscolo e almeno un carattere speciale) e definizione centralizzata delle password; – divieto di lasciare attiva una sessione di lavoro in caso di allontanamento dal PC; – necessità di nuovo login con password dopo diversi minuti di inattività; – predisposizione di misure per un'adeguata protezione delle apparecchiature incustodite; – mappatura e monitoraggio dei sistemi da remoto; – predisposizione di adeguato riscontro delle password di abilitazione per l'accesso ai Sistemi Informativi della PA, possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche funzioni/strutture aziendali;

	- in dettaglio i dipendenti provvedono in autonomia alla creazione di profili per comunicare/inviare documentazione alla PA. Il Servizio IT prevede attività di training ed aggiornamento al fine di sensibilizzare i dipendenti di ITSMAKER in relazione ai predetti aspetti. Tutti i dipendenti ricevono aggiornamenti on line (Chat/Teams) sull'evoluzione delle funzioni e delle procedure dei sistemi informativi; - previsione dell'utilizzo della firma digitale per la trasmissione della documentazione alla PA da parte delle funzioni preposte a tale attività; - previsione di adozione di misure di protezione dei documenti elettronici (Crittografia, Firma digitale -in fase di sviluppo); - obbligo, per gli utenti, di attività di formazione on-line finalizzati alla sensibilizzazione all'uso appropriato degli strumenti informatici ed alle misure di sicurezza; - adozione di direttive e norme di carattere etico, dirette ai singoli utenti, riguardanti tutti i processi legati all'Information Technology e finalizzate alla sensibilizzazione in tale ambito;

	- regole volte a prevedere: limitazione dell'utilizzo dei sistemi informatici o telematici ai soli fini lavorativi; accesso alle informazioni aziendali solo previa autorizzazione della direzione; accesso alle informazioni aziendali solo mediante gli strumenti concessi ed autorizzati; riservatezza delle informazioni aziendali; elaborazione dei dati nel rispetto delle modalità previste dalle procedure aziendali; integrità dei dati elaborati; impossibilità di installare sui sistemi informatici/telematici societari software o hardware non autorizzati; impossibilità di introdurre sul luogo di lavoro dispositivi hardware/software non autorizzati; - predisposizione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business; - definizione formale dei criteri per l'identificazione dei soggetti proprietari dei dati e per la loro classificazione (tramite One Drive-SharePoint); - controllo del trasferimento dei dati sensibili mediante supporti esterni o rimovibili; - adozione di una regola nella quale è definita la modalità di crittografia che i dipendenti devono adottare per lo scambio dati; - esplicito riferimento, nelle procedure adottate, della responsabilità dei dipendenti nei confronti delle informazioni loro affidate; - formalizzazione, delle regole per il corretto utilizzo dei beni aziendali destinati allo scambio ed elaborazione di dati (PC desktop, laptop, cellulari, ecc.) che sono sottoscritte da tutti i collaboratori che utilizzano tali beni; - divieto assoluto di accesso ai siti a pagamento, a quelli contenenti materiale osceno ovvero collegato, a qualsiasi titolo, ad attività illecite; - divieto di configurare Client di posta non aziendali; - limitazioni nell'utilizzo di dispositivi elettronici che prescrivono che l'accesso ad Internet sia consentito per finalità attinenti l'attività lavorativa mentre viene tollerato il moderato utilizzo per fini personali purché lo stesso, direttamente o indirettamente, non costituisca reato; - centralizzazione a livello globale del coordinamento delle attività legate alla sicurezza informatica; - adeguata comunicazione delle procedure di sicurezza informatica (fisica/logica) (es.: utilizzo di password, ecc.); - presenza di personale tecnico preparato e preposto principalmente a garantire il buon funzionamento dei sistemi informativi;

	- predisposizione di specifici controlli su: rete aziendali e informazioni che vi transitano; instradamento (routing) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza; installazione di SW sui sistemi operativi; - utilizzo di software antivirus che controllano il traffico di rete in entrata ed in uscita e sensibilizzazione, digitalmente tracciata, sul tema nei confronti degli gli utenti; - periodico aggiornamento dei sistemi informativi; - installazione di un proxy server e/o firewall che effettui il monitoraggio del traffico di dati segnalando eventuali anomalie e mantenendone traccia; - predisposizione di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi; - adozione di un sistema di Software/hardware Inventory che monitora singolarmente ogni PC/Utente; - inventariazione dei software e hardware per ogni singolo Utente segnalando eventuali anomalie; - tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali; - predisposizione di un controllo periodico volto a riconciliare il numero di licenze acquistate vs il numero di utenti autorizzati; - predisposizione di un elenco dei SW aziendali e dei relativi amministratori di sistema; in dettaglio è prevista una mappatura periodica. Per ogni sistema viene definito un System Manager (amministratore lato tecnico) e un System Owner (lato funzionale). - adeguata archiviazione della documentazione relativa al ciclo di approvazione delle modifiche/cancellazioni/integrazioni dei siti internet; - adeguato tracciamento del processo di aggiornamento degli applicativi/DB; - formalizzazione di una procedura per il back up dei dati, gestita a livello centrale; - necessaria autorizzazione formale a procedere in caso sia necessario effettuare un *restore* dei dati di back-up; - custodia dei back-up in luogo protetto da furti e incendi nonché diverso rispetto a quello in cui sono custoditi i dati (backup locale(PC) e sulla rete); - pedissequo rispetto, da parte di ITSMAKER, della normativa sulla privacy; - predisposizione di apposite verifiche sui mezzi di comunicazione interni ed esterni al fine di prevenire la diffusione di informazioni sensibili.

Area a rischio n. 3: ATTIVITÀ DI COMUNICAZIONE ESTERNA	
Funzioni aziendali coinvolte	Direttore Responsabile Operativo Referente Orientamento Referente Sito web Referente Gestione eventi Referente Canali social Referente Ufficio stampa
Attività sensibili	a) Gestione dei rapporti con i mass media, compresi: - contatti con giornalisti e/o rappresentanti dei mass media (giornali, radio, televisione) - gestione delle iniziative con i mass media (giornali, radio, televisione) e i social (Facebook, eventi stream, ecc.) b) Scelta e pubblicazione dei testi/immagini e di qualsiasi altro contenuto suscettibile di essere protetto da diritti di proprietà industriale/intellettuale c) Pubblicità
Reati astrattamente ipotizzabili	*Art. 171, primo comma, lettera a-bis, L. 633/1941* *Art. 171 bis, secondo comma, L. 633/1941* *Art. 171, terzo comma, L. 633/1941* *Art. 171 ter, L. 633/1941*
Principali controlli esistenti	– definizione, approvazione e aggiornamento di una procedura che disciplina il processo di gestione del sito internet; – definizione formale dei ruoli, delle responsabilità, dei flussi informativi tra le varie funzioni aziendali coinvolte: – chiara segregazione delle funzioni coinvolte nel processo; in particolare, il sito internet è gestito da Digital 24, inoltre è previsto un referente interno che provvede ad approvare e verificare i contenuti presenti sul sito internet; – definizione di ruoli e delle responsabilità deputate ad intrattenere rapporti con i mass media; definizione del Referente della gestione del sito internet aziendale – monitoraggio periodico dei siti internet al fine di verificare che la loro gestione avvenga secondo le linee guida stabilite; – chiara identificazione nel sito internet predisposto, della fonte di tutte le informazioni riportate sul sito stesso, nonché i destinatari di tali informazioni e gli obiettivi; – specifico coinvolgimento del CTS nel caso in cui il materiale prodotto per la comunicazione abbia contenuti scientifici;

	– l'elaborazione dei contenuti sviluppati per la pubblicazione sul sito web ITSMAKER di carattere promozionale, è riservata agli operatori previsti nella funzione Comunicazione; – definizione di uno specifico iter di approvazione dei contenuti e del materiale da pubblicare attraverso il sito web, al fine di verificare la coerenza dei contenuti con gli obiettivi e le aree di intervento; – svolgimento di procedure di verifica per comunicati stampa, strutturate in vari controlli sulle successive bozze dei comunicati fino alla versione definitiva attraverso il coinvolgimento delle funzioni responsabili;.

Area a rischio n. 4: GESTIONE DEI MATERIALI PROMOZIONALI	
Funzioni aziendali coinvolte	Direttore Responsabile Operativo Referente Orientamento Referente Sito web Referente Gestione eventi Referente Canali social
Attività sensibili	Diffusione e distribuzione di materiale tecnico/omaggi quali, ad es., brand reminder esupporti cartacei e/o elettronici e/o informatici ecc., suscettibili di essere protetti dal diritto d'autore
Reati astrattamente ipotizzabili	*art. 171 bis, primo e secondo comma, L. 633/1941* *art. 171, terzo comma, L. 633/1941* *art. 171 ter, L. 633/1941*
Principali controlli esistenti	– regolamentazione delle attività in cui si esplica il processo di gestione del materiale informativo/promozionale; nonché i principi etici di comportamento – identificazione chiara dei ruoli aziendali responsabili delle funzioni coinvolte nel processo; – definizione delle funzioni coinvolte nelle attività relative alle fasi di progettazione, approvazione, esecuzione, chiusura e rendicontazione della gestione del materiale informativo/promozionale; – distribuzione all'esterno di omaggi promozionali di un valore economico percepito trascurabile, infungibili e acquistati direttamente dall'azienda a livello centrale;

Principali controlli esistenti	- attinenza dei materiali informativo/promozionali alle attività formative esercitate; - contenuti dell'informazione verso l'esterno sempre aggiornata e documentata; - adeguata e formale approvazione dei materiali informativi/promozionali da un punto di vista tecnico e valutazione del costo; - monitoraggio del valore di eventuali materiali informativo/promozionali (brand reminder) distribuiti agli allievi, ai docenti e al personale interno, al fine di rispettare le regole etiche; - cessione a titolo gratuito del materiale informativo di consultazione tecnica o di lavoro alle strutture formative di pari grado presenti nella Rete ITS; - netta separazione tra informazione e pubblicità, nel rispetto della regola della trasparenza, in merito alla pubblicità su giornali e riviste, garantendo sempre al lettore l'immediata riconoscibilità del messaggio promozionale in qualunque sua forma, sia essa redazionale che tabellare; - disciplina attraverso procedure/linee guida del richiamo del materiale informativo/promozionale in caso di blocco divulgativo/sospensione del materiale obsoleto; - attività di controllo volto a verificare che eventuale materiale ricevuto da fornitori di beni (stampe, brand reminder) o partner risulti coerente con il materiale informativo/promozionale richiesto e da diffondere; - archiviazione di tutta la documentazione relativa ai materiali informativo/promozionali sviluppati; - previsione ed apposizione di modifiche sul materiale informativo/promozionale ottenuto dai soci o dagli altri Enti (finanziatori o non), al fine di allinearlo alle esigenze di marketing e alla normativa vigenze; - selezione delle agenzie che si occupano di sviluppare la creazione dei materiali informativi/promozionali dall' elenco fornitori e/o attraverso una gara tra almeno due fornitori; - disciplina formale dei rapporti con i fornitori di materiali informativi/promozionali attraverso la stipula di contratti; in particolare, i suddetti contratti vengono redatti secondo formule contrattuali standard; - definizione di un'apposita clausola risolutiva all'interno dei contratti in caso di violazione del Modello ex D.Lgs. 231/01; - approvazione di un contratto da parte di un soggetto dotato di idonea procura (nei limiti e negli ambiti consentiti); - conformità delle informazioni contenute nel materiale informativo/promozionale con la regole previste dall'Ente Finanziatore.

PRINCIPI GENERALI DI COMPORTAMENTO E PRESCRIZIONI SPECIFICHE.

I PRINCIPI GENERALI DI COMPORTAMENTO

Nell'espletamento della propria attività per conto di ITSMAKER, i responsabili della funzione coinvolta nell'area *"a rischio reato*" sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello.

A tutti i destinatari del Modello è fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dall'art. 25novies del Decreto;

- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto realizzarla;

- di duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale, o comunque per trarne profitto, senza averne diritto, programmi per elaboratori, banche dati protette ovvero qualsiasi opera protetta dal diritto d'autore e da diritti connessi, incluse opere a contenuto letterario, musicale, multimediale, cinematografico, artistico;

- di diffondere tramite reti telematiche - senza averne diritto - un'opera dell'ingegno o parte di essa;

- di mettere in atto pratiche di file sharing, attraverso lo scambio e/o la condivisione di qualsivoglia tipologia di file attraverso piattaforme di tipo peer to peer.

-di rispettare tutte le procedure previste dall'Ente per la prevenzione della commissione delle ipotesi di reato presupposto di cui alla presente parte speciale.

È, inoltre necessario:

- che tutte le attività e le operazioni svolte per conto di ITSMAKER – ivi incluso per ciò che attiene i contatti relativi a rapporti con Enti paritari o finanziatori - 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;

- che sia rispettato il principio di separazione di ruoli e responsabilità nelle fasi dei processi interni dell'Ente;

- che sia assicurata la massima rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure interne, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività "sensibili" nelle aree ''a rischio reato" indicate;

- che coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi all'espletamento delle suddette attività ''sensibili'' pongano particolare attenzione all'attuazione degli adempimenti stessi e riferiscano immediatamente all'Organismo di Vigilanza (di seguito, anche 'OdV') eventuali situazioni di irregolarità.

Inoltre, ai fini dell'attuazione dei comportamenti di cui sopra, ITSMAKER:

- ha inserito nelle norme di comportamento (o nel Codice Etico) adottate dall'Ente specifiche previsioni riguardanti i delitti in materia di violazione dei diritti d'autore;

- ha previsto sanzioni in caso di violazione del Modello anche con riferimento alle fattispecie di cui alla presente Parte Speciale;

- ha previsto la realizzazione di una adeguata attività di comunicazione e formazione sui contenuti del Codice Etico e del Modello di organizzazione, gestione e controllo;

- ha disposto regole sull'utilizzo di materiale protetto dal diritto d'autore;

- ha previsto la formalizzazione di contratti e di clausole specifiche per la gestione dei diritti d'autore;

- ha previsto il divieto di installazione e utilizzo non autorizzato di sistemi di file sharing.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.

ATTIVITA' E VERIFICHE DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza verifica che le procedure adottate siano rispettate e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza segnala la necessità di adeguamento ed eventuali necessità di integrazione delle prescrizioni specifiche di cui sopra e delle relative procedure di attuazione.

L'OdV incontra periodicamente i responsabili di funzione per uno scambio informativo al fine di verificare eventuali carenze o necessità di ulteriori interventi a presidio dell'area interessata.

L'ODV vaglia le informazioni e le segnalazioni ricevute nella casella di posta elettronica dedicata.

L'ODV informa l'ente delle modifiche legislativa e delle buone prassi per la gestione della prevenzione del rischio commissione reato presupposto.

PROCEDURE A PRESIDIO DELLA PRESENTE PARTE SPECIALE

Le procedure a presidio della seguente Parte Speciale sono previste:

- MODELLO ORGANIZZATIVO PRIVACY E REGISTRO DEL TRATTAMENTO DATI.
- REGOLAMENTO AZIENDALE – CODICE ETICO INFORMATICO
- MANUALE ITS GESTIONE QUALITA'
- MANUALE GESTIONE ATTIVITÀ FORMATIVE