SEZIONE D

Delitti informatici e trattamento illecito di dati
Delitti in violazione del diritto d'autore

Art. 24-bis D. Lgs. 231/2001
Legge 633/1941 (art. 25-novies D. Lgs. 231/2001)

Approvazione	Consiglio di Amministrazione del 10/12/2014
Revisioni	……

Art. 24-*bis*.
Delitti informatici e trattamento illecito di dati

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

Art. 25-*novies*.
Delitti in materia di violazione del diritto d'autore (1).

1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a bis), e terzo comma, 171-bis, 171-ter, 171- septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.
2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174- quinquies della citata legge n. 633 del 1941.

(1) Articolo inserito dall'articolo 15, comma 7, lettera c), della legge 23 luglio 2009, n. 99

INDICE

1. Le fattispecie di criminalità informatica e violazione del diritto d'autore previste nel D.lgs. 231/2001

Il D.lgs. 231/01 prevede alcune fattispecie criminose che possono essere realizzate attraverso l'ausilio di sistemi informatici o telematici che, in taluni casi, sono state oggetto di valutazione in altre parti speciali del modello organizzativo.
La Società ha ritenuto opportuno indicare le misure adottate al fine di scongiurare il verificarsi di comportamenti illeciti connessi alla disponibilità di mezzi informatici, in quanto la sicurezza dei sistemi informatici è ritenuta elemento essenziale del sistema di controllo aziendale.
Oltre al reato di frode informatica di cui all'art. 640 *ter* c.p., già considerato nella sezione di parte speciale A, il legislatore ha inserito successivamente ulteriori ipotesi delittuose che qui rilevano nei limiti in cui siano commesse nell'interesse o a vantaggio di Ca.Nova S.p.A.
L'ipotesi che la commissione di talune fattispecie integri il suddetto requisito è un rischio alquanto marginale ma si è ritenuto opportuno inserire una sezione specifica in ragione del fatto che il sistema informatico prevede la gestione di tutti i dati aziendali ed occorre pertanto un corretto utilizzo dello stesso.
L'art. 24-*bis* che prevede i "*Delitti informatici e trattamento illecito di dati*" è stato introdotto dalla Legge n. 48/08, legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, convenzione redatta a Budapest il 23 novembre 2001.
Fondamentale per il corretto inquadramento delle fattispecie di reato contemplate dall'art. 24-*bis* è la definizione di sistema informatico, ovvero ogni sistema di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione di dati su supporti adeguati, per mezzo di impulsi elettronici.
In ragione dell'oggetto della presente sezione si richiama inoltre il reato di cui all'art. 171 *bis* della legge 22 aprile 1941 n. 633 il quale, unitamente ad altre fattispecie criminose, è stato inserito nel D.lgs 231/01 all'art. 25 *novies* che prevede i "*Delitti in materia di violazione del diritto d'autore*".
Infatti, nonostante le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

Si riporta per maggiore chiarezza una breve descrizione delle fattispecie delittuose interessate:

- *Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)*

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico.
Il reato può essere integrato, ad esempio, qualora, una volta ottenuto un finanziamento, venga violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

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

Il reato consiste nell'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza ovvero nella permanenza contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
Pare opportuno evidenziare che il delitto è procedibile d'ufficio solo qualora esso sia stato commesso nella sua forma aggravata, ovvero quando 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 ancora da chi esercita anche abusivamente la professione di

investigatore privato, o con abuso della qualità di operatore del sistema; così come se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; ovvero 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.
I fatti sono procedibili d'ufficio anche qualora 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.

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

La condotta criminosa si realizza attraverso la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o software altrui.
Si precisa che il reato è procedibile a querela della persona offesa, mentre è procedibile d'ufficio se il fatto viene commesso con violenza alla persona o con minaccia, ovvero con abuso della qualità di operatore del sistema.

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

La norma anticipa la tutela considerando integrato il reato da fatti diretti 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, anche qualora dalla condotta posta in essere non derivi la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, che viene considerata una mera circostanza aggravante.

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

Tale ipotesi di reato si configura attraverso la distruzione, il danneggiamento, il rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o l'ostacolarne gravemente il funzionamento attraverso la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi informatici altrui, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi.

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

Tale fattispecie di reato si perfeziona qualora un soggetto, 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.

- *Documenti informatici (art. 491-bis c.p.)*

La norma, richiamata dall'art. 24-*bis* del D. Lgs. 231/01, precisa che se alcuna delle falsità previste dal capo terzo, del titolo settimo, del libro secondo del Codice Penale relativo alla falsità in atti, riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- *Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)*
  "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";

- *Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)*
  "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni";

- *Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)*
  "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";

- *Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)*
  "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";

- *Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)*
  "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";

- *Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)*
  "Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità,
  è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro";

- *Falsità materiale commessa da privato (art. 482 c.p.)*
  "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";

- *Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)*
  "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";

- *Falsità in registri e notificazioni (art. 484 c.p.)*
  "Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00";

- *Falsità in scrittura privata (art. 485 c.p.)*
  "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata";

- *Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.)*
  "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito";

- *Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)*
  "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";

- *Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)*
  "Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private";

- *Uso di atto falso (art. 489 c.p.)*
  "Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno";

- *Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)*
  "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. Si applica la disposizione del capoverso dell'articolo precedente";

- *Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)*
  "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";

- *Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)*
  "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".

- *Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di*

mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis l.633/1941 comma 1);

La norma sanziona la condotta di chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE). La norma disciplina altresì l'ipotesi in cui il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

- *Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171 bis l. 633/1941 comma 2).*

È punito chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati.

- *Duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento - proiezione in pubblico, trasmissione a mezzo della radio o della televisione con qualsiasi procedimento, di videocassette, musicassette, di qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale e' prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Societa' italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato*; *(art. 171 ter 633/1941 comma 1 lett. a, d).*

La norma sanziona la condotta di chi abusivamente duplica, riproduce, trasmette o diffonde o proietta in pubblico videocassette, musicassette,o qualsiasi altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale e' prescritta, l'apposizione di contrassegno da parte della Societa' italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato.

*****

Come evidenziato in premessa non è ravvisabile un rischio neppure residuale di commissione di taluni reati, per la difficoltà di ipotizzare un interesse aziendale esclusivo o concorrente correlato con quello del soggetto agente.

Si tratta dei seguenti delitti di sabotaggio informatico:

- *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)*
- *Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)*
- *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)*
- *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)*

In ragione dell'attività svolta da Ca.Nova S.p.A. si deve escludere altresì la ravvisabilità delle fattispecie di cui agli artt. 171, primo comma, lettera a bis), e terzo comma, 171-ter (ad esclusione delle fattispecie sopra richiamate di cui al primo comma lett. a e d), 171- septies e 171-octies della legge 22 aprile 1941, n. 633.

Sono peraltro da escludere tutte le fattispecie di reato la cui commissione può avvenire solo da parte di Pubblici Ufficiali o di Incaricati di un Pubblico Servizio, poiché i soggetti appartenenti a Ca.Nova S.p.A. non rivestono tale qualifica.

Trattasi dei seguenti delitti:

- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)
- Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)
- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p)

E' infine da escludere la fattispecie di *"Frode informatica del soggetto che presta servizi di certificazione di firma elettronica" (art. 640-quinquies c.p.)* in quanto reato che può essere commesso solamente da soggetto qualificato.

2. Destinatari e obiettivi della "Parte speciale D"

La Parte Speciale D disciplina i comportamenti posti in essere da amministratori, dirigenti e dipendenti di Ca.Nova S.p.A. nell'utilizzo dei sistemi informatici o telematici dell'Azienda.

Nello specifico, la presente Parte Speciale ha lo scopo di:

a) fornire le «regole di comportamento» che gli amministratori, i dirigenti ed i dipendenti, sono tenuti ad osservare ai fini della corretta applicazione del Modello;
b) fornire all'Organismo di Vigilanza, e ai responsabili delle altre funzioni aziendali che cooperano con il medesimo, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

3. Processi sensibili

Le attività nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici e telematici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione (a titolo esemplificativo, si considerino l'area amministrativa, l'area commerciale, l'area di sviluppo e progettazione, l'area personale).
I reati sopra considerati hanno come presupposto la disponibilità di un terminale e la concreta disponibilità di accesso alle postazioni di lavoro; per tale ragione, le aree di attività ritenute più specificamente a rischio ("Aree di Attività a Rischio") sono quelle che comportano l'utilizzo di un personal computer, l'accesso alla posta elettronica, l'utilizzo di programmi informatici e l'accesso a internet.

Le attività sensibili individuate, con riferimento ai Reati Informatici o telematici richiamati nella presente parte speciale, sono le seguenti:

a. Gestione e utilizzo dei sistemi informatici e telematici nonché delle informazioni e dei dati aziendali (c.d. "patrimonio informativo") nel cui ambito sono ricomprese le attività di:

a) protezione dei dati e Politica di sicurezza interna;
b) gestione del profilo utente e del processo di autenticazione;
c) gestione e protezione della postazione di lavoro;
d) gestione degli accessi verso l'esterno;
e) gestione e protezione delle reti;
f) gestione degli output di sistema e dei dispositivi di memorizzazione;
g) sicurezza fisica (es. sicurezza cablaggi, dispositivi di rete);

b. Operatività amministratori di sistema

c. Utilizzo della posta elettronica e delle reti telematiche:

d. Gestione delle autorizzazioni e delle licenze di programmi software e banche dati, monitoraggio e controllo dei software installati.

e. Gestione degli accessi ad opera di terzi

f. Gestione della trasmissione e della proiezione di videocassette, contenuti audio ,o qualsiasi altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive

4. Principi generali di comportamento

Ai fini della prevenzione dei reati sopra indicati, il Modello prevede l'espresso divieto a carico dei destinatari di porre in essere, o concorrere in qualsiasi forma nella realizzazione di comportamenti tali da integrare le fattispecie considerate nella presente Parte Speciale.
A tal fine, Ca.Nova S.p.A. pone, a carico dei destinatari, l'espresso divieto di:

a. alterare documenti informatici o telematici, pubblici o privati, aventi efficacia probatoria
b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati
c. accedere abusivamente al sistema informatico o telematico della Società al fine di alterare o cancellare dati o informazioni
d. accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati
e. 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
f. 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
g. svolgere attività di approvvigionamento, produzione, diffusione di apparecchiature 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
h. svolgere attività di modifica 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

j. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità
k. produrre e trasmettere documenti in formato elettronico con dati falsi o alterati
l. accedere a portali o banche dati di terzi qualora non si sia in legittimo possesso delle credenziali di accesso
m. divulgare, cedere o condividere le proprie credenziali di accesso
n. procedere all'installazione di prodotti *software* in violazione degli accordi contrattuali di licenza d'uso e, in generale, di leggi e regolamenti
o. 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
p. acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui.

Nell'ambito delle suddette regole, è previsto, in particolare, l'obbligo di:

a. comportarsi in conformità alle norme di legge, di regolamento, alle procedure aziendali esistenti in ogni attività che comportino l'utilizzo di un terminale e l'accesso a sistemi informatici. Ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate, che devono essere utilizzate esclusivamente per l'espletamento della propria attività e non possono essere cedute a terzi. Tali risorse devono essere conservate in modo appropriato e Ca.Nova S.p.A. dovrà essere tempestivamente informata di eventuali furti o danneggiamenti
b. ogni dipendente è tenuto alla segnalazione a QUA di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni), che provvederà ad archiviare e mettere a disposizione tutta la documentazione relativa all'incidente, inviandone copia all'OdV
c. impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente
d. dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati
e. osservare rigorosamente tutte le norme poste dalla legge a tutela della Privacy e agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano
f. garantire ed agevolare ogni forma di controllo, svolta nel rispetto dell'art. 4 dello Statuto dei Lavoratori, diretta a impedire la commissione di fattispecie delittuose
g. evitare di introdurre o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente autorizzate
h. evitare di trasferire all'esterno dell'Azienda o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie funzioni
i. evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione di quest'ultimo
j. utilizzare la connessione a reti telematiche o reti dati per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento. L'accesso a reti telematiche o a reti dati dovrà avvenire per ragioni esclusivamente lavorative salva diversa autorizzazione rilasciata dalla funzione competente
   Non è consentito accedere da terminali, in qualsiasi modo legati all'attività lavorativa svolta per la Società, a materiale vietato dalla legge (ad es. contenuti pedopornografici) o che possa costituire pericolo per la sicurezza della rete informatica o telematica.
k. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche

l. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa
m. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software
n. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni
o. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda
p. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici e telematici
q. provvedere alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale.

Tutti sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

5. Procedure specifiche

Ca.Nova S.p.A. ha predisposto appositi presidi organizzativi di controllo e si è dotata di adeguate soluzioni di sicurezza, nel rispetto della normativa sulla privacy, per prevenire e controllare i rischi in tema di tecnologia dell'informazione, a tutela del proprio patrimonio informativo e dei dati personali dei soggetti interessati.
Le misure di sicurezza adottate ricomprendono in particolare, la previsione di *password*, ovvero codici di accesso nominativi o numerici, la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico.
È altresì regolamentata la rigorosa custodia delle credenziali di accesso alle postazioni di lavoro, un sistema di controllo degli accessi alle banche dati, la sensibilizzazione del personale e una protezione *antivirus*.

Ulteriori misure da adottare per ridurre le minacce all'integrità e alla riservatezza dei sistemi informatici possono essere:
- limitazioni dell'accesso al computer o ai dati che vengono comunicati, elaborati o stampati;
- misure per valutare l'affidabilità delle persone impiegate nello sviluppo e nella gestione dei sistemi computerizzati;
- controlli che mirano a segnalare tentativi di uso non autorizzato del sistema;
- interventi finalizzati ad assicurare la ripartizione delle responsabilità in maniera da ridurre al massimo le minacce derivanti da un esercizio dei poteri non autorizzato.

a. Gestione e utilizzo dei sistemi informatici e telematici nonché delle informazioni e dei dati aziendali (c.d. "patrimonio informativo")

Le misure di sicurezza adottate ricomprendono, anche con particolare attenzione all'accesso a programmi riservati:
- la previsione di *firewall* e di *password*, ovvero codici di accesso riservati nominativi o numerici, la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico;
- la rigorosa custodia delle credenziali di accesso alle postazioni di lavoro;
- la previsione di screensaver che consentano il blocco automatico delle postazioni qualora non vengano utilizzate per un determinato periodo;
- un sistema di controllo degli accessi alle banche dati;
- la sensibilizzazione delle funzioni coinvolte segnalando la 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;
- la previsione di un'attività di formazione e addestramento volta a diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

- una protezione antivirus

Si vedano le procedure EDP – 01- PR “Utilizzo dei sistemi informatici” e PER-03-PR “Selezione e assunzione risorse umane”.

b. Operatività degli amministratori di sistema

L’abilitazione per la connessione ad Internet e il servizio di posta elettronica vengono gestiti dall’Amministratore di Sistema o da altra figura tecnicamente competente a cui sono assegnate la responsabilità del corretto funzionamento degli strumenti elettronici, del monitoraggio costante dei livelli dei sistemi al fine di garantire la massima efficienza, della storicizzazione dei processi, della realizzazione e conservazione delle copie di backup, nonché di assicurare l’assistenza tecnica e formativa degli utenti.

c. Utilizzo della posta elettronica e delle reti telematiche

La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell’ambito dell’attività lavorativa.
Si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati da Ca.Nova S.p.A. per le comunicazioni personali.
Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale:
“*Ai sensi della normativa sulla Privacy, il contenuto del presente messaggio e dei relativi allegati ha natura strettamente personale ed è riservato al solo destinatario. L'eventuale lettura, comunicazione o diffusione non autorizzate del contenuto del messaggio violerebbero pertanto i diritti dei soggetti interessati. In caso di erronea ricezione siete pregati di informarci con sollecitudine*”.
Nel caso in cui il dipendente non presti più la sua attività lavorativa presso la Ca.Nova S.p.A., la casella di posta elettronica sarà prontamente disattivata. Se per esigenze lavorative sorge la necessità di accedere al contenuto di tale casella di posta, il responsabile della struttura organizzativa a cui il dipendente è assegnato potrà inoltrare motivata richiesta all’amministratore di sistema e al dirigente di riferimento.
Qualora si verifichino anomalie nell’invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l’amministratore di sistema.

La rete internet può e deve essere utilizzata dal dipendente a supporto all’attività lavorativa.
Al fine di ridurre il rischio di un utilizzo improprio di internet, quale ad esempio il caricamento o lo scaricamento di documenti non attinenti con l’attività lavorativa, la visione di siti internet non pertinenti con l’attività svolta, il collegamento a reti o forum comunque estranei alle mansioni del dipendente, e allo stesso tempo al fine di evitare per quanto possibile controlli che potrebbero comportare il trattamento di dati personali, anche non pertinenti, sensibili e giudiziari, sono di seguito evidenziati i principi che devono essere rispettati e le misure che Ca.Nova S.p.A. si riserva di adottare:
- rispetto della normativa vigente in materia di protezione di diritti di proprietà intellettuale nell’acquisizione, riproduzione, condivisione di immagini, di musica, filmati, software;
- utilizzo di sistemi e filtri che possono prevenire determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui è concesso l’accesso e categorie di siti cui non è concesso l’acceso (“black lists”), in quanto non correlati con la prestazione lavorativa;
- conservazione dei log di connessione dei dipendenti per finalità di accertamento e repressione dei reati nel rispetto di quanto previsto dalla normativa vigente.

Si invita comunque il dipendente a utilizzare internet nel rispetto delle leggi vigenti e prestando particolare cautela al fine di non importare virus, spam o altri programmi informatici danno.

d. Gestione delle autorizzazioni e delle licenze di programmi software e banche dati

Ca.Nova S.p.A. si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, l'Azienda si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che hanno causato danno all'Azienda, che ledono diritti di terzi o che , comunque, sono illegittime.

Inoltre, si rammenta che, conformemente a quanto previsto dal Documento Programmatico sulla sicurezza e in osservanza della vigente normativa, i dati relativi all'utilizzo della posta elettronica e di internet sono conservati per periodi di tempo strettamente limitati, secondo le modalità e le tempistiche indicate nello stesso Documento Programmatico.

e. Gestione degli accessi ad opera di terzi

In relazione alle eventuali attività di manutenzione da remoto ai PC delle segreterie connessi ad internet, il personale tecnico autorizzato da Ca.Nova S.p.A. potrà utilizzare specifici software. Tali programmi verranno utilizzati per assistere l'utente durante la normale attività informatica ovvero di svolgere manutenzione su applicazioni e su hardware. L'attività di assistenza e manutenzione avverrà previa autorizzazione telefonica da parte dell'utente interessato. La configurazione del software da utilizzare per gli interventi da remoto, prevedranno un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al PC.

f. Gestione della trasmissione e dela proiezione di videocassette, contenuti audio ,o qualsiasi altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive

Si veda la procedura PAV.04.PR "Gestione Amministrativa Veicoli" che riporta nello specifico le modalità di pagamento periodico degli oneri SIAE per gli autobus di noleggio dotati di dispositivi audiovisivi.

6. Compiti e poteri dell'OdV

Il sistema di controllo predisposto da Ca.Nova S.p.A. prevede la supervisione ad opera dell'Organismo di Vigilanza, soggetto istituzionalmente preposto alla verifica dell'idoneità ed efficacia del modello.

L'OdV, pertanto, effettua periodicamente specifici controlli sulle attività connesse ai "processi sensibili" al fine di verificare il rispetto dei Principi Generali di comportamento e delle istruzioni operative come sopra indicate.

E' stata all'uopo redatta specifica procedura che regolamenta i flussi informativi nei confronti dell'OdV, al fine di fornire allo stesso le informazioni necessarie per l'espletamento dell'attività di verifica e controllo (*Procedura "Flussi informativi nei confronti dell'OdV"*).

In ogni caso all'OdV vengono garantiti autonomi poteri di iniziativa e controllo e potrà avere accesso in qualunque momento a tutta la documentazione aziendale ritenuta rilevante.

Nell'ambito dei propri poteri potrà indire, a sua discrezione, riunioni specifiche con i soggetti deputati alla gestione dei "processi sensibili" e potrà attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello.

L'inosservanza dei principi e delle istruzioni previste nella presente parte speciale è passibile di sanzione disciplinare secondo quanto indicato nella parte generale alla sezione "Sistema disciplinare".