Parte speciale O

REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

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

La "parte speciale O" è dedicata alla trattazione dei reati in materia di violazione del diritto di autore così come individuati nell'art. 24 *novies* d.lgs. n. 231 del 2001.
Di seguito viene riportato l'elenco delle fattispecie criminose prese in considerazione dalle suddette disposizioni, le modalità attraverso le quali queste fattispecie criminose possono essere compiute nonché le "macro aree" sensibili, i ruoli aziendali coinvolti e i "protocolli di prevenzione" attuati all'interno della Società. Infine, vengono riportati anche i c.d. "processi strumentali" e i compiti generali dell'OdV.

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

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

Art. 171-*bis*

Testo della norma

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582,00 a euro 15.493,00. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La 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.

Autore del reato

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

Descrizione

La norma in questione contempla due distinte ipotesi delittuose.
La fattispecie prevista dal comma 1 consiste nella duplicazione dei programmi per elaboratore o nella distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, o concessione in locazione dei programmi contenuti in supporti sprovvisti del contrassegno SIAE.
Nel caso della duplicazione, la condotta deve essere abusiva, cioè posta in essere in violazione delle norme che regolamentano la medesima attività.
Le altre condotte attengono alla commercializzazione di programmi contenuti in supporti privi del contrassegno SIAE.
L'ipotesi di cui al comma 2, invece, prende in considerazione il contenuto di una banca-dati. La condotta può consistere nella riproduzione su supporti non contrassegnati dalla SIAE, nel trasferimento su altro supporto, nella distribuzione, nella comunicazione, nella presentazione o dimostrazione in pubblico del contenuto di una banca-dati, in violazione di quanto previsto dagli artt. 64-*quinquies* e 64-*sexies*.
In alternativa, sono incriminate le condotte di estrazione e reimpiego della banca-dati, in violazione delle disposizioni di cui agli artt. 102-*bis* e 102-*ter*.
Infine, sono punite le condotte di distribuzione, vendita e concessione in locazione di una banca-dati.
Comune a tutte le condotte è il fine di trarne profitto. L'elemento soggettivo è quindi il dolo specifico.
In relazione ai reati previsti dall'articolo in questione è prevista, a norma dell'art. 171 *sexies*, comma 2, la confisca dei supporti fonografici, audiovisivi, ecc. già duplicati, nonché degli strumenti e dei materiali non ancora utilizzati per commettere i reati stessi, ma destinati a commetterli.

Esemplificazioni

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

- La Società, al fine di trarne profitto, su supporti non contrassegnati SIAE, riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies.
- La Società esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter.
- La Società distribuisce, vende o concede in locazione una banca di dati.

1 Le "attività sensibili" in relazione ai reati in materia di violazionedel diritto di autore (art. 25-*novies*, D. Lgs. 231/01): elencazione.

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

- Gestione delle attività di accesso ai sistemi informatici e telematici e loro applicazioni (autenticazione, account e profili)
- Gestione degli accessi fisici agli strumenti informatici.

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

In occasione dell'implementazione dell'attività di *risk mapping*, sono state individuate, nell'ambito della struttura organizzativa ed aziendale di Palma Boria STA, delle "macro aree" di attività sensibili, ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati di cui al punto n. 1. Nell'elaborazione, queste "macro aree" – fortemente caratterizzate – sono state tuttavia immediatamente calate all'interno delle fattispecie di reato esaminate. Sono stati inoltre identificati i ruoli aziendali coinvolti nell'esecuzione di tali attività e che, astrattamente, potrebbero commettere i reati qui considerati.
Nell'espletamento delle rispettive attività/funzioni, oltre alle regole stabilite nel Modello di organizzazione,

gestione e controllo (di seguito "Modello"), i soggetti aziendali coinvolti nella gestione delle "macro aree" di attività sensibili individuate in relazione ai reati in materia di violazione del diritto di autore di cui all'art. 25-*novies* del Decreto sono tenuti, al fine di prevenire e impedire il verificarsi dei reati qui considerati, al rispetto di una serie di "Protocolli preventivi": tali protocolli possono essere "PROTOCOLLI PREVENTIVI", "PROTOCOLLI PREVENTIVI DI SISTEMA" o "PROTOCOLLI PREVENTIVI SPECIFICI", a seconda che riguardino, i primi, i principi a cui si devono ispirare le procedure aziendali, i secondi, ad esempio, l'organizzazione della Società o la formazione del personale, e i terzi, la previsione di procedure aziendali specifiche.
Di seguito è riepilogato il quadro in precedenza esposto.

GESTIONE DELLE ATTIVITÀ DI ACCESSO AI SISTEMI INFORMATICI E TELEMATICI E LORO APPLICAZIONI (AUTENTICAZIONE, ACCOUNT E PROFILI)

GESTIONE DEGLI ACCESSI FISICI AGLI STRUMENTI INFORMATICI

Con riferimento ad i controlli preventivi relativi a tale area, si rimanda a quanto previsto nella "Parte Speciale J - reati in tema di criminalità informatica e di trattamento illecito di dati".

3 I compiti dell'Organismo di Vigilanza

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'OdV nel documento approvato dal Consiglio di Amministrazione e denominato "Parte speciale B - struttura, composizione, regolamento e funzionamento dell'Organismo di Vigilanza", in relazione alla prevenzione dei reati di cui alla presente Parte speciale, l'OdV, tra l'altro, deve:

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