

**COET S.r.l.**

Via Civesio 12 - 20097 San Donato Milanese (MI)

# Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. n. 231/2001

## PARTE SPECIALE

### Delitti informatici e reati in materia di violazione del diritto d'autore (art. 24-bis e 25-novies D.Lgs. 231/2001)

**Emissione:**

Data 19.12.2025

Firma

**Approvazione:**

Data 19.12.2025

Firma

**Stato delle revisioni**

N. Versione

Data approvazione

Descrizione

01

Prima emissione

## 1. DELITTI INFORMATICI E REATI IN MATERIA DI DIRITTO D'AUTORE (ART. 24-BIS E 24-NOVIES D.LGS. N. 231/2001)

### 11.2. Introduzione e funzione della presente Parte Speciale

La presente Parte Speciale si riferisce sia ai delitti informatici richiamati dall'art. 24-bis del D.Lgs. n. 231/2001 (di seguito anche "Decreto"), sia ai reati in materia di violazione del diritto d'autore richiamati dall'art. 24-novies del Decreto, in considerazione dell'affinità delle rispettive aree considerate "a rischio-reato", nonché dei processi dell'azienda rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei suddetti reati.

La presente Parte Speciale riporta le fattispecie di reato sopra indicati ed individua le cosiddette attività a rischio-reato (ossia quelle nel cui ambito potrebbero teoricamente essere realizzate le fattispecie di reato qui in esame), specificando i principi comportamentali ed i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle predette attività.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- definire i principi generali di comportamento e di controllo ai quali tutti i Destinatari del Modello devono conformarsi al fine di prevenire la commissione dei reati ai quali riferisce la presente Parte Speciale;
- assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Il Consiglio di Amministrazione, nel definire tale documento, a ulteriore conferma della volontà aziendale di operare secondo principi etici così come già contemplati nel proprio Codice Etico, intende sensibilizzare tutto il personale a mantenere comportamenti corretti e idonei a prevenire la commissione di reati.

### 1.2 Le fattispecie di reato richiamate dagli artt. 24-bis e 24-novies del D.Lgs. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti apicali o sottoposti della Società è collegato il regime di responsabilità del D.Lgs. 231/2001, 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, si riporta, qui di seguito, una descrizione dei reati richiamati dagli artt. 24-bis e 24-novies del Decreto.

#### Le fattispecie di reato richiamati dall'art. 24-bis del D.Lgs. 231/2001

Le tipologie di reato informatico si riferiscono a una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e, in altri, lo strumento attraverso cui l'autore intende realizzare altra fattispecie penalmente rilevante.

#### ➤ **Falsità in un documento informatici (articolo 491-bis c.p.)**

L'art. 491-bis c.p. dispone che la disciplina relativa ai reati in tema di falso in atto pubblico previsti dal

Capo II del Titolo VII del Libro II del codice penale ("della falsità in atti": art. 476 c.p. e ss.), commessi con riguardo ai tradizionali documenti cartacei, si estende ai documenti informatici pubblici aventi efficacia probatoria.

In particolare, come per gli atti, le condotte di reato potranno configurarsi come "falsità ideologica" (quando nell'atto – documento sono contenute attestazioni o dichiarazioni non veritiere) o come "falsità materiale" (quando esiste una divergenza tra autore apparente ed autore reale del documento o quando il documento sia stato alterato dopo la sua formazione).

I principali delitti ipotizzabili sono: la falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.) o in certificati o autorizzazioni amministrative (art. 477 c.p.), la falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.) o in certificati o autorizzazioni amministrative (art. 480 c.p.), la falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.), la falsità in registri e notificazioni (art. 484 c.p.), la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, lett. p, D.lgs. 82/2005).

A titolo esemplificativo, si pensi alla falsificazione di documenti informatici da parte di enti che procedono a rendicontazione elettronica di attività, ovvero alla falsificazione di documenti informatici contenenti gli importi dovuti dall'ente alla PA nel caso di flussi informatizzati dei pagamenti tra privati e PA (es. riduzione degli importi) o alterazione dei documenti in transito nell'ambito del SIP A (Sistema Informatizzato pagamenti della PA) al fine di aumentare gli importi dovuti dalla PA all'ente. Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

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

L'art. 615-ter è posto a tutela della riservatezza delle comunicazioni ed informazioni e sanziona la condotta di chi, abusivamente, si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto ad escluderlo.

Ai fini della punibilità non rileva la rivelazione dell'informazione indebitamente captata o il danneggiamento del sistema informatico.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente.

➤ ***Detenzione e diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)***

Il reato in esame sanziona la condotta di chi, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Ai fini dell'integrazione della fattispecie di reato è richiesto il dolo specifico dell'agente, caratterizzato dal perseguimento del fine di profitto per sé o altri o di arrecare danno ad altri.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-quater, pertanto, sono punite 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 (ad esempio, badge, carte di credito, bancomat e smart card).

Si pensi, ad esempio, alla detenzione e utilizzo di *password* di accesso a siti di enti concorrenti al fine di acquisire informazioni riservate; ovvero alla detenzione ed utilizzo di *password* di accesso alle caselle e-mail dei dipendenti, allo scopo di controllare le attività svolte nell'interesse dell'azienda anche in violazione della legge sulla privacy o dello statuto dei lavoratori.

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

Tale reato, si realizza qualora 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".

Questo delitto è integrato, ad esempio, nel caso in cui il soggetto si procuri un virus, idoneo a danneggiare un sistema informatico o qualora si producano o si utilizzino delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi elettronici.

Questi fatti sono punibili solo nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento. Si tratta di fattispecie che potrebbero verificarsi nell'ipotesi in cui un dipendente della Società effettui attacchi di *cracking*, *hacking*, *spoofing* per alterare i dati relativi, a titolo di esempio, a dossier, autorizzazioni etc.

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

Tale reato, si integra qualora un soggetto “fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni”, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione. L'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente effettui un attacco informatico di *sniffing* mediante l'utilizzo di sistemi atti a intercettare comunicazioni informatiche/telematiche di enti concorrenti nella partecipazione a gare di appalto per conoscere l'entità dell'offerta del concorrente, ovvero atti a impedire o interrompere comunicazioni onde impedire che un ente concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.

➤ ***Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)***

Il reato in esame sanziona la detenzione, diffusione o installazione di dispositivi tecnologici volti a intercettare le comunicazioni telefoniche o informatiche.

➤ ***Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)***

La fattispecie reato si realizza quando un soggetto “distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui”. La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia o se commesso abusando della qualità di operatore del sistema.

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

➤ ***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.)***

L'art. 635-ter sanziona chiunque commetta un fatto diretto a distruggere, deteriorare, cancellare,

alterare, sopprimere informazioni, dati o programmi utilizzati dallo Stato o da un ente pubblico o di pubblica utilità.

La fattispecie di reato è strutturata come delitto aggravato dall'evento, poiché è punito il compimento di atti diretti a cagionare quanto previsto dalla norma e se il danneggiamento si realizza si applica una pena più grave.

È sufficiente il dolo generico, ovvero si prescinde dalle finalità avute di mira dal reo, essendo sufficiente la coscienza e volontà della condotta e dell'altruità dei dati.

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Il reato in esame potrebbe, ad esempio, essere commesso nell'interesse della Società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della Società.

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

Il reato si realizza quando un soggetto "mediante le condotte di cui art 635-bis c.p. (danneggiamento di dati, informazioni e programmi informatici), 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". La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Si tenga conto 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 danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus).

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

Questo reato si configura quando "il fatto di cui all'art. 635-quater (Danneggiamento di sistemi informatici o telematici) 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 sanzione è aumentata se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, diversamente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-ter), 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 del sistema stesso.

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



Questo reato si configura quando "il soggetto che presta servizi di certificazione di firma elettronica, 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".

Questo reato è dunque un reato c.d. proprio in quanto può essere commesso solo da parte dei certificatori qualificati, o meglio, i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

➤ **Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11 D.L. 105/2019 convertito con modificazioni dalla L. 133/2019)**

Il reato punisce "chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6, lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

\*\*\*\*

Le fattispecie di reato di cui agli artt. 640-*quinquies* c.p. e di cui all'art. 1, comma 1 D.L. 105/2019, richiamate dall'art. 24-*bis* del Decreto, non si ritengono applicabili alla Società in considerazione dell'attività dalla stessa svolta.

**Le fattispecie di reato richiamate dall'art. 25-novies del D.Lgs. 231/2001**

L'art. 25-novies del DLgs, 231/2001 individua, quali ipotesi di reato idonee ad originare la responsabilità amministrativa dell'ente una molteplicità di violazioni della legge 633/41 relative alla protezione del diritto d'autore (d'ora in poi LDA), rappresentate essenzialmente dall'abusiva utilizzazione di opere o parti di opere tutelate dal diritto d'autore o di materiali protetti dagli altri diritti connessi al suo esercizio.

Si evidenzia che per alcuni generi di opere (ed in particolare per le opere musicali o cinematografiche e per i relativi supporti) vi sono altre ipotesi di reato (art. 473 c.p. "contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni" e art. 474 c.p. "introduzione nello Stato e commercio di prodotti con segni falsi"), di cui si è già trattato nella Parte Speciale relativa ai reati contro l'industria e il commercio e delitti in materia di proprietà industriale.

Prima di procedere all'analisi delle singole fattispecie penali poste a tutela del diritto d'autore, si precisa che tutte le ipotesi delittuose previste dalla LDA sono punite a titolo di dolo: ciò significa che, per dare luogo a responsabilità penale, i diversi comportamenti descritti dal legislatore dovranno essere realizzati prevedendo e volendo la violazione del diritto d'autore.

Pertanto, premessa indispensabile per la realizzazione della condotta penalmente rilevante è la consapevolezza, da parte del soggetto agente di non essere titolare del diritto.

A ciò si aggiunga sin d'ora che, nelle diverse fattispecie di reato previste dalla LDA, in alcuni casi il dolo viene declinato come dolo generico (ad esempio, nell'art. 17, comma 1, lett. a-bis, la condotta

assume rilevanza se posta in essere “a qualsiasi scopo”), in altri come dolo specifico (ad esempio nell’art. 171-ter LDA, le condotte descritte assumono rilevanza penale solo se connotate dal fine specifico di lucro).

Si evidenzia, altresì, che dal 15 novembre 2024, è venuto a cessare l’obbligo di apporre il contrassegno antipirateria o “bollino SIAE” su supporti da distribuire in Italia, contenenti suoni o immagini in movimento riproducenti opere soggette a tutela di diritto d’autore (musicali, liriche, teatrali, cinematografiche, letterarie, ecc.), per effetto di una modifica legislativa intervenuta sull’art. 181-bis della Legge n. 633/41. Resta però obbligatorio richiedere licenza a SIAE (Società italiana degli autori e editori) per i diritti d’autore e facoltativo richiedere i contrassegni a SIAE o ad altri organismi di gestione collettiva o entità di gestione indipendenti per le consuete finalità di anticontraffazione.

➤ ***Abusiva messa a disposizione del pubblico di un’opera dell’ingegno o di parte di essa (art. 171, comma 1 lett. a-bis e comma 3 LDA)***

Il reato punisce, salvo quanto disposto dall’art. 171-bis e 171-ter, 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.

La norma, sotto il profilo dell’elemento soggettivo, è quindi connotata dal dolo generico (“a qualsiasi scopo”).

La fattispecie incriminatrice in esame è stata introdotta dall’art. 3 del 7/2005, allo scopo di reprimere la duplicazione e diffusione abusiva di opere dell’ingegno attraverso la tecnica del c.d. *peer to peer*. La norma configura di fatto una tutela penale anticipata; infatti, il reato si realizza una volta che l’opera sia stata messa a disposizione del pubblico indipendentemente dal fatto che un altro utente della rete proceda poi allo scaricamento nel suo computer.

Il reato è aggravato, ai sensi del comma 3 della disposizione in esame, nel caso in cui sia commesso in violazione anche dei c.d. “diritti morali d’autore” e precisamente: sopra un’opera altrui non destinata alla pubblicazione (una simile previsione è posta a tutela degli inediti); con usurpazione della paternità dell’opera: la norma fa riferimento al cosiddetto plagio, che ricorre quando l’opera viene presentata con una paternità non rispondente al vero; con deformazione, mutilazione o altra modificazione dell’opera, se queste determinano un’offesa all’onore o alla reputazione dell’autore.

➤ ***Abusiva utilizzazione a scopo di profitto di programmi per elaboratore (di seguito anche software (art. 171-bis LDA)***

L’art. 171-bis, comma 1 punisce 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 ai sensi della legge (LDA).

Tale norma, dunque, sanziona un complesso di attività illecite poste in essere su un software, e in particolare: la duplicazione abusiva di software al fine di trarne profitto; l’importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di software contenuti su supporti non contrassegnati ai sensi della legge LDA, al fine di trarne profitto.



La LDA individua poi le condizioni per la protezione del software, riconoscendo in particolare, all'art. 2 n. 8 la tutelabilità dei *“programmi per elaboratore, in qualsiasi forma espressi, purché originali, quale risultato di creazione intellettuale dell'autore”*, ed escludendo *“le idee e i principi che stanno alla base di qualsiasi elemento di un programma”*.

Il reato in questione è connotato dal dolo specifico, in quanto prevede espressamente che le condotte siano poste in essere per scopo di profitto o - nel solo caso della detenzione - per scopo commerciale o imprenditoriale.

La giurisprudenza penalistica, tende ad attribuire al fine di profitto una portata ben più ampia di quella dello scopo di lucro, tale da ricomprendere addirittura lo scopo di conseguire qualsiasi utilità o vantaggio, anche di tipo non direttamente patrimoniale. Ne consegue che il reato in esame è integrato anche in caso di duplicazione e di utilizzo del software senza licenza d'uso regolarmente acquistata, a prescindere da una sua eventuale successiva commercializzazione: il risparmio di spesa che deriva da tali attività, infatti, se non integra il fine di lucro, integra con ogni probabilità lo scopo di profitto.

È riconducibile a questa fattispecie penale anche il comportamento del legittimo utilizzatore del software il quale, pur essendo in possesso di un'unica licenza, duplichi il programma al fine di utilizzarlo su diversi terminali di sua proprietà.

Maggiori dubbi sorgono invece in ordine all'ipotesi della condivisione, fra più terminali connessi in rete e riferibili allo stesso soggetto, di un software per il quale sia stata acquisita una licenza singola. La soluzione che, tuttavia, appare maggiormente equilibrata è quella di non ritenere configurabile l'illecito penale in questione poiché l'estensione della tutela penale a tale ipotesi si fonderebbe su un'applicazione analogica della norma penale in senso meno favorevole al reo, vietata ai sensi dell'art. 14 delle disposizioni sulla legge in generale.

La norma in esame fa riferimento a condotte poste in essere su supporti non contrassegnati ai sensi della legge LDA.

Ai sensi dell'articolo 181-bis (così come modificato dall'articolo 15, comma 3-ter, lettera e), numero 1), del D.L. 16 settembre 2024, n. 131, convertito con modificazioni dalla Legge 14 novembre 2024, n. 166) e agli effetti di cui agli articoli 171-bis e 171-ter, la Società italiana degli autori ed editori (SIAE), gli altri organismi di gestione collettiva e le entità di gestione indipendenti possono apporre, su richiesta degli interessati, un contrassegno su ogni supporto contenente programmi per elaboratore o multimediali nonché su ogni supporto contenente suoni, voci o immagini in movimento, che reca la fissazione di opere o di parti di opere tra quelle indicate nell'articolo 1, primo comma, destinati ad essere posti comunque in commercio o ceduti in uso a qualunque titolo a fine di lucro. Analogo sistema tecnico per il controllo delle riproduzioni di cui all'articolo 68 potrà essere adottato con decreto del Presidente del Consiglio dei ministri, sulla base di accordi tra la SIAE, gli altri organismi di gestione collettiva o le entità di gestione indipendenti e le associazioni delle categorie interessate.

L'apposizione del contrassegno sui predetti supporti avviene previa attestazione da parte del richiedente circa l'assolvimento degli obblighi derivanti dalla normativa sui diritti d'autore e sui diritti connessi.

Anche per quanto concerne le attività di importazione, distribuzione e vendita di programmi contenuti in supporti non contrassegnati, di cui alla seconda parte della disposizione in esame, il Legislatore ha modificato l'originale dolo specifico, trasformandolo da fine di lucro in fine di profitto.

Per la diversa ipotesi di detenzione è invece ora previsto che essa debba essere caratterizzata da uno scopo commerciale o imprenditoriale. Vi è quindi la volontà del Legislatore di punire espressamente la detenzione del programma abusivo non solo al fine di farne commercio a terzi, ma anche allo scopo di utilizzarlo nell'ambito dell'attività della propria azienda.

L'ultima parte del primo comma dell'art. 171-bis punisce le condotte di commercializzazione (e quindi (l'importazione, la distribuzione, da vendita, da detenzione a scopo commerciale o imprenditoriale, la concessione in locazione) di mezzi atti a rimuovere arbitrariamente o ad eludere dispositivi di protezione dei software. In tale categoria possono ad esempio ricomprendersi i c.d. *cracks* (programmi "sprotettori") i *key-generators* (applicazioni in grado di generare codici per lo sblocco di software protetti), come anche le chiavi *hardware* (realizzate per sostituire quelle originali) o altri strumenti simili.

L'art. 171-bis comma 2 punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati 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.

Vengono pertanto sanzionate una serie di condotte relative alle banche dati, contraddistinte tutte dallo scopo di profitto e consistenti nella: abusiva riproduzione, su supporti non contrassegnati, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca dati, in violazione degli artt. 64 *quinquies* e 64 *sexies*; abusiva estrazione o reimpiego della banca dati in violazione degli artt. 102 *bis* e 102 *ter*; abusiva distribuzione, vendita o concessione in locazione di una banca dati.

Gli elementi caratterizzanti le banche dati sono individuabili sulla scorta della definizione contenuta nell'art. 2 n. 9 LDA: nella raccolta di una pluralità di dati indipendenti tra loro; Nella disposizione sistematica o metodica di tali dati; nell'individuale accessibilità degli stessi.

Condizione necessaria per l'applicazione ad una banca dati della tutela del diritto d'autore è la sua qualificazione come opera d'ingegno, in quanto in essa sia rintracciabile il c.d. "carattere creativo", inteso come espressione della personalità dell'autore.

Qualora invece la banca dati non possa ritenersi creativa. la stessa sarà oggetto dei soli diritti connessi, nella particolare accezione del diritto "*sui generis*" di cui agli artt. 102 *bis* e 102 *ter* LDA.

A tale proposito, la prima delle citate disposizioni disciplina i diritti del costituente della banca dati non creativa, ovvero di colui che abbia effettuato investimenti rilevanti per la sua costituzione. In particolare, questi ha la facoltà per la durata di anni decorrenti dal 1 gennaio dell'anno successivo alla data di completamento della banca dati, di vietare l'estrazione o il reimpiego della sua totalità o di una parte sostanziale di essa ovvero anche l'estrazione o il reimpiego di sue parti non sostanziali, che siano tuttavia ripetuti e sistematici e presuppongano quindi operazioni contrarie alla normale gestione della banca dati.

L'art. 102 *ter*, invece, nel disciplinare le facoltà dell'utente legittimo della banca dati non creativa, stabilisce in primo luogo che questi non può in alcun modo recare pregiudizio ai diritti del suo autore o del suo costituente, né eseguire operazioni che siano in contrasto con la normale gestione della banca dati. Sono comunque consentiti all'utente legittimo, senza il necessario consenso del

costitutore, l'estrazione o il reimpiego di parti non sostanziali, valutate in termini qualitativi e quantitativi del contenuto della banca di dati, per qualsivoglia fine effettuate.

➤ ***Abusiva utilizzazione, per uso non personale e ai fini di lucro, di varie tipologie di opere protette dal diritto d'autore e dai diritti connessi (art. 171-ter LDA)***

L'art. 171-ter, comma 1, LDA accorpa al proprio interno una serie di condotte diverse, attuate in violazione del diritto d'autore e dei diritti connessi, che possono essere riepilogate come di seguito:

– Lettera a)

abusiva - per fini di lucro e per uso non personale - integrale o parziale duplicazione, riproduzione, trasmissione o diffusione, con qualsiasi procedimento: di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio di 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.

– Lettera b)

abusiva - per fini di lucro e per uso non personale - integrale o parziale duplicazione, riproduzione, trasmissione o diffusione, con qualsiasi procedimento, di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati.

– Lettera c)

per fine di lucro e per uso non personale, introduzione nel territorio dello Stato, detenzione per la vendita o distribuzione, commercio, noleggio o cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo della radio o televisione con qualsiasi procedimento, trasmissione in pubblico delle duplicazioni o delle riproduzioni abusive di cui alle lettere a) e b).

– Lettera d)

compimento delle attività di cui alla lettera precedente su supporti per i quali è prescritta l'apposizione di contrassegno ai sensi della LDA, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato.

– Lettera e)

in assenza di accordo con il legittimo distributore, ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

– Lettera f)

introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, vendita, concessione in noleggio, cessione a qualsiasi titolo, promozione commerciale installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

– Lettera f bis)

fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per la vendita o il noleggio, o detenzione per scopi commerciali di attrezzature, prodotti o componenti ovvero prestazione di servizi che abbiano la prevalente finalità o l'uso commerciale di 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.

– Lettera h)

abusiva rimozione o alterazione delle informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, comunicazione o messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

– Lettera h-bis)

,esecuzione della fissazione su supporto digitale, audio, video o audiovisivo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettuazione della riproduzione, esecuzione o comunicazione al pubblico della fissazione abusivamente eseguita.

➤ ***Mancata comunicazione alla SIAE dei dati di identificazione dei supporti (art. 171-septies LDA)***

L'art. 171-septies punisce: b) salvo che il fatto non costituisca più grave reato, chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

➤ ***Fraudolenta produzione o importazione di apparati di decodifica (art. 171-octies LDA)***

Il reato punisce, qualora il fatto non costituisca più grave reato, 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.

\*\*\*

Appare remoto nel contesto di Coet il rischio di commissione delle fattispecie di reato richiamate dall'art. 24-novies del D.Lgs. 231/2001 e indicate nell'art. 171-ter lettere da e) ad h).

## **2 Identificazione delle attività a rischio-reato**

Ai fini della presente Parte Speciale, la Società, ha provveduto a svolgere un'analisi dei processi aziendali, che ha consentito di individuare le attività nel cui ambito potrebbero astrattamente essere realizzate fattispecie di reato richiamate dagli artt. 24-bis e 25-novies del Decreto.

Qui di seguito sono elencate le c.d. attività sensibili o a rischio-reato:

- **Gestione della sicurezza informatica di software protetti;**
- **Acquisto ed utilizzo di programmi ed opere dell'ingegno protette dal diritto d'autore;**
- **Gestione del sito internet aziendale e del materiale informativo.**

Eventuali integrazioni delle suddette aree a rischio reato potranno essere proposte al Consiglio di Amministrazione dall'Organismo di Vigilanza e dagli altri organi di controllo della società per effetto dell'evoluzione dell'attività di impresa e conseguentemente di eventuali modifiche dell'attività svolta dalle singole funzioni aziendali.

## 2.1 Principi di comportamento e di controllo

Il sistema di controlli applicabili alle attività individuate è stato definito sulla base degli spunti forniti dalla normativa e dalle indicazioni contenute nelle Linee Guida di Confindustria nonché dalle *best practice* internazionali.

Si individuano qui di seguito i principi che informano le specifiche procedure interne dell'azienda previste in relazione a qualsiasi operazione/attività che coinvolga un ente della Pubblica Amministrazione, nonché le regole di condotta elaborate dalla società in relazione a tale ambito di applicazione.

È fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato richiamate dagli artt. 24-bis e 24-novies del Decreto.

Sono altresì proibite la violazione dei principi e delle regole previste dal Codice etico e di condotta aziendale del gruppo Hitachi e delle Procedure Operative attinenti all'area specifica di competenza.

Relativamente all'attività a rischio-reato **“Gestione della sicurezza informatica ed installazione di software protetti”**.

Nell'ambito dello svolgimento delle normali attività della Società potrebbero in ipotesi configurarsi i reati informatici sopra indicati e, più in particolare, quelli inerenti all'alterazione di documenti aventi efficacia probatoria, alla gestione degli accessi ai sistemi informativi interni di concorrenti terzi e alla diffusione di virus o programmi illeciti.

La rete informatica è gestita attraverso l'ausilio di servizi erogati da fornitori esterni qualificati, che definiscono, insieme alla Società, tutte le politiche in materia di sicurezza informatica, attribuendo altresì gli accessi al sistema.

Ai destinatari che, per ragioni del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione dei sistemi informativi aziendali è fatto obbligo di:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- utilizzare esclusivamente i software, le applicazioni, i files e le apparecchiature informatiche fornite dall'azienda e farlo esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- aggiornare le password secondo la periodicità richiesta;
- garantire la tracciabilità dei documenti prodotti attraverso l'archiviazione delle varie versioni dei documenti o comunque garantire meccanismi di tracciabilità delle modifiche;
- assicurare meccanismi di protezione dei file quali le password e la conversione dei documenti in formato non modificabile;
- rispettare le procedure adottate dalla Società a tutela del sistema.

Nell'ambito di tali attività è fatto divieto di:

- violare o accedere illegalmente a un sistema informatico ovvero a un domicilio informatico;
- violare la riservatezza degli utenti che utilizzano tecnologie informatiche;
- violare norme di sicurezza con l'intenzione di ottenere illegalmente informazioni all'interno di un computer o di altro sistema informatico;
- danneggiare, cancellare, modificare o sopprimere, senza autorizzazione, dati informatici;
- impedire, interdire o bloccare senza autorizzazione il funzionamento di un sistema informatico;
- acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società;
- divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali;
- comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- porre in essere, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse della Società, comportamenti di qualsivoglia natura atti a ledere diritti di proprietà intellettuale altrui;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita o comunque mettere in circolazione, al fine di trarne profitto, beni/opere realizzati usurpando il diritto d'autore o brevetti di terzi;
- installare sui sistemi informativi aziendali programmi per elaboratore non assistiti da valida licenza d'utilizzo;
- installare sui sistemi informatici aziendali software (c.d. P2P, files sharing o instant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di files, quali filmati, documenti, canzoni, opere letterarie;



- scaricare sui personal computer aziendali programmi prelevati da internet o da sistemi per to peer, anche qualora trattasi di software gratuiti (freeware) o shareware, salvo espressa autorizzazione del Responsabile della Sicurezza dei Sistemi Informativi;
- installare sui personal computer aziendali apparati di comunicazione propri (ad esempio modem);
- ascoltare sui personal computer aziendali files audio o musicali, nonché visionare video e/o immagini, su qualsiasi supporto essi siano memorizzati, se non a fini prettamente lavorativi;
- diffondere, tramite reti telematiche, un'opera dell'ingegno o parte di essa;
- duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale, o comunque per trarne profitto, programmi per elaboratori, banche dati, opere a contenuto letterario, musicale, multimediale, cinematografico, artistico per i quali non siano stati assolti gli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi al suo esercizio.

Ai fini dell'attuazione dei principi, regole generali e dei divieti elencati nel paragrafo precedente, devono rispettarsi i principi di controllo qui di seguito descritti:

- i server devono essere collocati in locali dedicati e messi in sicurezza;
- il personale IT deve essere dotato delle utenze con poteri per operare sul sistema IT ( per cui devono esser previste specifiche autorizzazioni);
- gli accessi ed i log delle utenze con poteri di amministratori di sistema devono essere tracciati;
- per l'attivazione di ogni nuova utenza deve essere necessaria una richiesta formale, effettuata dalla Funzione Risorse Umane;
- ai dipendenti prima della consegna delle credenziali di accesso nominative, deve essere consegnata la policy aziendale adottata per la sicurezza, i diritti e le restrizioni del sistema informativo;
- i diritti associati ad ogni tipo di utenza, nonché le restrizioni, devono essere personalizzate sulla base della risorsa a cui si riferiscono;
- in caso di licenziamento o di dimissioni, la Funzione Risorse Umane deve formalizzare la richiesta di cancellazione dell'utenza utilizzando appositi canali telematici;
- periodicamente, la Funzione IT deve effettuare dei controlli sia sui devices per il controllo dei programmi installati e delle relative licenze detenute, sia sulle utenze non più utilizzate;
- il sistema informativo deve essere protetto da firewall e da software antivirus/antispam, periodicamente aggiornati;
- la funzione IT gestisce in coordinamento con gli Amministratori di Sistema, il file server con le funzioni di backup;
- deve essere impedito - anche eventualmente inibendo la funzionalità delle porte usb e delle unità CD ROM dei terminali - agli utenti differenti dagli amministratori di sistema di installare software o applicazioni, con la sola esclusione dei soggetti espressamente individuati dalla funzione aziendale competente per ragioni inerenti all'attività lavorativa svolta;
- le licenze dei sistemi informativi e degli applicativi diffusi installati sugli elaboratori devono essere gestiti dalla Funzione IT;
- le richieste di aggiornamento, modifica o installazione di nuovi applicativi negli elaboratori devono essere autorizzati esclusivamente dalla Funzione IT.

Relativamente all'attività a rischio-reato **“Acquisto ed utilizzo di programmi ed opere dell'ingegno protette dal diritto d'autore”**.

Ai destinatari che, per ragioni del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione dei sistemi informativi aziendali è fatto obbligo di osservare quanto previsto nella presente Parte Speciale. Inoltre è fatto obbligo di:

- verificare costantemente l'assenza sui dispositivi aziendali di cui si è in possesso di software non autorizzati e contenuti in una black list aggiornata dalla Funzione IT;
- mettere a disposizione i dispositivi aziendali di cui si è in possesso al fine di consentire eventuali controlli da parte di soggetti a ciò autorizzati.

Nell'ambito delle citate attività è fatto divieto di:

- porre in essere, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse della Società, comportamenti di qualsivoglia natura atti a ledere diritti di proprietà intellettuale altrui;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita o comunque mettere in circolazione, al fine di trarne profitto, beni/opere realizzati usurpando il diritto d'autore o brevetti di terzi;
- installare sui sistemi informativi aziendali programmi per elaboratore non assistiti da valida licenza d'utilizzo;
- installare sui sistemi informatici aziendali software (c.d. P2P, files sharing o instant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di files, quali filmati, documenti, canzoni, opere letterarie;
- scaricare sui personal computer aziendali programmi prelevati da internet o da sistemi peer to peer, anche qualora trattasi di software gratuiti (freeware) o shareware, salvo espressa autorizzazione della Funzione IT;
- installare sui personal computer aziendali apparati di comunicazione propri (ad esempio modem);
- ascoltare sui personal computer aziendali files audio o musicali, nonché visionare video e/o immagini, su qualsiasi supporto essi siano memorizzati, se non a fini prettamente lavorativi;
- duplicare, importare distribuire vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale, o comunque per trarne profitto, programmi per elaboratori, banche dati, opere a contenuto letterario, musicale, multimediale, cinematografico, artistico per i quali non siano stati assolti gli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi al suo esercizio.

Ai fini dell'attuazione dei principi, regole generali e dei divieti elencati nel paragrafo precedente, devono rispettarsi i principi di controllo qui di seguito descritti:

- deve essere effettuata una analisi da parte dell'amministratore di sistema e della Funzione IT dei contratti di licenza stipulati dalla Società e una verifica della corrispondenza del numero di copie concesse in licenza di uno specifico software con il numero di copie effettivamente installato sui computers presenti in azienda;

- l'acquisto di licenze software deve essere effettuato presso una fonte (rivenditore o altro) certificata ed in grado di fornire garanzie in merito alla originalità/autenticità del software;
- deve essere verificata l'esistenza di certificato di autenticità (o di documentazione equipollente) in relazione ai prodotti preinstallati;
- deve essere verificata l'originalità, anche tramite il controllo sull'effettiva presenza del cd "bollino SIAE", di tutti i supporti di memorizzazione presenti in azienda.

Relativamente all'attività a rischio-reato "**Gestione del sito internet aziendale e del materiale informativo**".

Ai destinatari che, per ragioni del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione dei sistemi informativi aziendali è fatto obbligo di:

- garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge (con particolare riferimento a quelle in materia di diritto d'autore) e contrattuali;
- assicurare che testi, tabelle e altre illustrazioni tratte da riviste, manuali o opere siano riprodotti integralmente e fedelmente (nel rispetto delle limitazioni previste dalle normative o da previsioni contrattuali), con l'indicazione esatta della fonte.

Nell'ambito delle citate attività è fatto divieto di:

- diffondere -tramite reti telematiche - un'opera dell'ingegno o parte di essa;
- impiegare beni aziendali per adottare condotte che violino la tutela dei diritti d'autore;
- consentire citazioni che, avulse dal contesto da cui sono tratte, possono risultare parziali e/o contraddittorie rispetto agli intendimenti dell'autore.

In tutte le attività a rischio-reato sopra individuate, l'informazione e la formazione assumono una funzione imprescindibile.