Parte Speciale "B"

Delitti informatici e trattamento illecito di dati

1. PREMESSA

La presente Parte Speciale è dedicata ai reati informatici previsti dall'art. 24-*bis* del Decreto, introdotto dall'art. 7 della legge 18 marzo 2008, n. 48. Si tratta di reati commessi mediante l'impiego di tecnologie informatiche o telematiche e caratterizzati da diverse tipologie di condotta.

Alcuni di questi reati sono connotati dall'uso illegittimo degli strumenti informatici e finalizzati all'accesso abusivo in un sistema informatico, alla modifica o al danneggiamento dei dati ivi contenuti, ovvero al danneggiamento del medesimo. Altri riguardano condotte di intercettazione illegittima di comunicazioni informatiche o telematiche. Infine, è prevista la fattispecie di frode informatica del soggetto certificatore della firma elettronica.

Si segnala che, ai fini penali, la legge parifica il documento informatico pubblico all'atto pubblico scritto e quello privato alla scrittura privata cartacea.

I reati di cui agli artt. 615-*quater*, 615-*quinquies*, 617-*quater* e 617-*quinquies* c.p. sono stati modificati dalla Legge 23 dicembre 2021, n. 238.

Da ultimo, l'art. 20 della Legge 90/2024 ha apportato una serie di modifiche all'art. 24-bis del D.lgs. 231/2001.

2. I REATI DI CUI ALL'ART. 24-*BIS* DEL DECRETO

2.1. – Falsità riguardanti un documento informatico (art. 491-*bis* c.p.)

L'articolo prevede *"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."*

Lo scopo della norma è la tutela della fede pubblica attraverso la salvaguardia dell'integrità del documento informatico nella sua valenza probatoria.

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

Ai sensi dell'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 minaccia o violenza sulle cose o alle persone, ovvero se è palesementearmato;

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

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da tre a dieci anni e da quattro a dodici anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

La disposizione in esame offre una tutela ampia, comprensiva e anticipata che si sostanzia nel c.d. "*ius excludendi alios*", avente a oggetto tutti i dati raccolti nei sistemi informatici protetti, indipendentemente dal loro contenuto, purché attinenti alla sfera di pensiero o alle attività, lavorative e non, dell'utente, in modo da assicurare una protezione da qualsiasi tipo di intrusione che possa avere anche ricadute economico-

patrimoniali.

Per sistema informatico a mente della Convenzione di Budapest del 23 novembre 2001 si intende qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base a un programma, compiono l'elaborazione automatica dei dati.

Il delitto di cui all'art. 615-*ter* c.p. integra un reato di mera condotta che si perfeziona con la violazione del domicilio informatico, mediante l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, a nulla rilevando che si verifichi un'effettiva lesione della riservatezza degli utenti.

Le condotte punite dal primo comma consistono: a) nell'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (da intendere come accesso alla conoscenza di dati o informazioni contenuti nel sistema, effettuato sia da lontano, sia da vicino); b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione (da intendersi come il fatto di chi persista nella già avvenuta introduzione, inizialmente autorizzata o casuale, continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema).

Secondo la giurisprudenza di legittimità quel che rileva è il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che non può considerarsi autorizzato ad accedervi e a permanervi, sia quando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro), sia quando ponga in essere operazioni di natura diversa da quelle di cui egli è incaricato e in relazione alle quali l'accesso gli è consentito.

L'articolo pertanto punisce a titolo di dolo generico le condotte non solo di chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ma anche di chi vi si trattiene contro la volontà, espressa o tacita, del titolare che ha il diritto di escluderlo.

L'articolo in commento è stato da ultimo modificato dalla Legge 28 giugno 2024, n. 90.

2.3. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.)

Ai sensi dell'art. 615-*quater* c.p. "*Chiunque, al fine di procurare a sé o ad altri un vantaggio 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 a due anni e con la multa sino lire dieci milioni.*

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"

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

La fattispecie prevede che *"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 quattro a dieci annise il fatto è commesso:

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

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

La norma è indirizzata all'impedimento dell'intercettazione fraudolenta, che si verifica quando si prende conoscenza di comunicazioni altrui, in modo occulto e senza autorizzazione. Si tratta di una fattispecie a dolo generico e, salvo le aggravanti previste dal quarto comma, il reato è procedibile a querela della persona offesa.

In particolare, l'intercettazione si ha quando il messaggio giunge integralmente al destinatario, l'interruzione quando l'invio del messaggio viene interrotto e, pertanto, non giunge al destinatario, l'impedimento quando il messaggio non riesce nemmeno a partire.

2.5. - Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.)

L'articolo dispone che: "*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.

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

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

La norma offre una forma di tutela anticipata rispetto a quella prevista dall'art. 617-*quater*, punendo comportamenti prodromici alle condotte descritte nel precedente articolo. Per la realizzazione della fattispecie è sufficiente il mero pericolo di arrecare danno alla libertà di comunicare e alla riservatezza.

Le condotte consistono nella installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, a nulla rilevando l'effettivo funzionamento delle stesse.

2.6. – Estorsione informatica (art. 629, comma terzo, c.p.)

Ai sensi della norma in commento, " *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*".

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

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

La pena è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato".

La fattispecie si differenzia rispetto al danneggiamento ordinario per gli interessi tutelati inerenti la realtà informatica e telematica.

Le condotte sono rappresentante dalla distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi altrui.

La condotta della "cancellazione", secondo la giurisprudenza di legittimità, deve essere interpretata nella accezione informatica e non semantica del termine, ossia come la "rimozione da un certo ambiente di determinati dati, in via provvisoria attraverso il loro spostamento nell'apposito cestino o in via 'definitiva' mediante il successivo svuotamento dello stesso". Pertanto, del tutto irrilevante, ai fini della sussistenza del reato, è il fatto che i file cancellati possano essere recuperati *ex post* attraverso una specifica procedura tecnico-informatica.

Secondo tale impostazione, la configurabilità del reato di danneggiamento informatico non viene dunque preclusa dall'eventuale reversibilità del danno, ritenendosi sufficiente che il bene tutelato sia stato - anche solo temporaneamente - oggetto di manomissione o alterazione rimediabile attraverso un postumo intervento riparatorio.

2.8. - Danneggiamento di informazioni, dati e programmi informatici pubblici o di pubblico interesse (art. 635-*ter* c.p.)

Ai sensi dell'art. 635-*ter* c.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)".

La norma punisce i medesimi fatti sanzionati dall'art. 635 *bis* allorquando l'attività si diriga avverso informazioni, dati e programmi informatici di interesse militare o relativi all'ordine pubblico, alla sicurezza pubblica, alla sanità, alla protezione civile o comunque di interesse pubblico. Sono inoltre previste delle

aggravanti nei casi indicati ai commi successivi.

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

L'articolo dispone: "*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da due a sei anni.*

La pena è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato".

La fattispecie richiama le condotte di cui all'art. 635-*bis* c.p. e punisce condotte ulteriori, quali l'introduzione o la trasmissione di dati, informazioni o programmi, che danneggino, distruggano, rendano anche in parte inservibili o ostacolino il funzionamento di altrui sistemi informatici o telematici.

2.10. – 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)

Ai sensi della norma in commento "*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 euro10.329.*
La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter,secondocomma,numero1).
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".

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

Ai sensi della norma in commento: *"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".*

L'articolo punisce le condotte dell'art. 635 *quater* dirette a sistemi informatici o telematici di pubblica utilità.

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

L'articolo dispone: *"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."*

L'articolo tutela l'attività di rilascio di un certificato qualificato rispetto ad attività poste in essere dal certificatore che per fini ed interessi di tipo privato viola gli obblighi previsti dalla legge.

La fattispecie richiede il dolo specifico rappresentato dal fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

2.13. Reato di ostacolo o condizionamento dei procedimenti per la Sicurezza Cibernetica e delle relative attività ispettive e di vigilanza (art. 1., co. 11 D.L. 105/2019)

Con il Decreto Legge 21 settembre 2019, n. 105, cd. DL Cyber Security, il legislatore ha introdotto una serie di misure volte a tutelare la sicurezza cibernetica nazionale e, in particolare, al fine di: garantire l'integrità e la sicurezza delle reti; configurare un sistema di organi, procedure e misure, al fine di consentire un'efficace valutazione tecnica della sicurezza degli apparati e dei prodotti, tenendo conto degli standard definiti a livello internazionale e dell'UE.

Il nuovo reato di violazione delle norme delle norme in materia di perimetro di sicurezza nazionale cibernetica è un reato proprio poiché solo coloro che rientrano nel perimetro sono assoggettati agli obblighi previsti dalla normativa in questione e alla vigilanza delle preposte autorità e, pertanto, potrebbero essere incriminate. Si configura come reato a forma vincolata, essendo sanzionata la violazione di determinati

obblighi, secondo determinate modalità, ovvero il rilascio di informazioni false o l'omissione di informazioni dovute e l'ostacolo alle funzioni di vigilanza. La norma fa riferimento, infatti, solo a: procedimenti di formazione degli elenchi (co.2, l.b)); procedimenti di affidamento (co.6, l.a)); funzione di vigilanza (co.6,l.c)).

2.14. Trattamento sanzionatorio per le fattispecie di cui all'art. 24-*bis* del Decreto

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 duecento a settecento quote.**

In relazione alla commissione del delitto di cui all'art. 629, comma terzo, del codice penale si applica all'ente **la sanzione pecuniaria da trecento a ottocento quote**

In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e 635-*quater.1* del codice penale, si applica all'ente **la sanzione pecuniaria sino a quattrocento quote.**

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 Decreto per i casi di frode informatica in danno dello Stato o di altro Ente pubblico e di cui all'art.1,co.11, d.l. 105/2019, si applica all'ente **la sanzione pecuniaria sino a quattrocento quote.**

Nei casi di condanna per uno dei delitti indicati nel superiore n. 1) si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per il delitto indicato nel comma *1-bis* si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni.

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

3. DESTINATARI E PROCESSI AZIENDALI COINVOLTI

La presente parte speciale si riferisce a tutte le attività aziendali svolte tramite l'utilizzo dei Sistemi Informatici aziendali, del servizio di posta elettronica e dell'accesso a Internet.

La presente parte speciale prevede, quindi, che nell'espletamento delle rispettive attività, i soggetti coinvolti nelle predette attività sensibili, siano tenuti al rispetto dei principi di comportamento e delle procedure che regolamentano tale area a rischio.

4. I PRINCIPI GENERALI DI COMPORTAMENTO

La presente parte speciale prevede che nell'espletamento delle rispettive attività, i soggetti coinvolti nelle predette attività sensibili, compresi collaboratori esterni, siano tenuti, al fine di prevenire e

impedire il verificarsi dei reati previsti dagli artt. 24 bis del D. Lgs. 231/01, al rispetto dei seguenti principi di comportamento.

L'espletamento delle attività indicate nella presente parte speciale, è presidiato da specifici protocolli conformi ai requisiti UNI EN ISO 27001:2017, coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001 e del Codice Etico adottati dalla Società.

La presente parte speciale prevede l'espresso divieto a carico dei destinatari di :

– porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra indicate;

– porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra indicate, possano potenzialmente diventarlo.

È inoltre sancito l'espresso obbligo di:

- tenere comportamenti in linea con i principi espressi nel Codice Etico e nel presente Modello Organizzativo;
- rispettare tutte le norme di legge applicabili e le procedure interne adottate;
- inserire un'apposita clausola contrattuale che i Consulenti, i Partner ed i Fornitori devono sottoscrivere in cui dichiarano di essere a conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali);
- 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;
- monitorare periodicamente i programmi software utilizzati ed il numero delle licenze in possesso.

5. - LE AREE A RISCHIO ED I PRESIDI DI CONTROLLO ESISTENTI

Nel presente paragrafo, sono elencate le aree "a rischio reato" identificate nel corso della fase di *risk assessment,* con l'avvertenza che, per ciascuna area, sono altresì indicate:

- le cd. "attività sensibili", ovvero quelle nel cui ambito è effettivamente sussistente il rischio di commissione delle fattispecie delittuose, ed i reati astrattamente ipotizzabili;
- le funzioni aziendali coinvolte, fermo restando che in tutte le aree è ipotizzabile il coinvolgimento dell'Organo Amministrativo, in quanto dotato di poteri gestionali e di rappresentanza sostanziale della Società;
- i controlli vigenti in seno alla Società, ovvero gli strumenti adottati al fine di mitigare il rischio di commissione dei reati.

Area a rischio n. 1: tutte le attività aziendali svolte tramite l'utilizzo dei Sistemi Informatici aziendali, del servizio di posta elettronica e dell'accesso a Internet.

Attività sensibili:

a) gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione;

b) evoluzione della piattaforma tecnologica e applicativa IT;

b) gestione dei flussi di comunicazione elettronici con Enti Pubblici;

c) utilizzo di software e di banche dati;

d) utilizzo di sistemi informatici di gestione e controllo degli adempimenti fiscali e amministrativi.

Procedure specifiche di organizzazione e controllo:

1) individuare e adottare le misure adeguate di sicurezza di natura organizzativa, fisica e logistica,in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o distruzione delle risorse informatiche e che si pongano quale obiettivo quello di:

- tutelare la sicurezza delle informazioni;
- prevedere eventuali controlli di sicurezza specifici per tipologia di asset;
- prevedere eventuali controlli di sicurezza destinati a indirizzare i comportamenti e le azioni operative degli Esponenti Aziendali.

2) rispettare i principi comportamentali posti a presidio del rischio di commissione dei delitti informatici, volti ad assicurare l'osservanza dei seguenti parametri di sicurezza del patrimonio informatico della Società previsti dai principali standard internazionali in tema di sicurezza delle informazioni:

- 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.

In particolare, è vietato:

(a) connettere ai sistemi informatici della Società personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato

(b) 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;

(c) 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;

(d) 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;

(e) ottenere credenziali di accesso a sistemi informatici o telematici aziendali dei clienti o di terze parti con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;

(f) divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

(g) 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;

(h) manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

(i) 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;

(l) acquisire e/o utilizzare prodotti tutelati dal diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;

(m) comunicare a persone non autorizzate, interne o esterne alla Società i controlli implementati

sui sistemi informativi e le modalità con cui sono utilizzati;

(n) 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;

(o) lo spamming come pure ogni azione di risposta al medesimo;

(p) inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi;

(q) utilizzare per finalità diverse da quelle lavorative le risorse informatiche (es. personal computer fissi o portatili) assegnate dalla Società;

(r) alterare documenti elettronici, pubblici o privati, con finalità probatoria.

3) Informare tutti i destinatari eventualmente autorizzati all'utilizzo dei sistemi informatici inordine alla 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;

4) formare i dipendenti, in modo diversificato in ragione dellerispettive 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;

5) sottoscrizione da parte dei dipendenti, nonché degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi, di uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;

6) informazione rivolta ai dipendenti e, in generale, a 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;

7) limitazione degli accessi alle stanze server unicamente al personale autorizzato;

8) protezione, per quanto possibile, di 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;

9) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venire disattivati;

10) impedire l'installazione e l'utilizzo di software non approvati dalla Società e non correlati con l'attività professionale espletata per la stessa;

11) informazione rivolta agli 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;

12) limitazione dell'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;

13) divieto di installazione e di utilizzo, sui sistemi informatici della Società, 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 della Società;

14) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, protezione degli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;

15) previsione di 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;

16) limitazione dell'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;

17) cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;

18) nei rapporti contrattuali con i Fornitori di servizi software e banche dati sviluppati in relazione a specifiche esigenze aziendali, previsione di 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.

Area a rischio n. 2: Gestione degli adempimenti fiscal-tributari

Attività sensibili:

1) installazione, manutenzione, aggiornamento e gestione di *software* di soggetti pubblici utilizzati anche per lo scambio di dati ed informazioni riguardanti tutti gli adempimenti previdenziali ed assistenziali.

Procedure specifiche di organizzazione e controllo:

1) rispetto dei ruoli, compiti e responsabilità definiti dall'organigramma nella gestione di sistemi, strumenti, documenti o dati informatici;

2) formale identificazione dei soggetti deputati alla gestione di sistemi, strumenti, documenti o dati informatici;

3) definizione delle modalità di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi;

4) rivisitazione periodica dei diritti d'accesso degli utenti;

5) accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati;

6) controlli formalizzati sugli accessi atti a presidiare il rischio di accesso non autorizzato alle informazioni, ai sistemi, alle reti e alle applicazioni, nonché atti a prevenire danni ed interferenze ai locali ed ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;

7) segregazione delle funzioni al fine di garantire operativamente la separazione del livello esecutivo da quello approvativo;

8) autenticazione individuale dell'utilizzo di dispositivi hardware e software dedicati per l'implementazione delle politiche di navigazione in internet e scambio delle informazioni (firewall, proxy server, ecc.);

9) meccanismi di protezione per lo scambio di informazioni tramite internet, posta elettronica e dispositivi rimovibili;

10) implementazione di misure di sicurezza atte a garantire l'accesso alle informazioni da parte di terze parti solo previa autorizzazione formale e nel rispetto degli accordi di riservatezza e confidenzialità stipulati;

11) implementazione di ambienti logicamente e fisicamente separati al fine di controllare e testare le modifiche software fino al rilascio in produzione;

12) definizione formale delle modalità di protezione da software pericolosi;

13) definizione formale delle modalità di gestione dei back-up delle informazioni e dei software;

14) formale classificazione delle informazioni e dei sistemi informatici gestiti dalla Società;

15) controlli formalizzati atti a presidiare il rischio di appropriazione e modifica indebita delle informazioni di proprietà della Società con conseguente perdita di autenticità, riservatezza ed integrità dell'asset informativo;

16) definizione delle modalità di custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, ecc.) e previsione di regole di *clear screen* per gli elaboratori utilizzati;

17) definizione delle tempistiche per la chiusura delle sessioni inattive;

18) formale definizione delle modalità operative per l'individuazione e la gestione degli incidenti e dei problemi;

19) verifica periodica di tutti gli incidenti singoli e ricorrenti al fine di individuarne le relative cause;

20) verifica periodica dei trend sugli incidenti e sui problemi al fine di individuare le azioni preventive al verificarsi di problemi in futuro;

21) valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi e che tenga conto della normativa applicabile in materia e dei principi etici della Società;

22) previsione di specifiche attività di formazione ed aggiornamenti periodici sulle procedure di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;

23) obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa per i dipendenti e per i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;

24) tracciabilità di tutte le operazioni effettuate per la gestione dei sistemi, strumenti, documenti o dati informatici utilizzati dalla Società.

6. – I COMPITI 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* D. Lgs. n. 231/2001 sono i seguenti:

- svolgere verifiche sul rispetto della presente Parte Speciale e valutare la loro efficacia a prevenire la commissione dei reati di cui all'art. 24-*bis* del D. Lgs. n. 231/2001. Con riferimento a tale punto l'OdV potrà proporre ai soggetti competenti della Società 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;
- 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);

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

Allo scopo di svolgere i propri compiti l'OdV può accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti, nonché acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

In particolare, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici della presente Parte Speciale ovvero alle procedure aziendali attinenti alle aree sensibili sopra individuate.