PARTE SPECIALE – E –

Delitti informatici e in materia di violazione del diritto d'autore

CAPITOLO E.1

E.1.1. Le fattispecie dei delitti informatici (art. 24-*bis* del Decreto 231) e in materia di violazione del diritto d'autore (art. 25-*novies* del Decreto 231)

La presente Parte Speciale si riferisce ai delitti informatici (art. 24-*bis*), nonché ai delitti in materia di violazione del diritto d'autore introdotti dalla Legge 99/2009 tra i reati presupposto sanzionabili ai sensi del Decreto 231 (art. 25-*novies*).

Si descrivono qui di seguito le singole fattispecie di reato per le quali gli artt. 24-*bis* e 25-*novies* del D. Lgs. n. 231/2001 prevedono una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi. A tal riguardo si sottolinea che, nonostante le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno trattarli un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le Attività Sensibili risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i princìpi comportamentali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

E.1.2. Delitti informatici

Sulla base delle analisi condotte, sono considerati applicabili ad Artsana i seguenti reati:

Art. 491-bis c.p. – Falsità in documenti informatici	*La norma stabilisce che i delitti di falsità in atti previsti dal Codice Penale (Capo III, Titolo VII, Libro II) sono punibili anche nel caso in cui l'oggetto della condotta sia un "documento informatico pubblico", ovvero un documento pubblico avente efficacia probatoria, in quanto rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti.*
Art. 615-ter c.p. – Accesso abusivo ad un sistema informatico o telematico	*Tale reato si realizza quando un soggetto si introduca abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza.* *A tal riguardo si sottolinea come il Legislatore abbia inteso punire l'accesso non autorizzato ad un sistema informatico o telematico tout court, e dunque anche quando ad esempio all'accesso non segua un danneggiamento di dati (si pensi all'ipotesi in cui un*

	soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio, limitandosi ad eseguire una copia, oppure procedendo solo alla visualizzazione di informazioni). *La suddetta fattispecie delittuosa si realizza, altresì, nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema.* *Il delitto potrebbe essere astrattamente configurabile, ad esempio, nell'ipotesi in cui un dipendente della Società acceda, abusivamente, utilizzando password indebitamente carpite, al sistema informatico di una società concorrente per prendere cognizione di dati riservati durante una negoziazione commerciale.*
Art. 615-quater c.p. – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	*Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.* *L'art. 615 quater c.p., pertanto, punisce le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.* *I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (quali badge o smart card).* *La norma punisce, inoltre, il rilascio di istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.* *A titolo di esempio, il reato potrebbe configurarsi nel caso in cui un dipendente della Società, una volta procuratesi le credenziali, comunichi o consegni a terzi codici, parole chiave o altri mezzi necessari all'accesso al sistema informatico di una società concorrente.*
Art. 615-quinquies c.p. – Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	*Tale reato si realizza qualora qualcuno, 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 procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.* *A titolo di esempio, il reato potrebbe configurarsi qualora un dipendente della Società effettui attacchi di hacking per alterare i dati relativi, ad esempio, ai dossier dei prodotti di una società concorrente.*
Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici	*Il reato punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.* *A titolo di esempio, il reato potrebbe ravvisarsi nella condotta del dipendente della Società che proceda alla eliminazione o alterazione dei file di un programma informatico di un creditore della Società, al fine, ad esempio, di far sparire dati compromettenti o di celare la prova di un credito vantato da un fornitore nei confronti della Società.*
Art. 635-ter c.p. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o	*Tale reato si realizza quando un soggetto commetta 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.* *Tale delitto si distingue dal precedente poiché, in questo caso, viene attribuito rilievo penale non solo al danneggiamento in sé, ma anche*

comunque di pubblica utilità	*ai fatti preparatori del danneggiamento, e si configura pertanto come reato di pericolo; inoltre, le condotte dannose hanno ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati, ma destinati al soddisfacimento di un interesse di natura pubblica.* *A titolo esemplificativo, tale fattispecie potrebbe, astrattamente, realizzarsi nell'ipotesi in cui un dipendente della Società distrugga documenti informatici detenuti dall'Autorità giudiziaria relativi ad una ipotetica indagine nei confronti della Società.*
Art. 635-quater c.p. – Danneggiamento di sistemi informatici o telematici	*Il reato si realizza quando l'agente, mediante le condotte di cui all'art. 635 bis c.p. (e cioè distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. La differenza tra i due reati si ravvisa nella circostanza che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di cui al 635-quater quando invece riguarda solo i dati, informazioni, programmi, integrerà il delitto di danneggiamento dei dati previsto dall'art. 635-bis c.p.* *Si veda l'esempio di modalità di commissione dell'illecito indicato in corrispondenza del reato di cui all'art. 635-bis c.p., qualora la condotta abbia come conseguenza la distruzione, il danneggiamento o l'inservibilità di un sistema informatico o telematico altrui (per esempio, di un concorrente).*
Art. 635-quinquies c.p. – Danneggiamento di sistemi informatici o telematici di pubblica utilità	*Il reato si configura quando la condotta di cui all'art. 635-quater c.p. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.* *Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter c.p., quel che rileva è in primo luogo che il danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.* *A titolo esemplificativo, tale fattispecie potrebbe astrattamente realizzarsi nell'ipotesi in cui un dipendente della Società, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, danneggi sistemi informatici o telematici dell'Autorità giudiziaria (in caso di pendenza di una ipotetica indagine nei confronti della Società).*

E.1.3. Delitti in materia di violazione del diritto d'autore

Sulla base delle analisi condotte, sono considerati applicabili ad Artsana i seguenti reati:

Art. 171, co. 1, lett. a-bis) e co. 3 della Legge 22 aprile 1941 n. 633. – Divulgazione tramite reti telematiche di un'opera dell'ingegno	*La norma punisce la condotta consistente nel mettere a disposizione del pubblico un'opera dell'ingegno protetta, o parte di essa, mediante immissione in un sistema di reti informatiche, senza il consenso dell'avente diritto.* *Si tratta di una disposizione di carattere residuale, e cioè applicabile solo qualora il fatto non rientri tra le fattispecie previste dagli artt.*

protetta	*171-bis e 171-ter della Legge n. 633/1941, che mantiene tuttavia un'importanza sistematica in quanto, a differenza delle norme successive, non richiede il dolo specifico dello scopo di lucro o di profitto per il perfezionamento del reato.* *La condotta tipica si riferisce al cd. peer-to-peer ma include la sola immissione in Internet dei materiali protetti dal diritto d'autore e non le condotte successive di condivisione e diffusione, che consentono a chiunque di accedere alle opere in questione.* *Il comma 3 dell'art. 171 prevede alcune circostanze aggravanti delle ipotesi di reato formulate al comma 1 ed opera nelle ipotesi in cui l'opera non sia destinata alla pubblicazione, ovvero venga usurpata la paternità dell'opera (inclusa l'ipotesi di plagio), ovvero ancora l'opera venga deformata, mutilata o modificata in modo tale da arrecare danno all'onore ed alla reputazione dell'autore.*
Art. 171-bis della Legge 22 aprile 1941 n. 633. – Duplicazione, a fini di lucro, di programmi informatici o importazione, distribuzione, vendita, detenzione per fini commerciali di programmi contenuti in supporti non contrassegnati dalla SIAE	*La norma ha introdotto nel panorama normativo italiano la tutela penale del software e si suddivide in due commi. Il primo comma (inserito con il Decreto Legislativo 29 dicembre 1992, n. 518, attuazione della direttiva 91/250/CEE) tutela i programmi per elaboratore, o software; il secondo comma (inserito con Decreto Legislativo 6 maggio 1999, n. 169, attuazione della direttiva 96/9/CE) tutela le banche di dati. Le banche di dati, intese come "raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto" (cfr. art. 2, punto 9 della Legge n. 633/1941), sono protette se "per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore" (cfr. secondo comma dell'articolo 1 della Legge n. 633/1941). Per configurare i reati di cui all'art. 171-bis in parola è necessario il dolo specifico, poiché gli illeciti devono essere compiuti con lo scopo di profitto; si tratta di una nozione più ampia del fine di lucro, in quanto il fine di lucro implica un fine di guadagno economicamente apprezzabile o un incremento patrimoniale da parte dell'autore del fatto, mentre lo scopo di profitto può identificarsi con un vantaggio di diverso genere, per esempio il possibile risparmio di spesa derivante dall'utilizzo interno di copie non autorizzate di programmi per elaboratore.* *È inoltre elemento costitutivo della condotta la sua abusività, ovverosia che l'atto sia compiuto senza il consenso del titolare del diritto, e riguardi programmi o banche di dati contenuti in supporti non contrassegnati dalla Società Italiana degli Autori ed Editori (qui di seguito "SIAE").*
Art. 171-ter della Legge 22 aprile 1941 n. 633 – Duplicazione, riproduzione, trasmissione – per uso non personale e a scopo di lucro – di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio	*La disposizione è volta alla tutela dei titolari di diritti d'autore da un'ampia gamma di comportamenti di pirateria fonografica e videografica ed è volta in sintesi a sanzionare gli atti, compiuti in violazione dei diritti del titolare, di abusiva duplicazione e riproduzione dell'opera e di trasmissione e diffusione della stessa in pubblico, nonché le condotte di chi - pur non avendo partecipato alla duplicazione o riproduzione abusiva - importa o compie atti di distribuzione commerciale, di noleggio o di trasmissione abusiva delle riproduzioni "pirata". La norma è altresì volta a reprimere la contraffazione o alterazione dei contrassegni SIAE, l'accesso abusivo a servizi ad accesso condizionato (cioè con segnale criptato, che deve essere decodificato dall'utente mediante idonei apparecchi e dispositivi) o la loro diffusione non autorizzata, l'importazione, commercializzazione ed installazione di dispositivi per la decodificazione in grado di eludere le barriere tecniche che proteggono la criptazione di segnali codificati, l'elusione delle misure tecnologiche di protezione del diritto d'autore e l'alterazione o rimozione delle informazioni sul regime dei diritti d'autore.*

	Le condotte specifiche oggetto della disposizione sono numerose; a restringere tuttavia l'ambito di applicazione sono due requisiti necessari per integrate il fatto tipico: il fine della condotta per fare un uso non personale dell'opera dell'ingegno ed il dolo specifico del fine di lucro. *Oggetto della tutela sono le opere dell'ingegno, incluse le opere destinate al circuito radiotelevisivo e cinematografico e le opere letterarie, drammatiche, scientifiche, didattiche, musicali, drammatico-musicali e multimediali, nonché le opere incorporate in supporti di qualsiasi tipo, contenenti fonogrammi e videogrammi, per i quali è prescritta l'apposizione del contrassegno SIAE.*

CAPITOLO E.2

E.2.1 Attività Sensibili nell'ambito dei delitti informatici e delitti in violazione del diritto d'autore

A seguito di una approfondita analisi della realtà aziendale, le principali Attività Sensibili che la Società ha individuato al proprio interno sono le seguenti:

1) Assegnazione e utilizzo delle risorse ICT ad uso individuale da parte degli utenti interni ed esterni;
2) Accesso ad un sistema informatico o telematico e/o sottostante infrastruttura di un soggetto terzo (anche finalizzato al trasferimento di denaro, di valore monetario o di valuta virtuale) o di Artsana e/o accesso e gestione informatica di documenti con valore probatorio da parte di utenti interni ed esterni;
3) Installazione di software su hardware, postazioni di lavoro fisse o mobili, dispositivi di rete, comunicazione o di memorizzazione;
4) Attività di ricerca e sviluppo;
5) Attività di ricerca e sviluppo dell'area Fashion;
6) Definizione e svolgimento di attività di pubblicità, promozione e marketing;
7) Gestione dei contenuti del sito internet della Società e dei relativi social network, anche tramite soggetti terzi;
8) Gestione dei marchi e brevetti industriali.

CAPITOLO E.3

Princìpi di comportamento generali

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali e i soggetti che operano a livello periferico (consulenti, *service provider*, ecc.) nella misura in cui gli stessi possano essere coinvolti nelle Attività Sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici e di Delitti in violazione del Diritto d'Autore.

Nell'espletamento delle attività aziendali e, in particolare, nelle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (art. 24-*bis* e 25-*novies* del Decreto).

In particolare, non è ammesso:

- porre in essere quei comportamenti che (i) integrano le fattispecie di reato o, (ii) sebbene non costituiscano di per sé un'ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo);
- divulgare informazioni relative ai sistemi informatici aziendali che possano rivelare carenze e/o modalità di utilizzo distorte e non consentite degli stessi;
- utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di terze parti, comprensivo di archivi, dati e programmi;

- installare autonomamente nel PC in dotazione per uso aziendale *software* non autorizzati dalla Società;
- utilizzare illecitamente materiale tutelato da altrui diritto d'autore.

CAPITOLO E.4

E.4.1 Standard di Controllo Specifici relativi alle Attività Sensibili

Al fine di presidiare le Attività Sensibili e limitare il rischio di commissione di reati contro la Pubblica Amministrazione la Società – anche adottando apposite procedure – rispetta nell'ambito delle Attività Strumentali i seguenti Standard di Controllo Specifici.

Per le attività relative all'**Assegnazione e utilizzo delle risorse ICT ad uso individuale da parte degli utenti interni ed esterni** si applicano i seguenti Standard di Controllo Specifici:

46) Assegnazione delle risorse informatiche e telematiche

a) criteri di assegnazione delle risorse e servizi informatici;

b) definizione di livelli autorizzativi per l'assegnazione delle risorse e servizi informatici.

Per le attività relative all'**Accesso ad un sistema informatico o telematico e/o sottostante infrastruttura di un soggetto terzo (anche finalizzato al trasferimento di denaro, di valore monetario o di valuta virtuale) o di Artsana e/o accesso e gestione informatica di documenti con valore probatorio da parte di utenti interni ed esterni** si applicano i seguenti Standard di Controllo Specifici:

47) Controllo degli accessi

Garantire un adeguato sistema di controllo sull'accesso alle informazioni, al sistema informatico, alla rete, agli applicativi ed alla relativa infrastruttura, attraverso:

a) l'individuazione di ruoli e responsabilità nella gestione delle modalità di

accesso degli utenti ivi inclusi i procedimenti di registrazione e de-registrazione delle utenze per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi;

b) l'assegnazione di privilegi specifici ai diversi utenti o categorie di utenti in base ad un processo autorizzativo interno;

c) la rivisitazione periodica dei diritti d'accesso degli utenti.

48) Configurazione dei parametri di sicurezza

Garantire un adeguato sistema di controllo sull'accesso alle informazioni, al sistema informatico, alla rete, agli applicativi ed alla relativa infrastruttura, attraverso:

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

b) la chiusura di sessioni inattive dopo un limitato periodo di tempo;

c) la sospensione delle utenze in seguito ad un numero predefinito di tentativi di accesso fallito.

49) Sicurezza fisica

Prevenire:

a) accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature con particolare attenzione ai locali dedicati ai centri di elaborazione dati gestiti direttamente;

b) danni e interferenze alle apparecchiature che garantiscono la connettività e le comunicazioni.

50) Controllo degli accessi su sistemi di terzi

Garantire che in caso di accesso a sistemi di terze parti, ogni responsabile di funzione debba periodicamente elencare il relativo privilegio di accesso da parte degli utenti della propria unità. Le modalità di verifica degli account dovranno seguire quanto previsto ai punti a), b) e c) dello Standard di

Controllo Specifico "Controllo degli accessi".

Per le attività relative all'**Installazione di software su hardware, postazioni di lavoro fisse o mobili, dispositivi di rete, comunicazione o di memorizzazione** si applicano i seguenti Standard di Controllo Specifici:

51) Sicurezza perimetrale

Garantire che la protezione del sistema informatico e telematico da software pericoloso (es. worm e virus) venga garantita da parte della Società, in base alla tipologia dell'apparato e alla catena tecnologica in esame, attraverso l'utilizzo di antivirus, il processo di patch management e la configurazione di firewall. Qualsiasi modifica alle configurazioni di sicurezza perimetrale (es. apertura di porte verso l'esterno) è sottoposta ad adeguati controlli autorizzativi.

49) Sicurezza fisica

Prevenire:

a) accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature con particolare attenzione ai locali dedicati ai centri di elaborazione dati gestiti direttamente;

b) danni e interferenze alle apparecchiature che garantiscono la connettività e le comunicazioni.

52) Audit e monitoraggio

Garantire che la Società assicuri lo svolgimento di attività di monitoraggio / verifica periodica dell'efficacia e operatività del sistema di gestione della sicurezza informatica di Artsana sia in ambito applicativo sia in ambito infrastrutturale, adottando le misure di verifica più consone alle diverse categorie tecnologiche, in modo da garantire adeguate barriere difensive e al contempo individuare possibili abusi sul traffico in uscita.

53) Gestione degli incidenti e dei problemi di sicurezza informatica

Garantire che il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica includa:

a) l'adozione di canali gestionali per la comunicazione degli Incidenti e Problemi (relativamente a tutta la catena tecnologica);

b) l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause (relativamente a tutta la catena tecnologica);

c) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva (relativamente a tutta la catena tecnologica);

d) la produzione e l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive (relativamente a tutta la catena tecnologica);

e) la manutenzione delle basi dati contenenti informazioni su errori e vulnerabilità di sicurezza noti non ancora risolti e i rispettivi workaround.

Per le **Attività di ricerca e sviluppo; Attività di ricerca e sviluppo dell'area Fashion** si applicano i seguenti Standard di Controllo Specifici:

9) Gestione delle attività di ricerca e sviluppo (ivi inclusi i marchi e i brevetti)

a) l'individuazione di ruoli e responsabilità nelle attività di definizione dell'esigenza e del disegno, nonché nella formalizzazione della specifica tecnica;

b) la definizione delle modalità operative connesse alla protezione dell'Intellectual Property (che comprenda, tra l'altro, la verifica della sussistenza dei requisiti di brevettabilità dell'Intellectual Property o di registrazione dei marchi);

c) la definizione di modalità operative connesse alla verifica del rispetto dei requisiti normativi (che comprenda, tra l'altro, la verifica di norme/regolamenti in relazione a ciascuno Stato nel quale si intende commercializzare il prodotto);

d) la previsione di uno specifico iter di redazione, verifica e autorizzazione della specifica tecnica.

Per le attività relative alla **Gestione dei marchi e brevetti industriali** si faccia riferimento – per quanto di competenza – agli standard di controllo descritti nella Parte Speciale A con riferimento all'Attività Sensibile in oggetto. Inoltre, si applicano

i seguenti Standard di Controllo Specifici:

56) Gestione dell'Intellectual Property e portafoglio marchi

a) la definizione di principi, attività, ruoli e responsabilità in relazione allo sviluppo, gestione, protezione e valorizzazione dell'Intellectual Property e del portafoglio marchi;

b) la definizione di modalità operative connesse alla protezione dell'Intellectual Property e del portafoglio marchi (che comprenda, tra l'altro, la verifica della sussistenza dei requisiti di brevettabilità dell'Intellectual Property o di registrazione dei marchi);

c) la definizione di modalità operative in merito alle attività di acquisto / cessione / concessione di licenze d'uso (in & out), nonché di acquisto e/o cessione di Intellectual Property e marchi.

Per le attività relative alla **Definizione e svolgimento di attività di pubblicità, promozione e marketing, Gestione dei contenuti del sito internet della Società e dei relativi social network, anche tramite soggetti terzi** si faccia riferimento – per quanto di competenza – agli standard di controllo descritti nella Parte Speciale H.

CAPITOLO E.5

I controlli dell'OdV

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e princìpi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei princìpi procedurali ivi previsti ovvero dei princìpi contenuti nelle *policy* aziendali adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

L'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai princìpi procedurali specifici contenuti nella presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.

È, altresì, attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti aziendali rilevanti per lo svolgimento dei propri compiti.

CAPITOLO E.6

Flussi informativi nei confronti dell'Organismo di Vigilanza

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nel separato documento di riepilogo dei flussi informativi adottato dalla Società.