M.G.M.
Motori Elettrici S.p.A.

Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 8 giugno 2001 n. 231 s.m.i.

PARTE SPECIALE VII
REATI INFORMATICI E DI TRATTAMENTO DEI DATI
VIOLAZIONE DEL DIRITTO DI AUTORE

VERSIONE	DATA	ELABORATO DA	APPROVATO DA	AUTORIZZATO DA
0	14/05/2026	Consulente Esterno	Presidente	C.d.A.

Indice

1. Le fattispecie dei reati informatici e di trattamento illecito dei dati (art. 24-*bis* del D.Lgs. 231/2001)

1.1 Premessa

Ai fini di una migliore comprensione della normativa in materia di responsabilità amministrativa della Società, di seguito sono descritti, per tratti essenziali, i reati la cui commissione da parte dei soggetti riconducibili alla Società può generare responsabilità dell'ente con riferimento a tali categorie di reato e pertanto:

a) i delitti informatici e di trattamento illecito di dati contemplati all'art. 24-*bis* del D.Lgs. 231/01
b) il delitto di violazione del diritto di autore di cui all'art. 25-*novies* del D.Lgs. 231/01

I soggetti attivi del reato per ciascuna delle fattispecie delittuose sotto descritte sono: gli utenti generici, gli sviluppatori, i gestori di aree di sistema e, in generale, tutti i dipendenti che hanno un account o un pc in dotazione, gli amministratori di sistema nonché chiunque, anche solo in occasione di eventi straordinari (es. manutenzione, consulenti esterni, sviluppatori esterni), sia abilitato ad accedere ai sistemi proprietari o di terzi. Le fattispecie di reato si configurano in qualsiasi caso di violazione del sistema o di parti dello stesso e/o banche dati.

L'oggetto degli illeciti è il sistema informatico, comprese le banche dati e server interni ed esterni. In taluni casi anche i pc portatili e le altre tecnologie con accesso alla rete nonché gli HW i SW e tutti gli strumenti di memorizzazione di massa.

Nel descrivere le varie fattispecie incriminatrici, si indicheranno i reati la cui commissione da parte della Società è altamente remota se non improbabile, soprattutto riguardo al vantaggio o interesse dell'ente alla loro attuazione. Di ciò si terrà conto anche in fase di elencazione dei principi, protocolli e presidi cui la Società si è dotata al fine prevenzionale ai fini della valutazione di adeguatezza.

1.2 I reati di cui all'art. 24-*bis* del D.Lgs. 231/2001

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

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 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 dei dati, delle informazioni o dei programmi in esso contenuti.*

Qualora i fatti di cui ai commi primo e secondo riguardano 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 3 a 10 anni e da 4 a 12 anni.

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

L'intrusione abusiva in un sistema informatico si concretizza non appena vengono superate le misure di sicurezza del sistema stesso. E' punita la semplice intrusione senza alcuna differenza in seno all'effettivo danneggiamento o furto dei dati.

Possono commettere il delitto di cui all'art. 615 *ter* c.p. anche soggetti che, pur legittimati all'uso di un sistema, entrano in ambienti informatici cui l'accesso non è autorizzato. E' disciplinata anche l'ipotesi di permanenza non autorizzata qualora il responsabile dell'intrusione si trovi casualmente in una zona protetta del sistema, detta circostanza si realizza allorquando il reo "*vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*". Trattasi di reato di mera condotta, che si perfeziona con la violazione del cd "domicilio informatico", e quindi con l'introduzione del soggetto agente in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa.

Sul punto occorre, peraltro, precisare che il legislatore, con l'introduzione della fattispecie di reato de qua, non ha voluto tutelare solo i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma ha offerto una tutela più ampia che si concreta nello *ius excludendi alios* dell'utente, quale che sia il contenuto dei dati racchiusi nel sistema violato, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente stesso, sicché la tutela di legge si estende anche agli aspetti economico-patrimoniali dei dati sia che titolare dello *ius excludendi* sia persona fisica, sia giuridica, privata o pubblica, o altro ente.

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

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 uno a sei anni quando ricorre taluna delle circostanze di cui all'art. 615-ter, secondo comma, n.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.

Il reato di cui all'art. 615-*quater* c.p**.** sanziona la condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna 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. Il bene giuridico tutelato dalla norma in esame è senz'altro rappresentato da tutti quegli strumenti idonei a superare le barriere fisiche o virtuali poste a tutela di un sistema informatico/telematico.

Trattasi di reato di pericolo per la cui configurabilità è necessaria la sussistenza del dolo specifico.

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

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'art. 615-ter, terzo comma;
2) in danno di un pubblico ufficiale o nell'esercizio o a causa delle sue funzioni 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 amministratore di sistema.

L'art. 617-*quater* sanziona l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche (comma 1), nonché la condotta di chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni sopra indicate (comma 2).
In ordine alla condotta occorre precisare che l'intercettazione deve essere caratterizzata da una modalità fraudolenta, compiendosi con strumenti idonei a celarla ai comunicanti e/o al sistema informatico programmato per negare automaticamente gli accessi e le abusive intromissioni nelle comunicazioni informatiche e/o telematiche. Per

l'integrazione del reato de quo occorre che la comunicazione sia intercettata nel momento dinamico della sua trasmissione, trovando invece tutela nell'art. 616, 1° e 4° comma c.p., l'illecita presa di cognizione del contenuto di una comunicazione ormai avvenuta o già fissata in un supporto fisico.
In relazione al comma 1 va rilevato che le condotte di interruzione e impedimento consistono nel compimento di atti tecnicamente idonei, rispettivamente, a far cessare una comunicazione in corso e ad impedire che una nuova abbia inizio.
La previsione di cui all'art. 617 *quater* comma 2 non richiede invece quale presupposto del reato l'intercettazione fraudolenta delle comunicazioni, in quanto la ratio della tutela penale è quella di evitare che siano divulgate con qualsiasi mezzo di informazione al pubblico comunicazioni cosiddette "chiuse", destinate a rimanere segrete, delle quali l'agente sia comunque venuto a conoscenza.
Il delitto di cui all'art. 617-*quater* è perseguibile a querela di parte ma se sussistono specifiche circostanze aggravanti, individuate nel comma 4 della citata disposizione, la procedibilità è d'ufficio.

• 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.)

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.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.
Quando ricorre taluna delle circostanze di cui all'art. 617-quater, quarto comma numero 2), la pena è della reclusione da due a sei anni.
Quanto ricorre taluna delle circostanze di cui all'art. 617-quater, quarto comma, numero 1), la pena p della reclusione da tre a otto anni.

L'art. 617-*quinquies* punisce la detenzione, diffusione, produzione, uso o installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
Al fine della configurabilità del reato de quo è necessario che l'apparecchiatura installata sia concretamente idonea a realizzare le condotte sanzionate.
Qualora la comunicazione consista nello scambio di messaggi di posta elettronica, ha senso parlare di corrispondenza informatica intesa come ampliamento della tradizionale forma di 'corrispondenza', la cui libertà e segretezza sono ritenute 'inviolabili' dall'art. 15 della Costituzione. Ciò che si intende tutelare con gli articoli 617-*quater* e 617-

quinquies, sono proprio la libertà e la riservatezza delle comunicazioni informatiche, al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

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

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 pubblico servizio, con abuso dei poteri e 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 di sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

• ***Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-terc.p.)***

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).

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

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.

- ***Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.)***

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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 fino a euro 10.329.
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.

- ***Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.)***

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).

Gli articoli 635-*bis* e 635-*ter* c.p., introdotti con L. 48/2008, sanzionano i fatti di distruzione, danneggiamento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui, privati e pubblici. Gli articoli 635-*quater* e 635-*quinquies* c.p., anch'essi introdotti con la citata legge e modificati dalla L. 90/2024, proteggono invece da analoghe condotte di danneggiamento i sistemi informatici o telematici, privati e pubblici.
Queste quattro fattispecie di reato sostituiscono ora il "vecchio" reato di danneggiamento informatico di cui al previgente art. 635-*bis* c.p. , entrata nel codice ad opera della legge 547 del 1993, la quale aveva in questo modo preso atto, da una parte, della crescente importanza dei beni informatici e, dall'altra, della circostanza che poteva essere difficoltoso applicare al danneggiamento di beni immateriali, quali le informazioni memorizzate nel sistema o i programmi, il tradizionale reato di danneggiamento dell'art. 635 c.p., che tutela le "cose", intese nell'accezione di beni materiali.
Le disposizioni in esame non si limitano ad ampliare ed integrare la norma sul danneggiamento (art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispongono altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilo sanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali.
Oggetto di danneggiamento può essere innanzitutto il sistema informatico, eventualmente collegato a distanza con altri elaboratori, come nel caso dei sistemi telematici, e l'aggressione può riguardare tanto il sistema nel suo complesso quanto una o più delle sue componenti materiali, nonché i dati e i programmi informatici e le informazioni contenute nel sistema.
Occorre precisare infine che ove il fatto venga commesso con violenza o minaccia ovvero abusando della qualità di operatore di sistema, il legislatore ha previsto, per tutte le fattispecie di reato in esame, un aggravamento di pena e la procedibilità d'ufficio.
Gli articoli del Codice Penale summenzionati richiamati al primo comma dell'art. 24 bis del D.Lgs. 231/01 hanno come fattore comune il danneggiamento informatico che come tale può avvenire anche solo parzialmente. In ogni caso il dato comune, ai fini della rilevanza di cui alla richiamata normativa, è quello di creare un vantaggio o interesse nei confronti della società. E' inoltre possibile che dette condotte illecite possano essere poste in essere al fine di procurare un danno nei confronti di altra società o organo societario, al fine ad esempio di attuare politiche di concorrenza illecita, di furto di informazioni e know-how.

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

ll 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.

Tale reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Si tratta di reato proprio, ovvero realizzabile solo da soggetti che possiedano la qualifica richiesta dalla norma.

La fattispecie non è applicabile alla Società perché non fornisce, nemmeno indirettamente, tale servizio.

- ***Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019 n. 105)***

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, è punito con la reclusione da uno a tre anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote.

Il reato sanziona chiunque intralcia l'azione della P.A. e degli enti ed operatori del perimetro nazionale di sicurezza nazionale cybernetica volta ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

- ***Estorsione (art. 629, comma 3, c.p.)***

Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.

- ***Falsità di documenti informatici (art. 491-bis c.p.)***

Se alcuna delle falsità previste dal presente Capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici.

La configurazione tipica del reato di falso secondo la previsione dell'art. 491-*bis* è quella della "falsità in atti" applicabile e riferibile sia agli atti pubblici che alle scritture private, intendendosi per "documento informatico" qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.
Si tratta di una definizione "oggettiva" del falso, che perciò consente di prevedere "per estensione" almeno una serie di ipotesi penalmente rilevanti quali quelle previste dagli artt. 476 /493 *bis* CP concernenti atti pubblici o privati.
Tuttavia la particolare strutturazione della norma limita la nozione del "falso" alla avvenuta alterazione del dato informativo contenuto nel documento informatico solo qualora vi sia o sia documentabile una alterazione del "supporto" contenente dati o informazioni aventi efficacia probatoria oltre che nei programmi specificamente destinati alla relativa elaborazione.
Inoltre per "documento" e quindi "supporto" sarebbe la dottrina interpreta almeno sul piano degli effetti penali, qualsiasi "memorizzazione elettronica" in senso ampio e quindi qualsiasi "memorizzazione" di dati (testuali, grafici, fotografici, cinematografici e sonori, aggiungeremmo) effettuata in forma digitale attraverso appositi apparati hardware (e quindi anche mediante la memorizzazione in RAM del solo programma grafico eseguito e del file aperto solo ad esempio per trasmettere nelle forme di legge un documento falsamente composto e magari trasmesso per realizzare l'effetto di una falsa apparenza rivolta a terzi in buona fede, ma non memorizzato in memorie di massa vere e proprie).
Ed in effetti la predisposizione e l'utilizzazione di atti falsi si concretizza in una falsificazione a carattere virtuale, cioè una "simulazione" di un dato in realtà inesistente o "composto" da parti (grafiche o fotografiche) vere tagliate e incollate per finalità fraudolente, o falsamente attestanti un evento o una sottoscrizione nel caso, in verità più sofisticato, della alterazione dei dati alfanumerici che compongono le forme di sottoscrizione e di validazione degli atti pubblici e privati emessi o immessi in rete.

Il tutto, alla luce della ratio del D.Lgs 231/01 è quello dell'indebito vantaggio conseguito dalla "creazione" del falso e nell'interesse di chi lo ha compiuto di utilizzarlo per fini illeciti in un'ottica dolosa di prefigurazione di una realtà inesistente.
La portata applicativa della norma è estesa e può investire sia i più ampi settori societari, ma considerata la complessità della fattispecie deve riferirsi, principalmente agli organi direttivi ed al complesso decisionale – manageriale quale possibile utilizzatore del documento stesso all'interno della compagine societaria o parti di essa ovvero nei confronti di altre società o parti di essa.
L'ampiezza della formulazione della norma rende possibile non solo la tutela delle fattispecie che possono investire le problematiche di cui all'utilizzo della "firma digitale", ma anche delle sottoscrizioni di formulari mediante la mera indicazione del nome o mediante e-mail laddove sia dimostrabile la mancata associazione dei dati identificativi all'effettivo utente connesso.
Tuttavia non è semplice tale dimostrazione in concreto poiché il reato prospettabile confina e in un certo senso concorre con quello di cui all'art. 615-*quater* (detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici) e bene o male l'accesso stesso al sistema avviene dichiarando una identità ed esprimendo un consenso alla connessione da parte di un individuo che si identifica.

1.3. I delitti di cui all'art. 25-*novies* del D.Lgs. 231/2001 in materia di violazione dei diritti di autore

- ***Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)***

Salvo quanto disposto dall´art. 171-bis e dall´articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:
a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un´opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all´estero contrariamente alla legge italiana;
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;
a-ter) riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale;
omissis
La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell´opera, ovvero con deformazione, mutilazione o altra

modificazione dell´opera medesima, qualora ne risulti offesa all´onore od alla reputazione dell´autore.
La fattispecie, contraddistinta da una condotta generica qualificata solo dall'immissione in un sistema di reti telematiche, si aggrava nel caso previsto dal comma 3, per il quale: "*La pena è della reclusione fine ad un anno o della multa non inferiore a lire cinquemila se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore*".

La fattispecie è difficilmente realizzabile nell'interesse o a vantaggio della Società posto che il beneficio che teoricamente la Società potrebbe trarre da tale condotta sarebbe residuale rispetto all'entità della sanzione applicata.

• ***Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis, comma 1)***

• ***Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis,comma 2)***

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. 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 se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

• **Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito**

televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)

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 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, o 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 (S.I.A.E.), 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´art. 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.

È punito con la reclusione da uno a quattro anni e con la multa da da euro 2.582 a euro 15.493 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´art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni 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.

La pena è diminuita se il fatto è di particolare tenuità.

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 in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l´esercizio dell´attività produttiva o commerciale.

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.

L'art. 171-*ter* prevede la sanzionabilità con pene particolarmente severe di un ampio catalogo di condotte di violazione dei diritti d'autore e connessi. Le condotte elencate sono caratterizzate dall'abusività (la quale può essere identificata nell'assenza della prescritta autorizzazione da parte del titolare dei diritti d'autore e connessi), dal fine di lucro (che consiste nel fine di ricavare dall'attività illecita un guadagno), dal fatto che l'uso non sia personale, cioè travalichi l'ambito del godimento puro da parte del singolo utente.

E' importante sottolineare che anche l'art. 171-*ter* riguarda ogni tipo di violazione dei diritti d'autore e connessi, ivi comprese quelle commesse via Internet (quando queste siano caratterizzate dal fine di lucro).

Tuttavia, per le particolari caratteristiche sia del bene tutelato che delle modalità di realizzazione della condotta e del fine specifico perseguito, dette fattispecie sono difficilmente configurabili a carico di MGM posto che la Società non tratta opere dell'industria cinematografica o comunque in ambito culturale e dello spettacolo e il beneficio che teoricamente la Società potrebbe trarre da tale condotta sarebbe residuale rispetto all'entità della sanzione applicata.

- ***Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)***

La pena di cui all'articolo 171-ter, comma 1, si applica anche:

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

L'art. 171-*septies* prevede un ulteriore fattispecie di reato e sanziona, specificamente, la condotta dei produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 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 e di chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-*bis*, comma 2, della presente legge.

La fattispecie non è applicabile alla Società non soggetta agli obblighi SIAE.

- ***Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di 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 (art. 171-octies legge n.633/1941).***

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 a lire cinquanta milioni 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.

La pena non è inferiore a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

La Corte Costituzionale, con sentenza 16 - 29 dicembre 2004, n. 426 (in G.U. 1a s.s. 5/1/2005, n. 1), ha dichiarato l'illegittimità costituzionale del presente articolo "nella parte in cui, limitatamente ai fatti commessi dall'entrata in vigore di detto art. 171-octies fino all'entrata in vigore della legge 7 febbraio 2003, n. 22 (Modifica al decreto legislativo 15 novembre 2000, n. 373, in tema di tutela del diritto d'autore), punisce con sanzione penale, anziché con la sanzione amministrativa prevista dall'art. 6 del decreto legislativo 15 novembre 2000, n. 373 (Attuazione della direttiva 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato), l'utilizzazione per uso privato di 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.

La fattispecie è difficilmente configurabile avuto riguardo all'attività e agli interessi di MGM.

3. Processi Sensibili nell'ambito dei reati informatici, di violazione dell'industria e commercio e di violazione del diritto di autore

3.1 L'organizzazione dei sistemi aziendali

La Società ha adottato un sistema composto da 6 server con sistemi di back up e business continuity. Il sistema di posta elettronica è gestito da server interni ridondanti con Microsoft Exchange Server.
Ogni utente ha autorizzazzioni "user" e può accedere alla documentazione presente sui server laddove richiesto dall'azienda e autorizzato dagli account amministrativi.
Sono amministratori di sistema per i diversi server in gestione: Cristiano Piaceri, Italway srl, Roberto Maltagliati 01 Informatica e azienda Var4Team.

I PC e i vari apparati son acquistati da produttori o rivenditori autorizzati e dotati di apposita licenza. Sono adottate tutte le misure di sicurezza in linea con la normativa di riferimento. E' stato adottato un firewall perimetrale con prevenzioni intrusioni e vpn dedicate con certificato crittografato per l'accesso dall'esterno.

La Società ha provveduto a identificare gli amministratori di sistema e ha adottato il proprio Regolamento sull'uso dei sistemi informativi aziendali.

Dispone poi di un sistema di gestione del trattamento dei dati personali conforme alla normativa GDPR, che prevede uno specifico regolamento per la gestione delle informazioni riservate, per la privacy e per l'utilizzo dei sistemi informatici aziendali, tutta la modulistica necessaria per adempiere agli obblighi della normativa di riferimento.

Gli adempimenti relativi alla sicurezza del trattamento dei dati personali (D.Lgs. 196/03 e Regolamento Europeo 679/16) sono seguiti dall'Amministratore Delegato, con l'ausilio di un consulente esterno, per assicurare un trattamento lecito e legittimo dei dati personali e conforme agli standard di sicurezza prescritti dalla legge.

Soltanto il Presidente è dotato di smart card. La smart card è personale e non può essere ceduta a terzi, nemmeno in uso. I soli soggetti autorizzati all'utilizzo della smart card sono gli intestatari della stessa.

3.2. I Processi Sensibili

I Processi Sensibili ritenuti più specificatamente a rischio in relazione ai reati esposti nel par. 1 della presente Parte Speciale, individuati in esito all'*as-is analysis* come da par. 4.6 della Parte Generale, sono:

- Gestione e configurazione sistema informativi aziendali, di posta elettronica e di sistemi telematici
- Selezione dei fornitori e gestione degli approvvigionamenti
- Gestione adempimenti privacy

Detti Processi sono stati rilevati con riferimento alle seguenti Aree aziendali:

- *Presidente del Consiglio di Amministrazione*, in relazione alle deleghe consiliari ricevute;
- *Amministratore Delegato,* in relazione alle deleghe consiliari ricevute;
- *Amministrazione,* in relazione agli adempimenti in materia di privacy e in relazione alle attività di selezione dei fornitori svolte dall'ufficio acquisti.
- *Amministratori di Sistema,* i titolari di PC e di account aziendali, in relazione alle attività di utilizzo del sistema informativo aziendale; utilizzo della posta elettronica aziendale, ordinaria e certificata;

Di seguito verranno indicati i protocolli e sistemi di controllo adottati previa enunciazione dei principi di riferimento da osservare nella costruzione e/o implementazione del Modello.

4. Principi generali di riferimento

Tutti coloro che sono dotati delle credenziali di accesso ai sistemi di MGM devono osservare le procedure aziendali e rispettare i principi di:

- riservatezza, intesa come garanzia che una informazione sia accessibile solo a chi è autorizzato;
- integrità, intesa come salvaguardia dell'accuratezza e della completezza dell'informazione e dei metodi di elaborazione;
- disponibilità, intesa come garanzia che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse associate, quando richiesto.

Inoltre è fatto loro divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del D.Lgs. 231/01);
- connettere ai sistemi informatici di MGM personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del referente IT;
- procedere a installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano il diritto d'autore;
- modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- acquisire, possedere, o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati, ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici;
- ottenere credenziali di accesso a sistemi informatici o telematici con metodi o procedure differenti da quelle autorizzate da MGM;
- divulgare, cedere o condividere con personale interno o esterno di MGM le proprie credenziali di accesso ai sistemi e alla rete aziendale;
- accedere abusivamente a un sistema informatico altrui – ovvero nella disponibilità di altri dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, comprensivo di archivi, dati e programmi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- acquisire e/o utilizzare prodotti tutelati dal diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;

- comunicare a persone non autorizzate, interne o esterne a MGM, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- usare lo spamming come pure ogni azione di risposta al medesimo;
- inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi;
- utilizzare per finalità diverse da quelle lavorative le risorse informatiche (es. personal computer fissi o portatili) assegnate dalla Società;
- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- scaricare file o immagini o contenuti personali sui dispositivi aziendali e accedere a siti i cui contenuti ledano la libertà o la dignità umana e siano indecorosi, pornografici o pedopornografici.

I Destinatari sono inoltre tenuti a rispettare scrupolosamente tutte le norme vigenti, e in particolare:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- garantire la tracciabilità dei documenti prodotti;
- assicurare meccanismi di protezione dei file, quali, ad esempio, password da aggiornare periodicamente, secondo le prescrizioni comportamentali della Società;
- utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;
- utilizzare unicamente materiale pubblicitario (i.e. materiale fotografico) autorizzato.

MGM si impegna, a sua volta, a porre in essere i seguenti adempimenti:

- informare adeguatamente tutti i Destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi, dell'importanza di:
    - mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
    - utilizzare correttamente i software e banche dati in dotazione;
    - non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali;
- prevedere attività di formazione e addestramento periodico in favore dei dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore dei destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

- far sottoscrivere ai dipendenti, nonché agli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;
- informare i dipendenti e, in generale, tutti i Destinatari del Modello eventualmente autorizzati all'utilizzo dei sistemi informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- limitare gli accessi alle stanze server unicamente al personale autorizzato;
- proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative a un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venire disattivati;
- impedire l'installazione e l'utilizzo di software non approvati da MGM e non correlati con l'attività professionale espletata per la stessa;
- informare gli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore e in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- limitare l'accesso alle aree e ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti a individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;
- impedire l'installazione e l'utilizzo, sui sistemi informatici di MGM, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, Virus, etc.) senza alcuna possibilità di controllo da parte di MGM;
- qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a MGM, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;
- prevedere un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti, degli stagisti e degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi;
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti e degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;

- provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;
- prevedere, nei rapporti contrattuali con i Fornitori di servizi software e banche dati sviluppati in relazione a specifiche esigenze aziendali, clausole di manleva volte a tenere indenne la Società da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi.

Inoltre, con riferimento al processo di gestione degli adempimenti relativi alla privacy per assicurare un trattamento lecito e legittimo dei dati personali e conforme agli standard di sicurezza prescritti dalla legge, è fatto obbligo di:

- attenersi scrupolosamente alle disposizioni dettate dal Reg. UE 679/16 e dall'Authority competente, avendo cura di predisporre la modulistica di riferimento e di formare periodicamente il personale sulla normativa di riferimento e sull'uso dei presidi presenti in azienda.

Riguardo al processo di selezione dei fornitori e gestione degli approvvigionamenti, è fatto obbligo di avvalersi di fornitori di HW e SW dotati delle apposite licenze alla vendita e/o dei diritti di proprietà intellettuale e/o d'autore sui prodotti oggetto dell'attività, quale requisito imprescindibile della qualificazione e dell'iscrizione nel registro dei fornitori nonché di controllare, in fase di consegna, che i prodotti siano della qualità, quantità e provenienza indicati in fase di ordine, non rechino alterazioni nei marchi o nei segni distintivi, abbiano l'imballo originale e siano muniti di certificazione di garanzia del produttore.

5. I controlli dell'OdV

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'OdV effettua periodicamente controlli a campione sulle attività sociali potenzialmente a rischio di reati informatici e di trattamento illecito dei dati, diretti a verificare la corretta osservanza delle procedure in essere.

A tal fine, si ribadisce che all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Con riferimento ai Processi Sensibili oggetto della presente Parte Speciale – 7, l'OdV dovrà effettuare:

(i) verifiche periodiche sul rispetto della normativa sulla privacy riguardo all'adozione delle misure di sicurezza necessarie a prevenire la commissione dei reati della fattispecie di quelle qui esaminate;

(ii) verifiche periodiche sull'espletamento delle comunicazioni alle autorità pubbliche;

(iii) un monitoraggio sull'osservanza del Regolamento per l'utilizzo dei sistemi informativi aziendali

(iv) l'esame di eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente e gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.

L'OdV dovrà predisporre, con cadenza semestrale, un rapporto scritto semestrale per il Consiglio di Amministrazione sull'attività svolta.