PARTE SPECIALE "E"
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (art. 24-bis del Decreto)

INDICE

DEFINIZIONI

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale "B" qui di seguito indicate:

- Credenziali: l'insieme degli elementi identificativi di un utente o di un account (generalmente UserID e Password).
- Dati Informatici: qualunque rappresentazione di fatti, informazioni, o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.
- Delitti Informatici: i reati di cui all'art. 24-bis del Decreto.
- Documento/i Informatico/i: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
- Password: sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.
- Peer to Peer: meccanismo di condivisione di contenuti digitali tramite una rete di personal computer, di regola utilizzati per scambio di file con contenuti audio, video, dati e software.
- Piano di Sicurezza: documento che definisce un insieme di attività coordinate che devono essere intraprese per implementare la politica di sicurezza del sistema.
- Postazione di Lavoro: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.
- Sicurezza Informatica: l'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.
- Sistemi Informativi: l'insieme della rete, dei sistemi, dei data base e delle applicazioni aziendali.
- Spamming: invio di numerosi messaggi indesiderati, di regola attuato attraverso l'utilizzo della posta elettronica.
- Virus: programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.

B.1 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto)

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati nella presente Parte Speciale "E", così come indicati agli artt. 24-bis del Decreto, che si propone di ottenere un corretto utilizzo delle risorse informatiche ed è caratterizzata da principi procedurali che mirano a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

B.1.1. LE TIPOLOGIE DI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto)

• Falsità in documenti informatici (art. 491-bis cod. pen.)

La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. Capo III, Titolo VII, Libro II), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un Documento Informatico, pubblico o privato, avente efficacia probatoria (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).

In particolare, si precisa che si ha "falsità materiale" quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente o sottoscrittore, con divergenza tra autore apparente e autore reale del documento (contraffazione), ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.

Si ha, invece, "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere.

Nel falso ideologico, dunque, è lo stesso autore del documento che attesta fatti non rispondenti al vero.

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

A titolo esemplificativo, integra il delitto di falsità in Documenti Informatici la condotta di chi falsifichi documenti aziendali oggetto di flussi informatizzati o la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati "sensibili" in vista di una possibile attività ispettiva.

• Accesso abusivo ad un sistema informatico o telematico (art. 615-ter cod. pen.)

Tale reato si realizza quando un soggetto si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

A tal riguardo si sottolinea come il legislatore abbia inteso punire l'accesso abusivo ad un sistema informatico o telematico tout court, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del

personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).
La suddetta fattispecie delittuosa si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.
Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, o acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa.

• Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. pen.)
Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.
L'art. 615-quater cod. pen., pertanto, punisce le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.
I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, Password o schede informatiche (quali badge o smart card).
Tale fattispecie si configura sia nel caso in cui il soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.
L'art. 615-quater cod.pen., inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.
Potrebbe rispondere del delitto, ad esempio, il dipendente della società (A) che comunichi ad un altro soggetto (B) la Password di accesso alle caselle e-mail di un proprio collega (C), allo scopo di garantire a B la possibilità di controllare le attività svolte da C, quando da ciò possa derivare un determinato vantaggio o interesse per la società.

• Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen.)
Tale reato si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso

pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.
Tale delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un Virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.

• Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. pen.)
Tale ipotesi di reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.
Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.
Il reato potrebbe configurarsi, ad esempio, con il vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara
.
• Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. pen.)
Questa fattispecie di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
La condotta vietata dall'art. 617-quinquies cod. pen. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.
Il reato si integra, ad esempio, a vantaggio della società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

• Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen.)
Tale fattispecie di reato si realizza quando un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

Il danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

• Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen.)
Tale reato si realizza quando un soggetto commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.
Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della società.

• Danneggiamento di sistemi informatici o telematici (art. 635-quater cod. pen.)
Questo reato si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis cod. pen., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.
Pertanto qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis cod. pen.

• Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen.)
Questo reato si configura quando la condotta di cui al precedente art. 635-quater cod. pen. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter cod.pen, quel che rileva è in primo luogo che il danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

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

Questo 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 di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato cd. proprio in quanto può essere commesso solo da parte dei certificatori qualificati, o meglio, i soggetti che prestano servizi di certificazione di Firma Elettronica qualificata.

Si precisa in ogni caso che la commissione di uno dei Delitti Informatici sopra descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno del dato/informazioni/programma/sistema informatico o telematico, possa determinare un interesse o vantaggio per il Gestione Italia.

Pertanto, nell'ambito della descrizione delle singole fattispecie criminose, si è tenuto conto di tale rilevante aspetto per l'elaborazione dei casi pratici proposti.

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei Delitti Informatici possono essere di natura pecuniaria, da 100 a 500 quote e di natura interdittiva, che variano a seconda della fattispecie criminosa realizzata.

B.2. AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, , le seguenti:

1. tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;
2. gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione;
3. gestione dei flussi informativi elettronici con la pubblica amministrazione;
4. utilizzo di software e banche dati;
5. gestione dei contenuti del sito Internet di Gestione Italia.

Eventuali integrazioni delle Aree a Rischio potranno essere disposte dagli amministratori di Gestione Italia al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

B.3 DESTINATARI DELLA PARTE SPECIALE: PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE.

Obiettivo della presente Parte Speciale è che i Destinatari si attengano - nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei

confronti di Gestione Italia- a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici.
In particolare, la presente Parte Speciale ha la funzione di:
a) fornire un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
b) fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.
Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, gli Esponenti Aziendali sono tenuti, in generale, a rispettare tutte le regole e i principi contenuti, per le parti di proprio interesse, nei seguenti documenti:
1. Codice Etico;
2. organigramma aziendale e schemi organizzativi;
3. ogni altra normativa interna rilevante ai fini della presente parte speciale.

B.4 PRINCIPI PROCEDURALI SPECIFICI

Al fine di garantire adeguati presidi nell'ambito delle singole Aree a Rischio, si prevedono qui di seguito le regole che devono essere rispettate di Gestione Italia, dagli Esponenti Aziendali nonché dagli altri soggetti eventualmente autorizzati nell'ambito delle suddette aree.
In particolare, è vietato:
1. connettere ai sistemi informatici di Gestione Italia, personal computer, periferiche e altre apparecchiature, o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
2. procedere ad installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso;
3. 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;
4. 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 (sistemi per individuare le Credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
5. ottenere Credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle autorizzate da Gestione Italia;
6. divulgare, cedere o condividere con personale interno o esterno a Gestione Italia le proprie Credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

7. accedere abusivamente ad 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;
8. manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
9. 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;
10. accedere abusivamente al sito Internet della Società al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali (immagini, infografica, video, ecc);
11. comunicare a persone non autorizzate, interne o esterne a Gestione Italia, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
12. 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;
13. lo Spamming come pure ogni azione di risposta al medesimo;
14. inviare attraverso un sistema informatico aziendale informazioni o dati falsificati o, in qualunque modo, alterati.

Il Gestione Italia si impegna, a sua volta, a porre in essere i seguenti adempimenti:
1. informare adeguatamente i Dipendenti, nonché gli stagisti e gli altri soggetti - come ad esempio i Collaboratori Esterni - 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;
2. prevedere attività di formazione e addestramento periodico in favore dei Dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore degli stagisti e degli altri soggetti - come ad esempio i Collaboratori Esterni - 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;
3. far sottoscrivere ai Dipendenti, nonché agli stagisti e 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;
4. informare i Dipendenti, nonché gli stagisti e gli altri soggetti - come ad esempio i Collaboratori Esterni - 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; impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

5. limitare gli accessi alle stanze server unicamente al personale autorizzato;
6. 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 ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
7. dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
8. impedire l'installazione e l'utilizzo di software non approvati da Gestione Italia e non correlati con l'attività professionale espletata per la stessa;
9. limitare l'accesso alle aree ed 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 ad 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;
10. impedire l'installazione e l'utilizzo, sui sistemi informatici di Gestione Italia, 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 del Gestione Italia;
11. 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 Gestione Italia, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai Dipendenti;
12. 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;
13. 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, degli stagisti e degli altri soggetti - come ad esempio i Collaboratori Esterni - eventualmente autorizzati all'utilizzo dei Sistemi Informativi;
14. provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;
15. 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 Gestione Italia da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano

determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi; prevedere che negli stessi rapporti vengano sottoscritti specifici documenti con cui si impegnino al corretto utilizzo e alla tutela delle risorse informative aziendali con cui entrano in contatto.

B.5 ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui all'art. 24 -bis e 24 -nonies del Decreto sono i seguenti:

o svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui all'art. 24-bis e 25-nonies del Decreto. Con riferimento a tale punto l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti del Gestione Italia eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sui Delitti Informatici, ovvero in occasione di mutamenti nell'organizzazione aziendale e nell'attività in relazione al progresso scientifico e tecnologico;

o proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

o esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Il Gestione Italia garantisce l'istituzione di flussi informativi proceduralizzati tra l'OdV ed i responsabili delle Direzioni competenti, ovvero ogni altro Esponente Aziendale ritenuto necessario che, in ogni caso, potranno essere sentiti dall'OdV ogni volta ritenuto opportuno.

L'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nel capitolo B.4 della presente Parte Speciale.

E' altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti aziendali rilevanti per lo svolgimento dei propri compiti.