MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D.LGS 231/01

MARINI SPA

PARTE SPECIALE VI

REVISIONE	DATA	OGGETTO	APPROVAZIONE
REV. 00	30/11/2021	PRIMA EMISSIONE	CDA MARINI del 30/11/2021
REV. 01	29/11/2024	SECONDA EMISSIONE	CDA MARINI del 29/11/2024

PARTE SPECIALE VI

IL MODELLO ORGANIZZATIVO DI MARINI SPA PER L'EVITAMENTO DEI REATI INFORMATICI E REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

Premessa

La presente Parte Speciale è dedicata alla prevenzione dei reati in materia di reati informatici e di reati connessi alla violazione dei diritti d'autore suscettibili di dar luogo alla responsabilità amministrativa di MARINI SPA (di seguito MARINI o la Società).

Ai fini della costruzione del presente Modello Organizzativo, le sopra menzionate categorie di reati sono oggetto di trattazione congiunta nella presente Parte Speciale data l'omogeneità delle fattispecie rilevanti, delle aree di rischio e relativi processi sensibili, nonché dei presidi di controllo.

Nei paragrafi successivi vengono descritti i reati informatici rilevanti sul piano della responsabilità aziendale ex art. 24-bis, nonché dei reati commessi in violazione del diritto di autore contemplati dall'art. 25-novies, del D.Lgs. 231/2001. Segue una descrizione dei processi sensibili con relativa evidenza delle modalità di astratta attuazione dei reati esaminati, nonché la enunciazione di regole generali di comportamento e la individuazione di protocolli di verifica e controllo finalizzati alla prevenzione del rischio penale di impresa.

Nello specifico è stato introdotto l'art. 24-bis del D. Lgs. 231/2001, modificato dalla L. 90 del 28 giugno 2024 che ha introdotto il comma 1 bis, ai sensi del quale si applica all'ente la sanzione pecuniaria da trecento a ottocento quote a seguito della commissione della nuova fattispecie di reato – introdotta dalla Legge sulla Cybersicurezza – legata all'estorsione informatica di cui all'art. 629, comma 3 del codice penale. Nei casi di condanna, inoltre, è prevista l'applicazione delle sanzioni interdittive di cui all'articolo 9, comma 2 del D. Lgs. 231/2001, per una durata non inferiore a due anni.

L'intento legislativo è quello di limitare la piaga estorsiva legata agli attacchi informatici di tipo "ransomware", provando a creare anche un argine al dilagare dei pagamenti dei riscatti richiesti dalle organizzazioni criminali.

La nuova norma ha anche modificato, aumentandole, le sanzioni previste al comma 2 e al comma 4 dell'art. 24 -bis.

1. TIPOLOGIE DI REATI INFORMATICI CUI E' ASSOCIABILE LA RESPONSABILITA' AZIENDALE EX ART. 24-BIS DEL D.LGS. 231/2001

Al fine di agevolare la piena conoscibilità da parte dei destinatari del Modello delle fattispecie penali incriminatrici richiamate dall'articolo 24-bis del D.Lgs. 231/2001, si riportano, testualmente, le previsioni di cui agli articoli di riferimento del Codice Penale.

Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico.

«*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da due a dieci anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da tre a dieci anni e da quattro a dodici anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.».

La disposizione punisce chiunque si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Con tale norma, il Legislatore intende infatti proteggere il "domicilio informatico", quale spazio ideale (ma anche fisico, in cui sono contenuti i dati informatici) di pertinenza della sfera individuale, nonché bene costituzionalmente protetto.

La disposizione presenta quindi elementi costitutivi comuni alla violazione di domicilio (artt. 614 e 615 c.p.) e si caratterizza per la previsione della duplice condotta di introduzione nel sistema e di permanenza in esso.

È inoltre importante rilevare come la manifestazione di volontà, da parte dell'avente diritto, di escludere chi si vuole introdurre (o chi si è introdotto, e si trattiene indebitamente) nel proprio domicilio informatico possa essere sia manifesta che tacita.

All'introduzione violenta (vale a dire contraria alla volontà del "proprietario") è equiparata quella clandestina (ovvero posta in essere in modo nascosto o fraudolento).

La norma prevede un aumento della pena nel caso in cui:

a) il fatto è commesso da pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso di poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso delle qualità di operatore del sistema;
b) se il fatto viene commesso con minaccia, violenza sulle cose o alle persone, o se palesemente armato;
c) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distribuzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati e delle informazioni o dei programmi in esso contenuti.

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

«Chiunque, 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 informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma».

La disposizione punisce chiunque, al fine di procurare a sé o ad altri un profitto o arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, importa, 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 al predetto scopo.

Si tratta pertanto di un reato di pericolo, in quanto la condotta descritta è punita al fine di evitare la consumazione di più gravi delitti, come ad esempio quelli di accesso abusivo a sistema informatico, o di frode informatica ai danni dello Stato o di altro ente pubblico.

La fattispecie richiede inoltre il dolo specifico, che consiste nel fine di procurare all'agente o ad altri un profitto ovvero di arrecare ad altri un danno.

Art. 615-quinquies c.p. – Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informativi diretti a danneggiare o interrompere un sistema informatico.

«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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329 ».

Anche questa disposizione è caratterizzata dal dolo specifico, consistente nello scopo di danneggiare illecitamente un sistema informatico o telematico.

Art. 617-quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.

«Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia, si procede d'ufficio e la pena è della reclusione da quattro a dieci anni se il fatto è commesso:

1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma;

2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema ».

Tale delitto è posto a presidio della inviolabilità dei segreti, con la finalità di assicurare la protezione delle comunicazioni e della corrispondenza in funzione dello sviluppo tecnologico.

La fattispecie in esame configura due differenti modalità di commissione del reato.

La prima, di cui comma 1, sussistente ogniqualvolta taluno in modo fraudolento intercetti le comunicazioni relative a un sistema informatico o telematico oppure le ostacoli od interrompa. La commissione di tali condotte rende sempre necessario un intervento dell'agente sulla rete, con cui pertanto egli interagisce.

La disposizione di cui al comma 2, invece, punisce la rivelazione delle comunicazioni di cui al primo comma. Si tratta di un comportamento illecito che non postula alcuna interazione con la rete violata e che può essere posto in essere anche da un soggetto che sia semplicemente entrato in possesso del contenuto delle comunicazioni protette.

Vi è poi la clausola di riserva, condotta che fa salva la disciplina di riferimento – in sostituzione di quanto previsto dall'art. 617-quater comma 2, qualora il fatto costituisca più grave reato. A tale proposito, può essere menzionata l'ipotesi in cui la rivelazione delle comunicazioni integri la rivelazione di un segreto di ufficio (art. 326 c.p.), con conseguente applicazione della disciplina prevista dell'art. 326 c.p. e corrispondente inapplicabilità dell'art. 617-quater c.p..

Circostanze aggravanti della condotta criminosa si rinvengono se:

- il fatto è commesso in danno di un sistema informatico utilizzato da ente pubblico o da azienda di pubblico servizio (public utility);
- il reato è compiuto da pubblico ufficiale, incaricato di pubblico servizio o da un amministratore di sistema.

Art. 617-quinques c.p. – Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche.

«*Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni 6.

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.»

Anche tale disposizione tutela la integrità e riservatezza delle comunicazioni, punendo l'installazione di apparecchiature prodromiche a condotte di intercettazione o alterazione delle comunicazioni medesime.

Per questa fattispecie di reato valgono le stesse ipotesi aggravanti previste dall'art. 617-quater c.p. (sistemi informatici della PA o di aziende di public utility, reato commesso da pubblico ufficiale, da incaricato di pubblico servizio o da amministratore di sistema).

Art. 635-bis c.p. - Danneggiamento di informazioni, dati e programmi informatici

«Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.».

Tale fattispecie rappresenta un delitto contro il patrimonio mediante violenza sulle cose, attagliato sulla ipotesi delittuosa del danneggiamento "comune", di cui all'art.635 c.p..

Le condotte descritte integrano ipotesi di aggressione unilaterale al patrimonio informatico altrui, cagionando alla persona offesa un peggioramento della propria situazione patrimoniale.

Inoltre, vi è un aggravamento di pena comune agli artt. 635-bis c.p., 635-ter c.p., 635-quater c.p. e 635-quinquies c.p., qualora ricorra la circostanza del fatto commesso con violenza alla persona o con minaccia oppure qualora l'agente commetta il fatto con abuso della qualità di amministratore di sistema (art. 635 comma 2 n. 1 c.p.).

Art.635-ter c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

«Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3) ».

Le fattispecie di cui agli artt. 635-ter c.p. e 635-quinquies c.p, prevedono un'anticipazione del momento consumativo del reato di danneggiamento informatico. Si prevede, infatti, che siano puniti i fatti diretti al danneggiamento, nelle varie forme e modalità descritte dalla norma, anche se dal fatto non deriva concretamente un danneggiamento vero e proprio.

In questi casi, infatti, il danneggiamento costituisce soltanto una circostanza aggravante del reato. Tale scelta trova spiegazione nella necessità di una intensa tutela dei dati pertinenti a soggetti pubblici o comunque di pubblica utilità.

Proprio per quanto si è detto, pare potersi ricomprendere tali fattispecie tra i reati di attentato o cd. "a consumazione anticipata". Si tratta di figure incompatibili con il delitto tentato perché in tali casi il tentativo equivale già alla consumazione del reato.

La disposizione in esame, nel tutelare il patrimonio altrui alla stregua di quella di cui all'art.635-bis, anticipa il momento consumativo del reato alle condotte prodromiche al danneggiamento, prescindendo quindi dal verificarsi dell'effettivo nocumento alle informazioni, ai dati o ai programmi informatici. Il danno costituisce soltanto una circostanza aggravante del reato.

Inoltre, vi è un aggravamento di pena comune agli artt. 635-bis c.p., 635-ter c.p., 635-quater c.p. e 635-quinquies c.p., qualora ricorra la circostanza del fatto commesso con violenza alla persona o con minaccia oppure qualora l'agente commetta il fatto con abuso della qualità di amministratore di sistema (art. 635 comma 2 n. 1 c.p.).

Art. 635-quater c.p. - Danneggiamento di sistemi informatici o telematici

«*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, 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 è punito con la reclusione da due a sei anni.*

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato».

La disposizione ricalca quella di cui all'art.635-bis c.p., salvo che per l'oggetto materiale, che è qui rappresentato dai "sistemi informatici o telematici". Da ciò discende una maggiore severità delle pene irrogabili.

Inoltre, vi è un aggravamento di pena comune agli artt. 635-bis c.p., 635-ter c.p., 635-quater c.p. e 635-quinquies c.p., qualora ricorra la circostanza del fatto commesso con violenza alla persona o con minaccia oppure qualora l'agente commetta il fatto con abuso della qualità di amministratore di sistema (art. 635 comma 2 n. 1 c.p.).

Art.635-quinquies c.p. - Danneggiamento di sistemi informatici o telematici di pubblico interesse.

«Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).».

Anche questa norma anticipa la soglia di punibilità alle condotte prodromiche al danneggiamento di sistemi informatici o telematici di pubblica utilità, ovvero al grave ostacolo al loro funzionamento.

La pena è aggravata nel caso in cui dal fatto derivi la distruzione, il danneggiamento o l'inutilizzabilità del sistema.

Inoltre, vi è un aggravamento di pena comune agli artt. 635-bis c.p., 635-ter c.p., 635-quater c.p. e 635-quinquies c.p., qualora ricorra la circostanza del fatto commesso con violenza alla persona o con minaccia oppure qualora l'agente commetta il fatto con abuso della qualità di amministratore di sistema (art. 635 comma 2 n. 1 c.p.).

Art. 640-quinquies c.p. - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica*[*].

«*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, 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, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro*».

La disposizione rinvia alla violazione di obblighi previsti da altra legge (quelli imposti per il rilascio di certificato di firma elettronica).

Il dolo è specifico e consiste nel fine di procurare all'agente o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

Art. 491-bis c.p. - Documenti informatici

«*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici*».

[*] fattispecie non applicabile a MARINI.

La Legge n. 48/2008 ha introdotto, tra i reati-presupposto di cui all'art. 24-bis del Decreto, l'art. 491-bis c.p., il quale, a sua volta, estende le ipotesi di falsità in atti di cui al Libro II, Titolo VII, Capo III c.p. a tutte le fattispecie delittuose in cui una o più delle suddette falsità abbiano ad oggetto un cd. "documento informatico".

Per "documento informatico" si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti [1] nonché destinato a dare quella certezza probatoria alla cui tutela sono preposte le norme penali

L'inserimento dell'art. 491-bis c.p. tra i reati presupposto rende necessaria una analisi sintetica delle ipotesi delittuose di cui al Capo III ("Della falsità in atti") del Titolo VII ("Dei delitti contro la fede pubblica") del Libro II del codice penale.

Preliminarmente può forse essere utile chiarire la distinzione, recepita nell'impianto codicistico, tra "falso materiale" e "falso ideologico".

Secondo l'interpretazione maggioritaria, tale distinzione postula le nozioni di "genuinità" e "veridicità" del documento e infatti:

- un documento è "genuino" se sussiste concordanza tra l'autore reale e l'autore apparente e se, una volta formato in via definitiva, non ha subito alterazioni;
- un documento è "veridico" se, oltre ad essere genuino in quanto compilato dall'autore apparente, contiene attestazioni conformi al vero.

Pertanto:

- il "falso materiale" si verifica in presenza di una condotta che esclude la genuinità dell'atto (ad esempio perché quest'ultimo è stato contraffatto, ossia compilato da persona diversa da quella all'apparenza autrice dello stesso, ovvero alterato, vale a dire modificato in epoca successiva rispetto alla sua definitiva formazione);
- il "falso ideologico" si verifica allorquando un documento attesta fatti non conformi al vero.

A) Falsità materiali

Art. 476 c.p. - Falsità materiale commessa dal pubblico ufficiale in atti pubblici

«*Il pubblico ufficiale che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.*

Se la falsità concerne un atto o parte di un atto che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni».

Art. 477 c.p. - Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative

«*Il pubblico ufficiale che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni*».

---

[1] *Cfr. art. 1 comma 1 lett. p) d.lgs. n. 235/2010, c.d. Codice dell'Amministrazione Digitale*

Art. 478 c.p. - Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti

«*Il pubblico ufficiale che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.*

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.

Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni».

I reati sin qui menzionati sono reati propri, in quanto per la configurabilità del delitto è necessaria la partecipazione, quale soggetto attivo, di un pubblico ufficiale; con questi, tuttavia, potrà concorrere un soggetto "non qualificato", ad esempio in veste di autore materiale del delitto o di istigatore dell'altrui proposito delittuoso.

Il bene tutelato è la "fede pubblica" intesa dai più come fiducia della collettività nella veridicità e genuinità di determinati oggetti, simboli e forme esteriori.

I delitti in esame sono procedibili d'ufficio, sono puniti a titolo di dolo generico ed è configurabile il tentativo.

Art. 482 c.p. - Falsità materiale commessa dal privato

«*Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.*

L'elemento di differenziazione rispetto alle ipotesi precedenti è rappresentata dal soggetto attivo in quanto autore del falso è il privato, cui la legge espressamente equipara il pubblico ufficiale che agisce fuori dall'esercizio delle sue funzioni».

Art. 493 c.p. - Falsità commesse da pubblici impiegati incaricati di un servizio pubblico

«*Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio, relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni*».

B) Falsità ideologiche

Art. 479 c.p. - Falsità ideologica commessa dal pubblico ufficiale in atti pubblici

«*Il pubblico ufficiale che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476*».

Art. 480 c.p. - Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative

«*Il pubblico ufficiale che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni*».

La differenza tra gli atti pubblici di cui all'art. 479 c.p. e i certificati o autorizzazioni amministrative ex art. 480 c.p. consiste in ciò: nei primi i fatti sono attestati come avvenuti alla presenza del pubblico ufficiale; nei secondi essi sono attestati come conosciuti dal pubblico ufficiale.

Si tratta di reati propri ed il dolo è generico.

Art. 483 c.p. - Falsità ideologica commessa dal privato in atto pubblico

«*Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.*

Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi».

Art. 493 c.p. - Falsità commesse da pubblici impiegati incaricati di un servizio pubblico

«*Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio, relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni*».

Art. 481 c.p. - Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità

«*Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da 51 a 516 Euro.*

Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro».

Art. 484 c.p. - Falsità in registri e notificazioni

«*Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a 309 Euro*».

C) Uso di atto falso

Art. 489 c.p. - Uso di atto falso

«*Chiunque, senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo*».

Presupposto del reato è l'avvenuta realizzazione di un reato di falso al quale l'agente della condotta di utilizzo non abbia partecipato, neanche prestando un contributo morale.

Soggetto attivo, quindi, potrà essere chiunque, purché non sia concorrente nel delitto di falso.

Il delitto è punito a titolo di dolo generico nell'ipotesi di uso di un atto pubblico falso. Il tentativo non è configurabile.

D) Soppressione, distruzione e occultamento, parziale o totale, di atti veri

Art. 490 c.p. - Soppressione, distruzione e occultamento di atti veri

Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero, o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute

Presupposto del reato è l'esistenza di un obbligo giuridico di conservazione del documento, almeno fino a quando questo mantiene una sua funzione probatoria. Soggetto attivo del reato può essere chiunque.

Oggetto materiale del reato sono solo gli atti originali e le copie autentiche che sostituiscono gli originali mancanti di atti pubblici.

"Sopprimere" vuol dire eliminare il documento con mezzi diversi dalla sua materiale distruzione.

"Occultare" sta a significare celare il documento impedendone la lettura o l'utilizzazione senza però attentare alla genuinità e veridicità dello stesso.

Il dolo è generico in relazione agli atti pubblici. Il tentativo è configurabile.

2. TIPOLOGIE DI REATI CUI È ASSOCIABILE LA RESPONSABILITÀ EX ART. 25-NOVIES D.LGS. 231/2001

I delitti in esame sono stati introdotti nel D.Lgs. 231/01 dalla Legge n. 99/2009, che ha operato un rinvio ad alcune delle fattispecie dettate in tema di diritto d'autore, ai sensi della Legge 22 aprile 1941, n. 633 (di seguito anche l.d.a.).

Le norme regolano i casi di violazione del diritto d'autore nelle ipotesi in cui sia usurpata, a vario modo - modificazione, distribuzione, riproduzione su supporti non contrassegnati SIAE, duplicazione per uso non personale- la paternità delle opere di ingegno altrui.

La norma è stata modificata dalla legge 14 luglio 2023, n. 93 ha introdotto la nuova lettera "h-bis" al comma 1 del suddetto art. 171-ter della Legge 633/1941.

Particolare rilievo rivestono la tutela penale del software e delle banche-dati e l'incriminazione della pirateria informatica. L'atto di pirateria è commesso da chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore. In particolare, uno dei fenomeni maggiormente diffusi in tema di pirateria informatica è il c.d. "*underlicensing*", che si verifica ogni qual volta vengono installate (duplicate) un numero di copie di un software maggiore rispetto al numero di copie effettivamente consentito dalla licenza d'uso del software medesimo, con ciò comportando un profitto aziendale in termini di risparmio di spesa. Il reato, tuttavia, si realizza anche attraverso il semplice utilizzo di un programma di software (ad es. software scaricato da Internet) per il quale non si dispone di una valida licenza o di una appropriata concessione di diritti di utilizzo. Inoltre, sono ricompresi anche eventuali abusi inerenti le banche dati (riproduzione, distribuzione, comunicazione, ecc.); gli accessi alle banche dati pubbliche, infatti, devono essere effettuati nel rispetto delle condizioni di utilizzo che accompagnano le stesse. La pirateria informatica, commessa nell'ambito di una

Società, implica non solo la responsabilità penale dell'operatore aziendale (o dell'outsourcer informatico) che duplica abusivamente il software, ma anche la responsabilità amministrativa della società stessa, nel caso in cui essa abbia ottenuto un vantaggio o perseguito un proprio interesse dalla condotta penalmente sanzionabile. Come sopra indicato, il vantaggio può essere rinvenuto anche nella mancata spesa per l'ottenimento di licenze d'uso del software utilizzato in azienda.

Al fine di agevolare la piena conoscibilità da parte dei Destinatari del Modello delle fattispecie penali incriminatrici richiamate dall'articolo 25-novies del Decreto, si riportano, testualmente, le previsioni di cui agli articoli di riferimento della legge n. 633/1941 e s.m.i. (c.d. legge sul diritto d'autore), seguite da una breve descrizione esplicativa delle suddette fattispecie.

Art.171, comma 1, lett. a bis, III c. L. 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

«*Salvo quanto previsto dall'art. 171-bis e dall'art. 171-ter, è punito con la multa da lire 100.000 [euro 51] a lire 4.000.000 [euro 2.065] chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:*

...

a-bis) 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".

III c.: «*La pena è della reclusione fino ad un anno o della multa non inferiore a lire 1.000.000 [euro 516], se i reati di cui sopra sono commessi sopra un'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*».

La condotta incriminata dalla fattispecie in esame è costituita dalla messa a disposizione del pubblico - senza averne diritto, a qualsiasi scopo e in qualsiasi forma - di un'opera dell'ingegno, e cioè della diffusione dell'opera affinché essa possa essere captata da un numero indeterminato di soggetti che possano accedervi dal luogo e nel momento scelti individualmente; tale diffusione può ad esempio essere realizzata mediante l'immissione in un sistema telematico.

Art. 171 bis L. 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)

«*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 lire cinque milioni [euro 2.582] a lire trenta milioni [euro 15.493]. 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 lire trenta milioni [euro 15.493] se il fatto è di rilevante gravità.*

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 artt. 64-quinquies e 64-sexies , ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli artt. 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 lire cinque milioni [euro 2.582] a lire trenta milioni [euro 15.493]. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni [euro 15.493] se il fatto è di rilevante gravità».

L'art. 171 bis l.d.a. ricorre tutte le volte in cui "chiunque":

1) 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 SIAE;
2) ovvero consente o facilita la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratore;
3) o ancora, 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 artt. 64-quinquies e 64-sexies l.d.a., ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli artt. 102-bis e 102-ter l.d.a., ovvero distribuisce, vende o concede in locazione una banca di dati.

Art. 171 ter L. 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)

«1. *È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 (da cinque a trenta milioni di lire) chiunque a fini di lucro;*
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, 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;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'articolo 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse;
h-bis) abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.
2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 (cinque a trenta milioni di lire) chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante concessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza le attività illecite di cui al comma 1.
3. La pena è diminuita se il fatto è di particolare tenuità.
4. La condanna per uno dei reati previsti nel comma 1 comporta:
a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.
5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici."

Art. 171 septies L. 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)

«*La pena di cui all'art. 171-ter, comma 1, si applica anche:*

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'art. 181-bis , i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;
b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'art. 181-bis, comma 2, della presente legge».

L'art. 171 ter l.d.a. configura una norma c.d. "multidisposizionale" (o a più fattispecie) che descrive ipotesi di frequente verificazione.

Di seguito, le più significative:

a) *la abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio; le stesse condotte che abbiano ad oggetto 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, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

b) l'introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, la messa in commercio, la concessione in noleggio o comunque la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della televisione con qualsiasi procedimento, la trasmissione a mezzo della radio, delle duplicazioni o riproduzioni abusive sopra delineate;

c) la vendita o la distribuzione, il noleggio o la cessione a qualsiasi titolo, la proiezione in pubblico o la trasmissione a mezzo della radio o della televisione di qualsiasi supporto contenga fonogrammi o videogrammi di opere artistiche o dell'ingegno per cui è prescritta l'apposizione di contrassegno da parte della SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

d) la ritrasmissione in pubblico, mediante qualsiasi mezzo – e in assenza di accordo con il legittimo distributore - di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

e) la promozione commerciale di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f) la fabbricazione, l'importazione, la pubblicità per la vendita o il noleggio, la detenzione per scopi commerciali di attrezzature, prodotti o componenti che abbiano la prevalente finalità o l'uso commerciale di eludere le misure tecnologiche che comprendono tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dai titolari dei diritti;

f-bis) la fabbricazione, l' importazione, la distribuzione, la vendita, il noleggio, la cessione a qualsiasi titolo, la pubblicizzazione per la vendita o il noleggio, o detenzione per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'articolo 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

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

h-bis) l'abuso, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, la stampa su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.

Tale norma, peraltro, sottopone a sanzione coloro che, esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rendono responsabili delle attività sopra delineate, ma anche chi, a fine di lucro, comunica al pubblico o immetta in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore o parte di essa.

Si tratta, per la maggior parte delle condotte ivi descritte, di un reato a consumazione anticipata, giacché – ad esempio - la formula legislativa «vende o pone altrimenti in commercio» non richiede l'effettivo compimento

di un negozio dispositivo, ma un'attività consistente nel porre in vendita o rendere disponibili per il noleggio supporti abusivamente riprodotti.

Art. 171-octies L. 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio)

«*Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da lire cinque milioni [euro 2.582] a lire cinquanta milioni [euro 25.822] 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.*

2. La pena non è inferiore a due anni di reclusione e la multa a lire trenta milioni [euro 15.493] se il fatto è di rilevante gravità».

Con riferimento alle ipotesi di messa in vendita, importazione promozione, installazione, modificazione e utilizzazione per uso pubblico e privato di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale – condotte descritte nell'ambito dell'art. 171 octies, l.d.a. – la medesima norma si preoccupa di fornire una nozione di "accesso condizionato". Si intendono infatti come 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".

3. MAPPATURA DELLE AREE E DELLE ATTIVITA' A RISCHIO

La mappatura delle aree operative della Società, svolta attraverso l'esame della documentazione aziendale ed una serie di interviste e sessioni di rilevazione su operatori "chiave" risultanti dall'organigramma aziendale, ha consentito di individuare i processi sensibili ove può essere presente il rischio di commissione dei reati previsti dall' art. 24-bis e dell'art. 25-novies del D.lgs. 231/2001. Nella trattazione seguente vengono dettagliate le attività maggiormente esposte al rischio di commissione dei reati in esame.

Area sensibile	Rischio Reato	Descrizione esemplificativa delle modalità di accadimento
		Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) Il Personale MARINI, in possesso di adeguato *background* tecnologico, potrebbe, in via ipotetica, forzare l'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza (società concorrente, banca dati privata, ente pubblico) per conoscere o sottrarre dati, informazioni, programmi nell'interesse dell'Azienda. **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)** Il Personale MARINI, in possesso di adeguato

IT	**REATI INFORMATICI**	background tecnologico, potrebbe, in via ipotetica, diffondere, cedere o mettere a disposizione di terzi – compresi esponenti di altre società del Gruppo- i codici di accesso a sistemi informatici di terze parti, al fine di procurare un vantaggio all'Azienda. **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)** Il Personale MARINI, in possesso di adeguato *background* tecnologico, potrebbe, in via ipotetica, forzare il sistema di autorizzazione e/o di autenticazione informatica previsti dalla rete interna, per diffondere virus, *malware*, *troyans* o altri programmi maligni nei sistemi informatici di terze parti (società concorrente, banca dati privata, ente pubblico), al fine di procurare un vantaggio all'Azienda. **Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)** Il Personale MARINI, in possesso di adeguato *background* tecnologico, potrebbe , in via ipotetica, attivare attacchi esterni ad un sistema informatico altrui, (società concorrente, banca dati privata, ente pubblico), mandando dolosamente in *crash* il sistema o provocandone il malfunzionamento, nell'interesse dell'Azienda. **Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)** Il Personale MARINI, in possesso di adeguato *background* tecnologico, potrebbe, in via ipotetica, procedere all'alterazione di un documento elettronico (es. registrazione contabile o certificazione di stato/caratteristiche) dalla quale possa derivare un interesse per l'Azienda o al fine di procurare un vantaggio all'Azienda.
IT	**REATI DI VIOLAZIONE DEL DIRITTO D'AUTORE**	Politiche di gestione IT che lascino liberi gli utenti di installare in locale programmi per elaboratore potrebbero astrattamente determinare un rischio di violazione del *copyright* che - se accompagnato da un vantaggio anche indiretto per l'azienda - potrebbe esporre la stessa a responsabilità 231. Stesso rischio potrebbe in astratto derivare in caso di debolezza delle politiche di gestione delle licenze sui sistemi operativi.

4. PROTOCOLLI DI VERIFICA E CONTROLLO DEI PROCESSI SENSIBILI - REATI INFORMATICI E IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

4.1. PREMESSA

Al fine di dare concreta attuazione organizzativa alle regole generali di prevenzione di cui al precedente paragrafo, di seguito vengono dettagliati i protocolli di controllo, diretti a regolamentare la formazione e l'attuazione delle decisioni aziendali, nella gestione dei processi sensibili sopra individuati.

4.2. PROTOCOLLI

Ciascun destinatario del Modello deve tenere comportamenti coerenti rispetto alle procedure formalizzate nonché alle prassi aziendali e, più precisamente, ai protocolli specifici per processo, come di seguito elencati

4.2.1. PROTOCOLLI SPECIFICI PER AREA

GESTIONE SISTEMI INFORMATIVI:

- Devono sempre essere presenti sistemi di gestione della sicurezza informatica tramite Antivirus, Firewall, AntiSpam, IDS (Intrusion Detection System) etc.;
- devono essere implementate politiche stringenti per il controllo degli accessi ai sistemi informatici, limitando l'accesso basato sulle necessità operative e sulle competenze specifiche;
- deve essere assicurato un accesso costante ai servizi IT affidabili, per mantenere l'efficienza operativa in tutta l'organizzazione;
- deve essere presente ed attuata la Policy sull'uso delle apparecchiature ICT/ di internet e della posta elettronica/ dell'informatica aziendale e dipartimentale;
- devono sempre essere presenti specifiche ed attuate procedure volte a disciplinare e tracciare le modalità di autorizzazione per la concessione di adeguati profili di accesso, di registrazione/modifica/cancellazione degli utenti, di definizione delle caratteristiche di sicurezza delle credenziali di autenticazione;
- deve essere presente e diffuso il documento riepilogativo delle principali procedure di comportamento per l'utilizzo dei sistemi informatici;
- devono essere presenti e diffuse prassi di comportamento per l'utilizzo corretto dei sistemi informatici, in base a quanto previsto dalla normativa vigente, anche in materia di privacy e di gestione ed utilizzo di dati e sistemi informatici e/o telematici;
- tutti gli *asset* aziendali informatici devono essere utilizzabili dagli utenti sulla base di appropriate password di accesso (periodicamente modificate) e livelli autorizzativi, definiti e attribuiti sulla base del ruolo, delle responsabilità e delle attività del singolo utente all'interno della Società;
- ad ogni utente deve essere associato un solo profilo abilitativo in relazione al proprio ruolo/funzione aziendale;
- al momento dell'ingresso nell'azienda, l'Ente IT fornisce ai nuovi dipendenti una sessione di *induction* sui sistemi IT per facilitare una rapida integrazione e comprensione degli strumenti;
- la gestione delle abilitazioni deve avvenire tramite la definizione di "profili di accesso" in ragione dei ruoli e delle funzioni svolte all'interno della Società;
- le attività di gestione ed utilizzo dei sistemi informatici/telematici e del patrimonio informativo aziendale da parte del personale (ivi compresi i collaboratori esterni e gli eventuali fornitori di servizi in *outsourcing*) devono essere assoggettate ad una costante attività di controllo, anche in funzione della verifica di possibili intrusioni esterne o verso sistemi informatici/telematici altrui;
- tutti gli eventi e le attività effettuate (tra le quali, ad es., gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, le variazioni dei profili degli utenti) devono risultare tracciate attraverso sistematica registrazione (ad es. Registro eventi standard dei server windows, Log dei firewall, Sistema dei ticket per le richieste di variazione permessi);
- devono essere attribuite precise responsabilità per garantire che il processo di sviluppo e manutenzione delle applicazioni informatiche, effettuato internamente o presso terzi, sia gestito in modo controllato e verificabile attraverso un adeguato e preciso iter autorizzativo;
- deve essere garantita la collaborazione con le altre funzioni aziendali per integrare le soluzioni IT con le strategie di business, migliorando l'efficacia organizzativa e la sinergia dei reparti:

- deve essere presente un sistema della gestione dei ticket IT interni ed esterni (SAP), per il log di sistema server (registro eventi windows), firewall (log), antivirus (log);
- devono essere adottate ed attuate misure adeguate ad assicurare che al termine del rapporto lavorativo con ciascuna risorsa aziendale (interna o esterna) siano restituiti tutti gli *asset* (PC, software, hardware, programmi informatici, etc.) della Società, siano rimossi tutti i diritti e disabilitate tutte le credenziali di accesso al patrimonio informatico ed informativo aziendale, tramite il modulo di *exit procedure* (disabilitazione di tutti gli accessi ai sistemi informatici e la restituzione degli asset assegnati);
- devono essere chiarite le responsabilità per la gestione degli aspetti di sicurezza informatica e conferiti poteri di controllo alle funzioni deputate allo sviluppo ed alla gestione dei sistemi informativi e al monitoraggio della sicurezza informatica/telematica;
- tramite Active directory devono essere definiti gruppi di accesso alle informazioni;
- le variazioni al contenuto dei profili di accesso sono eseguite dalle funzioni deputate al presidio della sicurezza informatica, su richiesta delle funzioni interessate e previa verifica in ordine alla corrispondenza delle abilitazioni informatiche richieste alle mansioni lavorative ricoperte, tramite un ticket proveniente dal *data owner*;
- gli uffici tecnici software, che per necessità lavorative dispongono di account amministratore locale sui propri dispositivi, assumono la responsabilità di non installare *software* non autorizzato o pirata, questa misura è fondamentale per prevenire violazioni del diritto di autore e garantire la sicurezza dei sistemi;
- le installazioni e l'uso di programmi informatici o di *software* così come l'utilizzo di apparecchi al di fuori delle strutture aziendali e, in generale, l'uso delle password di accesso devono essere sempre previamente autorizzati e tutti gli *asset* aziendali devono essere sempre precisamente identificati, inventariati e associati alla titolarità di un singolo utente, a cura della funzione deputata alla gestione della sicurezza informatica;
- gli utenti non devono avere accesso come "amministratori" al computer e non possono installare programmi in autonomia, salvo eccezioni debitamente giustificate e tracciate;
- per tutti gli utenti, deve essere mantenuto un inventario del software tramite un tool di raccolta dati;
- devono essere adottate misure avanzate di sicurezza informatica per prevenire il danneggiamento dei dati e degli *asset* IT, compresa la protezione contro gli accessi abusivi;
- devono essere adottate procedure chiare per la gestione e la segnalazione di incidenti di sicurezza, per assicurare una risposta rapida ed efficacie in caso di violazioni o minacce alla sicurezza dei dati;
- devono essere utilizzati strumenti avanzati di sicurezza, come soluzioni antivirus e sistemi di protezione dell'accesso ai dati, per mitigare i rischi principali, per mantenere un alto livello di sicurezza informatica al fine di: prioritizzare le misure di sicurezza, gestire le credenziali e gli accessi; fornire una risposta proporzionata agli incidenti;
- devono essere adottate misure idonee e procedure chiare per la gestione degli strumenti automatizzati;
- gli utenti dovranno essere formati rispetto agli strumenti automatizzati in utilizzo all'azienda e ai loro rischi.

5. ATTIVITA' DI CONTROLLO DELL'ORGANISMO DI VIGILANZA

Fatta salva l'attuazione degli ordinari compiti dell'OdV previsti nella Parte Generale del presente Modello, al fine specifico della prevenzione dei reati informatici e dei reati in materia di violazione del diritto d'autore, i controlli dell'OdV investono i seguenti aspetti:

- monitoraggio sull'efficacia e sul rispetto delle regole generali di prevenzione e dei principi generali di riferimento/protocolli posti a presidio dei processi sensibili;
- svolgimento di audit periodici sulla tenuta del sistema di sicurezza informatica aziendale ad *outsourcer* specializzati;
- verifica a campione sull'autenticità dei documenti informatici redatti all'interno di MARINI;
- verifica a campione sulla conformità dell'operato aziendale alle licenze d'uso dei software utilizzati nell'ambito di MARINI;
- esame di eventuali segnalazioni specifiche provenienti dagli altri organi di controllo o da qualsiasi dipendente, in merito alla violazione delle regole generali di prevenzione e dei principi di riferimento a presidio dei processi sensibili, anche in ottemperanza delle disposizioni e dei protocolli interni in tema di *whistleblowing*;
- predisposizione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute, tenendo conto della normativa sul *whistleblowing*.

Nel caso in cui, in seguito agli accertamenti svolti dall'OdV, emergessero elementi che facciano risalire alla scoperta della commissione di uno dei reati contemplati nella presente Parte Speciale, o al tentativo di commissione di uno dei reati suddetti, l'OdV dovrà riferire al Consiglio di Amministrazione di MARINI, al quale compete ogni decisione in merito alle sanzioni irrogabili (Cfr. Parte Generale – Sistema Sanzionatorio).