Società Acqua Lodigiana srl

PARTE SPECIALE F

Delitti in violazione del Diritto d'autore

Approvato dal Consiglio di Amministrazione di SAL S.r.l. nella seduta del 30/11/2020

Revisione 1 del 30/11/2020

Il Presidente SAL
Giuseppe Negri

INDICE

Storico delle modifiche

Versione	Causale	Data
Prima Versione	Emissione	26/02/2014

Revisione corrente:

Versione	Causale	Data
Revisione 1	Aggiornamento periodico	30/11/2020

PARTE SPECIALE "F" – DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE

1. Le fattispecie dei delitti in violazione del diritto d'autore richiamate dal d.lgs. n. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. n. 231/2001 è collegato il regime di responsabilità a carico della Società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal Decreto.

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del d.lgs. n. 231/2001, riportiamo, qui di seguito, una breve descrizione dei reati richiamati dall'art. 25-novies del D.Lgs n. 231/2001[1].

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, l. 633/1941 comma 1 lett a) bis)

La norma incriminante punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma 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.

Reati previsti dall'art.171, comma 1 commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3)

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui all'art.171, comma 1 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.

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, c. 1, l. 633/1941)

La fattispecie di reato punisce chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a

---

[1] *Si riportano solo alcuni dei reati richiamati dall'art.25-novies in quanto gli altri fanno riferimento a società con business specifico (es. società che operano in ambito radio/ televisivo/cinematografico e società editrici di opere, ivi inclusi a titolo esemplificativo locali quali palestre, bar, librerie, videoteche e siti internet in cui si proiettano/diffondono materiali protetti; produttori o importatori dei supporti non soggetti al contrassegno SIAE, società che producono e commercializzazione apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato).*

scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE). anche 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.

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, c. 2, l. 633/1941)

La fattispecie di reato punisce 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.

2. Le "attività sensibili" ai fini del d.lgs n. 231/2001

L'art. 6, comma 2, lett. a) del d.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal d.lgs. n. 231/2001.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui al precedente punto 1, le attività "sensibili" di SAL S.r.l., di seguito elencate:

1) **Gestione dei sistemi informativi e della sicurezza informatica**: riguarda le attività di gestione dei profili utente e del processo di autenticazione, creazione, trattamento, archiviazione di documenti elettronici con valore probatorio, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno, gestione e protezione delle reti e degli output di sistema e dei dispositivi di memorizzazione, nonché della sicurezza fisica (cablaggi, dispositivi di rete, ecc.).

3. Il sistema dei controlli

Il sistema dei controlli, perfezionato dalla Società sulla base delle indicazioni fornite dalle principali associazioni di categoria, quali le Linee Guida Confindustria, nonché dalle "best practice" internazionali, prevede con riferimento alle attività sensibili e ai processi strumentali individuati:

- Principi generali degli standard di controllo relativi alle attività sensibili;

– Standard di controllo "specifici" applicati alle singole attività sensibili.

3.1 Principi generali degli standard di controllo relativi alle attività sensibili

Gli standard di controllo specifici sono fondati sui seguenti principi generali:

- **Procedure**: gli standard si fondano sull'esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: gli standard si fondano sul principio secondo cui: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.
- **Segregazione dei compiti**: gli standard si fondano sulla separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Procure e deleghe**: gli standard si fondano sul principio secondo il quale i poteri autorizzativi e di firma assegnati debbano essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese.

3.2 Standard di controllo specifici

Qui di seguito sono elencati gli standard di controllo specifici relativi alle singole attività sensibili individuate:

1) Gestione dei sistemi informativi e della sicurezza informatica

- *Procedure*: l'attività sensibile è regolata dalla procedura "Gestione dei sistemi informativi e della sicurezza informatica" che prevede la descrizione di ruoli, responsabilità, modalità operative e controlli per la gestione del processo in oggetto ed in particolare:
- *Tracciabilità*: la Procedura "Gestione dei sistemi informativi e della sicurezza informatica" prevede:
  - Modalità per l'utilizzo di software e ed altri sistemi informativi protetti da licenze;
  - l'archiviazione di tutta la documentazione rilevante ai fini della tracciabilità del processo in oggetto.
- *Segregazione dei compiti*: il processo risulta segregato in quanto le attività operative di gestione e controllo dei sistemi informativi e della sicurezza

informatica sono affidate al Responsabile Servizi Informatici; le attività di controllo e la sottoscrizione dei documenti sono di competenza del Direttore Generale sulla base dei poteri conferiti dal CdA.

- *Ruoli e Responsabilità*: i ruoli e le responsabilità delle diverse fasi del processo in oggetto sono definiti dalla Società all'interno dei seguenti documenti:
  - Procedura "Gestione dei sistemi informativi e della sicurezza informatica";
  - Organigramma aziendale;
  - Documento "Organizzazione Aziendale" circa la descrizione delle mansioni per Aree funzionali.

Per i controlli aggiuntivi associati all'attività sensibile in oggetto, si rimanda a quanto previsto all'interno della "Parte Speciale H – Reati Informatici".