

PARTE SPECIALE B

- DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI -

Indice

1. I REATI DI CUI ALL'ART. 24 <i>BIS</i> DEL D. LGS. N. 231/2001.....	3
1.1) Accesso abusivo ad un sistema informatico o telematico (Art. 615 ter del codice penale)	4
1.2.) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617 quater del codice penale).....	4
1.3.) Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (Art. 617 quinquies del codice penale).....	5
1.4.) Danneggiamento di informazioni, dati e programmi informatici (Art. 635 bis del codice penale).....	5
1.5.) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635 ter del codice penale).....	5
1.6.) Danneggiamento di sistemi informatici o telematici (Art. 635 quater del codice penale)	6
1.7.) Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635 quinquies del codice penale).....	6
1.8.) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615 quater del codice penale).....	6
1.9) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615 quinquies del codice penale).....	6
1.10) Documenti informatici (Art. 491 bis del codice penale).....	7
1.11) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640 quinquies del codice penale).....	10
2. LE AREE A RISCHIO. I RUOLI AZIENDALI COINVOLTI. I REATI PROSPETTABILI.	10
3. IL SISTEMA DI CONTROLLI.....	17
4. PRINCIPI GENERALI DI COMPORTAMENTO.	19

1. I REATI DI CUI ALL'ART. 24 BIS DEL D. LGS. N. 231/2001

Con la legge 18 marzo 2008, n. 48, denominata "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23 novembre 2001) e norme di adeguamento dell'ordinamento interno", si sono ampliate le fattispecie di reato che possono generare la responsabilità dell'ente, introducendo, nel corpo del D. Lgs. n. 231/2001 (di seguito anche '**Decreto**'), l'art. 24 bis rubricato "*Delitti informatici e trattamento illecito di dati*", il quale stabilisce:

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

Preliminarmente deve essere osservato che il Legislatore ha previsto due tipologie di reati rilevanti ai fini del Decreto:

a) i reati propriamente informatici;

b) i reati di falso commessi mediante l'utilizzo di (o su) documenti/dati informatici.

Con riferimento alla prima categoria di reati (che saranno di seguito specificati), si rintracciano una serie di elementi comuni, vale a dire:

i) elemento oggettivo: seppure le condotte possano essere materialmente diverse, si tratta di illeciti penali in cui il computer o il sistema informatico o telematico costituisce il fulcro della condotta. Ed infatti il computer o il sistema informatico o telematico rappresentano o il mezzo/ modalità di realizzazione della condotta (condotte realizzate mediante l'uso del computer), o la natura dell'oggetto materiale (condotte realizzate contro il computer - sistema informatico o telematico)

Per 'sistema informatico/telematico' si intende «una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche». (Cass. Sez. VI Pen. 4 ottobre - 14 dicembre 1999, n. 3067). Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione") per mezzo di impulsi elettronici, su supporti adeguati di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici ("codice"), in combinazioni diverse: tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente.

ii) elemento soggettivo: sono tutti reati puniti a titolo di dolo (coscienza e volontà di commettere il reato), anche se per alcuni di essi è necessario, altresì, il dolo specifico (vale a dire un'intenzione ulteriore che l'agente deve perseguire nel compiere la condotta delittuosa: es. il fine di trarre profitto).

Si riporta, di seguito, la descrizione delle fattispecie incriminatrici richiamate e afferenti la categoria *sub a*).

1.1) Accesso abusivo ad un sistema informatico o telematico (Art. 615 ter del codice penale)

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 uno a cinque 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 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 uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Il reato potrebbe configurarsi, a titolo di esempio, qualora un dipendente della Società acceda, utilizzando password indebitamente carpite, al sistema informatico altrui (ad esempio competitor, ecc.) al fine di acquisire informazioni relative alle strategie aziendali ecc.

1.2.) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617 quater del codice penale)

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 sei mesi a quattro 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 uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) 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, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

A titolo di esempio, il reato potrebbe realizzarsi qualora un dipendente effettuasse un attacco di c.d. *sniffing* mediante l'utilizzo di sistemi atti ad intercettare comunicazioni informatiche/telematiche di un competitor per finalità di spionaggio industriale e/o conseguente diffusione.

1.3.) Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (Art. 617 quinquies del codice penale)

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte 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'art. 617-quater.

A titolo esemplificativo, il reato si configura mediante l'installazione di dispositivi tecnologici (es., sniffer e scanner di onde elettromagnetiche) volti ad intercettare le comunicazioni telefoniche, o informatiche wired e wireless.

1.4.) Danneggiamento di informazioni, dati e programmi informatici (Art. 635 bis del codice penale)

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 sei mesi a tre anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Il reato potrebbe configurarsi, ad esempio, qualora un dipendente della Società, alteri dati particolarmente rilevanti ai fini dell'attività di informazione scientifica quali: dati personali dei medici, prezzi di aggiudicazione delle gare, ecc.

1.5.) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635 ter del codice penale)

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 utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. 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 tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

A titolo esemplificativo, tale fattispecie potrebbe, astrattamente, realizzarsi nell'ipotesi in cui un dipendente della Società, acceda al sistema informatico del tribunale (al fine di alterare o cancellare informazioni raccolte durante un'ipotetica indagine) o dell'INPS (al fine di modificare le singole posizioni assicurative).

1.6.) Danneggiamento di sistemi informatici o telematici (Art. 635 quater del codice penale)

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 uno a cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Vale l'esempio fatto sopra per il reato di cui all'art. 635 bis.

1.7.) Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635 quinquies del codice penale)

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Vale l'esempio fatto sopra per il reato di cui all'art. 635 quater.

1.8.) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615 quater del codice penale)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, 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, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater.

Il reato potrebbe configurarsi, ad esempio, nel caso in cui un dipendente della Società effettui un attacco di social engineering, di forza bruta al fine di individuare le credenziali di accesso ad un sistema di un competitor.

Sotto un diverso profilo il dipendente potrebbe, una volta procuratesi le credenziali, riprodurre, diffondere, comunicare o consegnare a terzi i codici, parole chiave o altri mezzi necessari all'accesso al sistema informatico. Queste ultime condotte possono essere integrate anche qualora i codici le parole chiave o gli altri mezzi siano procurati da un soggetto terzo.

1.9) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615 quinquies del codice penale)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna

o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

A titolo di esempio, il reato potrebbe configurarsi qualora un dipendente della Società effettui attacchi di *cracking, hacking, spoofing* per alterare i dati relativi, ad esempio, ai dossier di registrazione/negoziazione dei farmaci di un competitor.

Con riferimento alla categoria di reati precedentemente indicata *sub b)* - i reati di falso commessi mediante l'utilizzo di (o su) documenti/dati informatici -, parimenti possono individuarsi una serie di elementi comuni:

i) definizione di 'documento informatico': qualunque supporto informatico contenente dati e informazioni aventi efficacia probatoria (quindi il documento informatico viene equiparato all'atto pubblico o alla scrittura privata avente efficacia probatoria).

ii) bene giuridico tutelato: il bene tutelato dalle norme è la "fede pubblica", vale a dire l'interesse a che i mezzi probatori siano genuini e veridici e alla certezza dei rapporti economici e giuridici.

iii) elemento oggettivo: in questa tipologia di reati si concretizza o nella condotta di alterare/manomettere il documento nella sua essenza materiale, ovvero nella sua genuinità (cd 'falsità materiale') ovvero in condotte che tendono ad incidere sul contenuto dello stesso, vale a dire sulla verità dei fatti in esso espressi (c.d. falsità ideologica).

iv) elemento soggettivo: i reati de quo sono puniti solo a titolo di dolo (è esclusa quindi la punibilità per colpa: negligenza, imperizia, imprudenza o inosservanza di leggi).

1.10) Documenti informatici (Art. 491 bis del codice penale)

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

La norma sopra citata estende le disposizioni in tema di falso in atto pubblico alle falsità riguardanti un documento informatico; i reati richiamati sono i seguenti:

- Articolo 476 codice penale (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.

- Articolo 477 codice penale (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 adempite le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

- Articolo 478 codice penale (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.

- Articolo 479 codice penale (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.

- Articolo 480 codice penale (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.

Con riferimento alle fattispecie sopra indicate, deve, preliminarmente, segnalarsi che i dipendenti della Società non rivestono la qualifica di pubblico ufficiale o incaricato di pubblico servizio (per la definizione si veda la Parte Speciale A). Di conseguenza i reati di falso in precedenza indicati, sono astrattamente configurabili, ai fini di cui al Decreto, solo nell'ipotesi in cui il dipendente/soggetto riferibile alla Società sia imputato di concorso esterno nei reati eventualmente commessi da coloro i quali dispongono della qualifica soggettiva prima detta.

Alla luce di quanto sopra specificato, dunque, i reati possono configurarsi in tutti i casi in cui il dipendente/soggetto riferibile alla Società contribuisca fattualmente o moralmente con atti e/o omissioni all'alterazione/modificazione/contraffazione/formazione/simulazione dei documenti informatici rilevanti ai fini dei precedenti articoli.

- Articolo 481 codice penale (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 e 51,00 a e 516,00.

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

Si veda quanto riportato nel punto precedente con la differenza che, in questo caso, il concorso deve accedere ad una condotta posta in essere dall'esercente una professione sanitaria (es. infermiere, medico, ecc.) o forense (es., avvocato).

- Articolo 482 codice penale (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.

In via esemplificativa, il reato sarebbe configurabile laddove un dipendente della Società alteri le ricevute bancarie telematiche di versamenti tributari.

- Articolo 483 codice penale (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.

A titolo esemplificativo tale fattispecie potrebbe trovare applicazione in nel caso in cui un dipendente della Società in sede di gara d'appalto, dichiara, per via telematica, che la Società ha adempiuto a determinati obblighi di legge al fine di partecipare alla gara stessa.

- Articolo 484 codice penale (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 e 309,00.

A titolo di esempio, un dipendente della Società potrebbe alterare il dossier da inviare all'AIFA per la registrazione di un farmaco al fine di fornire dati relativi a studi medico-scientifici falsi.

- Articolo 487 codice penale (Falsità in foglio firmato in bianco. Atto pubblico)

Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.

- Articolo 488 codice penale (Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali)

Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dall'articolo 487, si applicano le disposizioni sulle falsità materiali in atti pubblici.

Per le modalità esemplificative di questi reati valgono le considerazioni prima espresse con riferimento ai reati commessi dai pubblici ufficiali/incaricati di pubblico servizio.

- Articolo 489 codice penale (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.

A titolo di esempio tale fattispecie è astrattamente realizzabile qualora il dipendente della Società utilizzi documenti informatici falsi, senza aver concorso a falsificare il documento, per procurare un vantaggio alla Società.

- Articolo 490 codice penale (Soppressione, distruzione e occultamento di atti veri)

Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute.

A titolo esemplificativo, la fattispecie è astrattamente realizzabile nei casi in cui, il dipendente della Società acceda in un sistema informatico altrui e distrugga documenti aventi efficacia probatoria.

- Articolo 492 codice penale (Copie autentiche che tengono luogo degli originali mancanti)

Agli effetti delle disposizioni precedenti, nella denominazione di «atti pubblici» e di «scritture private» sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.

- Articolo 493 codice penale (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.

Queste fattispecie sono definitorie ai fini della eventuale estensione oggettiva o soggettiva dei reati di falso.

1.11) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640 quinquies del codice penale)

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.

2. LE AREE A RISCHIO. I RUOLI AZIENDALI COINVOLTI. I REATI PROSPETTABILI.

In occasione dell'implementazione dell'attività di *risk mapping*, è stata individuata, nell'ambito della struttura organizzativa ed aziendale di Novo Nordisk S.p.A. (in seguito '**Novo Nordisk**' o '**Società**' o '**Azienda**'), un'area "a rischio reato" denominata "**Gestione dei sistemi informativi**, ovvero un settore e/o processo aziendale rispetto al quale è stato ritenuto astrattamente sussistente il rischio di commissione dei reati informatici.

Nell'ambito della suddetta area sono state/i individuate/i:

- le relative **attività c.d. "sensibili"**, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in questione;
- **i ruoli aziendali coinvolti** nell'esecuzione di tali attività "sensibili" e che, astrattamente, potrebbero commettere i reati informatici, sebbene tale individuazione dei ruoli/funzioni non debba considerarsi, in ogni caso, tassativa, atteso che ciascun soggetto individuato nelle procedure potrebbe in linea teorica essere coinvolto a titolo di concorso; in particolare, nell'ambito dei ruoli coinvolti, sono state riportate anche le Società che, in virtù del contratto di servizi stipulato con Novo Nordisk (si veda par. **5.2.1.** della Parte Generale), svolgono le attività sensibili nell'interesse della Società;
- in via esemplificativa, i **principali controlli procedurali previsti** con riferimento alle attività che sono poste in essere nelle aree "a rischio reato", oltre alle regole definite nel Modello di organizzazione, gestione e controllo e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.) - dirette ad assicurare la chiara definizione dei ruoli e delle responsabilità degli attori coinvolti nel processo e l'individuazione dei principi di comportamento.

Di seguito verranno riportate le attività c.d. "sensibili" ricomprese nell'area "**GESTIONE SISTEMI INFORMATIVI/INFORMATION TECHNOLOGY**", individuata come "a rischio" con riferimento ai reati informatici.

Attività sensibile n. 1: GESTIONE DELLA SICUREZZA INFORMATICA A LIVELLO LOGICO (Gestione dei profili utente e del processo di autenticazione; Gestione degli accessi da e verso l'esterno)	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) <i>Accesso abusivo ad un sistema informatico o telematico (art. 615 ter, cod. pen.)</i></p> <p>2) <i>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater, cod. pen.)</i></p> <p>3) <i>Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies, cod. pen.)</i></p> <p>4) <i>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</i></p> <p>5) <i>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</i></p> <p>6) <i>Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</i></p> <p>7) <i>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</i></p> <p>8) <i>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici</i></p>

	<p>(art. 615 quater, cod. pen.)</p> <p>9) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</p> <p>10) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</p>
--	---

Attività sensibile n. 2: GESTIONE DELLA SICUREZZA INFORMATICA A LIVELLO FISICO (gestione e protezione della postazione di lavoro; sicurezza fisica)	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) Accesso abusivo ad un sistema informatico o telematico (art. 615 ter, cod. pen.)</p> <p>2) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater, cod. pen.)</p> <p>3) Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies, cod. pen.)</p> <p>4) Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</p> <p>5) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</p> <p>6) Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</p> <p>7) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</p> <p>8) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater, cod. pen.)</p> <p>9) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</p> <p>10) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</p>

Attività sensibile n. 3: GESTIONE DEL PROCESSO DI CREAZIONE, TRATTAMENTO, ARCHIVIAZIONE DI DOCUMENTI ELETTRONICI CON VALORE PROBATORIO	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) <i>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</i></p> <p>2) <i>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</i></p> <p>3) <i>Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</i></p> <p>4) <i>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</i></p> <p>5) <i>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater, cod. pen.)</i></p> <p>6) <i>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</i></p> <p>7) <i>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</i></p> <p>8) <i>Art. 491 bis, cod. pen. e reati di falso correlati:</i></p> <ul style="list-style-type: none"> • <i>Artt. 110 e 476 cod. pen. (Falsità materiale commessa dal pubblico ufficiale in atti pubblici);</i> • <i>Artt. 110 e 477 cod. pen. (Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative);</i> • <i>Artt. 110 e 478 cod. pen. (Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o provati e in attestati del contenuto di atti);</i> • <i>Artt. 110 e 479 cod. pen. (Falsità ideologica commessa dal pubblico ufficiale in atti pubblici);</i> • <i>Artt. 110 e 480 cod. pen. (Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative);</i> • <i>Artt. 110 e 481 cod. pen. (Falsità ideologica in certificati commesse da persone esercenti un servizio di pubblica necessità);</i> • <i>Art. 482 cod. pen. (Falsità materiale commessa dal privato);</i> • <i>Art. 483 cod. pen. (Falsità ideologica commessa dal privato in atto pubblico);</i> • <i>Art. 484 cod. pen. (Falsità in registri e notificazioni);</i>

	<ul style="list-style-type: none"> • <i>Artt. 110 e 487 cod. pen. (Falsità in foglio firmato in bianco. Atto pubblico);</i> • <i>Art. 488 cod. pen. (Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali);</i> • <i>Art. 489 cod. pen. (Uso di atto falso);</i> • <i>Art. 490 cod. pen. (Soppressione, distruzione e occultamento di atti veri);</i> • <i>Art. 492 cod. pen. (Copie autentiche che tengono luogo degli originali mancanti).</i>
--	--

Attività sensibile n. 4: GESTIONE DELLE ATTIVITA' DI MANUTENZIONE DEI SISTEMI ESISTENTI E GESTIONE DELLE ATTIVITA' DI ELABORAZIONE DATI	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) <i>Accesso abusivo ad un sistema informatico o telematico (art. 615 ter, cod. pen.)</i></p> <p>2) <i>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater, cod. pen.)</i></p> <p>3) <i>Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies, cod. pen.)</i></p> <p>4) <i>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</i></p> <p>5) <i>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</i></p> <p>6) <i>Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</i></p> <p>7) <i>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</i></p> <p>8) <i>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater, cod. pen.)</i></p> <p>9) <i>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</i></p> <p>10) <i>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</i></p>

Attività sensibile n. 5: GESTIONE E PROTEZIONE DELLE RETI	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) <i>Accesso abusivo ad un sistema informatico o telematico (art. 615 ter, cod. pen.)</i></p> <p>2) <i>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater, cod. pen.)</i></p> <p>3) <i>Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies, cod. pen.)</i></p> <p>4) <i>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</i></p> <p>5) <i>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</i></p> <p>6) <i>Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</i></p> <p>7) <i>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</i></p> <p>8) <i>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater, cod. pen.)</i></p> <p>9) <i>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</i></p> <p>10) <i>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</i></p>

Attività sensibile n. 6: ATTIVITA' DI BACK-UP DEI DATI E DEGLI APPLICATIVI	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) <i>Accesso abusivo ad un sistema informatico o telematico (art. 615 ter, cod. pen.)</i></p> <p>2) <i>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater, cod. pen.)</i></p> <p>3) <i>Installazione d apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies, cod. pen.)</i></p>

	<p>4) <i>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</i></p> <p>5) <i>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</i></p> <p>6) <i>Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</i></p> <p>7) <i>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</i></p> <p>8) <i>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater, cod. pen.)</i></p> <p>9) <i>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</i></p> <p>10) <i>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</i></p>
--	---

Attività sensibile n. 7: GESTIONE BANCHE DATI E SOFTWARE DELLA SOCIETÀ	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Reati astrattamente ipotizzabili	<p>1) <i>Accesso abusivo ad un sistema informatico o telematico (art. 615 ter, cod. pen.)</i></p> <p>2) <i>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater, cod. pen.)</i></p> <p>3) <i>Installazione d apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies, cod. pen.)</i></p> <p>4) <i>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis, cod. pen.)</i></p> <p>5) <i>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato e da altro ente pubblico o comunque di pubblica utilità (art. 635 ter, cod. pen.)</i></p> <p>6) <i>Danneggiamento di sistemi informatici o telematici (art. 635 quater, cod. pen.)</i></p> <p>7) <i>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies, cod. pen.)</i></p> <p>8) <i>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater, cod. pen.)</i></p> <p>9) <i>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies, cod. pen.)</i></p>

	<i>10) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies, cod. pen.)</i>
--	---

3. IL SISTEMA DI CONTROLLI.

Il sistema di controlli, implementato da Novo Nordisk, prevede, in relazione alle attività sensibili sopraindicate, l'adozione di una serie di controlli volti a garantire un sistema di gestione della sicurezza informatica:

- Fornitura dei servizi IT alla Novo Nordisk Region Europe in virtù di specifico contratto di servizio;
- la Società è dotata di un Quality Management System che definisce i requisiti e gli standard per la documentazione di tutti i processi IT;
- adozione di alcune procedure emesse dalla Capogruppo in relazione al processo di gestione dei sistemi informativi per i sistemi informativi gestiti dalla Capogruppo; la Società dispone di procedure volta a disciplinare il processo di gestione cambiamenti sui sistemi informativi, di una procedura volta a disciplinare il processo di gestione del sito internet: "Gestione del Sito internet www.novonordisk.it";
- chiara identificazione dei ruoli e delle responsabilità delle funzioni coinvolte nel processo di gestione dei sistemi informativi, anche per l'attuazione degli adempimenti previsti dalle leggi in vigore;
- diffusione delle procedure aziendali attraverso il sistema interno;
- chiara segregazione di funzioni e responsabilità nelle attività relative alla gestione della rete, all'amministrazione dei sistemi e allo sviluppo/manutenzione degli applicativi;
- predisposizione di specifiche regole nell'ambito delle procedure che disciplinano la gestione delle credenziali di accesso ai sistemi ed il loro monitoraggio periodico;
- adozione misure di sicurezza a livello globale per la gestione degli incidenti che definiscono ruoli, modalità operative e urgenze per tutte le fasi della gestione degli incidenti stessi;
- identificazione dei soggetti aventi parte nel processo di richiesta, verifica ed autorizzazione degli accessi;
- previsione nell'ambito delle procedure che disciplinano il sistema, della rimozione dei diritti di accesso al termine del rapporto di lavoro;
- predisposizione di procedure di batch;
- segregazione delle funzioni in relazione ad eventuali ulteriori incarichi ricoperti all'interno del Gruppo e previsione di un processo volto ad accertare la segregazione delle funzioni all'interno dei singoli processi tramite la revisione della richiesta dello specifico ruolo da parte del manager del dipartimento e dal "System Owner" ovvero il gestore dello specifico sistema informativo;
- separazione delle competenze garantita da una separazione degli accessi ai sistemi informativi;

- creazione/cancellazione delle utenze effettuate in accordo con la funzione Risorse Umane;
- gestione delle configurazioni dei PC e loro monitoraggio effettuato a livello centralizzato;
- identificazione di tutti gli utenti attraverso una user ID personale tramite il quale gli stessi accedono ai vari applicativi;
- effettuazione delle fasi di modifica delle utenze in accordo con l'Ente richiedente;
- previsione di criteri minimi di robustezza per la scelta delle password che sono soggette a rinnovo obbligatorio;
- inibizione dell'utilizzo della medesima password per più di una volta;
- obbligo del cambio della password al primo login;
- divieto di lasciare attiva una sessione di lavoro in caso di allontanamento dal PC;
- blocco di tutti i PC dopo diversi minuti di inattività e nuova richiesta dell'inserimento di un login e di una password per l'accesso;
- previsione di apposite misure per un'adeguata protezione delle apparecchiature incustodite;
- mappatura e monitoraggio dei sistemi stand alone;
- svolgimento di attività di training ed aggiornamento al fine di sensibilizzare i dipendenti della Società in relazione ai predetti aspetti;
- utilizzo della firma digitale per la trasmissione della documentazione alla PA da parte delle funzioni preposte a tale attività;
- previsione di apposite misure di protezione dei documenti elettronici;
- svolgimento di corsi di formazione on-line, organizzati dalla Società, finalizzati alla sensibilizzazione all'uso appropriato degli strumenti informatici ed alle misure di sicurezza;
- previsione di apposite misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse;
- definizione formale, all'interno delle proprie procedure, dei criteri per l'identificazione dei soggetti proprietari dei dati e per la loro classificazione;
- previsione di una procedura per il trasferimento dei dati sensibili mediante supporti esterni o rimovibili;
- previsione nelle procedure della responsabilità dei dipendenti nei confronti delle informazioni loro affidate;
- predisposizione presso la sede della Società di un Centro Elaborazione Dati (CED) il cui accesso è riservato al solo personale autorizzato;
- assegnazione degli asset della Società formalizzato nelle procedure adottate;

- allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'Organizzazione;
- gli accessi da remoto verso la rete aziendale avvengono tramite VPN crittografata;
- adozione di una procedura di change management che regola ogni tipo di cambiamento riguardante sistemi ed infrastrutture, definendo vari sub-processi ed i corrispondenti responsabili;
- formalizzazione di una procedura per il back up dei dati;
- definizione di un piano di Disaster Recovery System.

4. PRINCIPI GENERALI DI COMPORTAMENTO.

Tutte le risorse aziendali e, in particolare, coloro i quali rivestono posizioni rilevanti nell'utilizzo e nell'amministrazione dei sistemi informatici, devono ispirare la loro azione ai seguenti principi di comportamento:

- **Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- **Integrità:** garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- **Disponibilità:** garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico di tutti i destinatari del Modello 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 Decreto);
- violare i principi di seguito previsti.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;

d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;

h) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

i) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

l) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo che siano stati acquisiti con il loro espresso consenso e per motivi strettamente lavorativi;
- evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.