2024

Modello di Organizzazione, gestione e controllo

Parte Integrativa 5

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Approvata dal Consiglio di amministrazione del 26 febbraio 2024

INDICE

Parte Integrativa 5

Pag.

1. LE FATTISPECIE DI REATO PRESUPPOSTO DI RESPONSABILITÀ PER L'ENTE PREVISTE DALL'ART. 24 *BIS* D.LGS. 8 GIUGNO 2001 N. 231.

L'art. 24 *bis* D.Lgs. 8 giugno 2001 n. 231 prevede 11 fattispecie di reato che costituiscono presupposto di responsabilità per l'Ente.

Tenuto conto della natura di Finaosta S.p.A., delle attività dalla stessa svolte e dei presidi attualmente in essere, si ritengono sussistere **rischi trascurabili riguardo la possibile integrazione, nell'interesse o a vantaggio della Società, delle seguenti fattispecie**:

- **Detenzione, diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'art. 615 *quinquies* c.p.,** a norma del quale *"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, 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 sino a euro 10.329".*
- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche di cui all'art. 617 *quater* c.p.,** a norma del quale "*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.*
  Salvo che il fatto costituisca più grave reato la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
  I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
  Tuttavia, si procede d'ufficio e la pena è della reclusione da 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;*
     da chi esercita, anche abusivamente, la professione di investigatore privato.
- **Detenzione, diffusione ed installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche di cui all'art. 617 *quinquies* c.p.**, a norma del quale "*Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*
  La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617 quater".

Il rispetto delle disposizioni di cui al Codice Etico adottato dalla Società e dei principi generali di comportamento indicati nel prosieguo risultano presidi sufficienti a limitare i remoti rischi rilevati.

I delitti che, seguono, invece, si ritengono astrattamente configurabili, con profili di interesse o vantaggio per la Società, nell'ambito delle attività svolte da Finaosta S.p.A.

Per tutte il livello di rischio rilevato, tenuto conto dei presidi in essere, è basso.

Di seguito viene fornita una breve illustrazione dei contenuti delle disposizioni normative; nel capitolo che segue vengono individuati i processi sensibili e le Funzioni coinvolte nell'ambito delle attività

della Società mentre negli ultimi due capitoli vengono individuati i principi generali, i presidi interni e le regole specifiche di comportamento funzionali a rendere accettabile il livello di rischio residuo.

Fattispecie astrattamente configurabili nell'ambito delle attività svolte da Finaosta S.p.A.:

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

"*Se alcuna delle falsità previste dal presente capo 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, posta a tutela della fede pubblica, è stata introdotta al fine di assicurare una sanzione penale alle diverse forme di falso informatico aventi ad oggetto dati registrati nella memoria di un elaboratore o in un supporto informatico ad esso esterno ovvero dati che, in fase di trasmissione tra due elaboratori, non siano registrati su alcun supporto.

Anziché creare una o più fattispecie a sé stanti, il Legislatore ha ricondotto il falso informatico alle norme sulle falsità in atti già esistenti, stabilendo l'espressa equiparazione del documento informatico agli atti pubblici ed alle scritture private cui ciascuna di quelle norme fa, di volta in volta, riferimento.

L'equiparazione opera con riferimento alle seguenti disposizioni:

- falsità materiale commessa dal Pubblico Ufficiale in atti pubblici (art. 476 c.p.);
- falsità materiale commessa dal Pubblico Ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.);
- falsità materiale commessa dal Pubblico Ufficiale in copie autentiche di atti pubblici o privati ed in attestati del contenuto di atti (art. 478 c.p.);
- falsità ideologica commessa dal Pubblico Ufficiale in atti pubblici (art. 479 c.p.);
- falsità ideologica commessa dal Pubblico Ufficiale in certificati o in autorizzazioni amministrative (art. 480 c.p.);
- falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.);
- falsità materiale commessa da un privato (art. 482 c.p.);
- falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.);
- falsità in registri e notificazioni (art. 484 c.p.);
- falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.);
- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.);
- Uso di atto falso (art. 489 c.p.);
- Soppressione, distruzione o occultamento di atti veri (art. 490 c.p.);
- Falsità in testamento olografo, cambiale o titoli di credito (art. 491 c.p.).

Tutte le suddette ipotesi sono astrattamente rilevanti con riferimento a Finaosta S.p.A. posto che, nell'ambito della stessa, chi svolge funzioni di Responsabile Unico di Progetto (RUP) ai sensi del D.Lgs. 31 marzo 2023 n. 36 assume, nell'esercizio delle stesse, la qualifica di Pubblico Ufficiale[1] mentre i dipendenti quando svolgono attività strumentali per conto del Socio pubblico Regione Autonoma Valle d'Aosta, si qualificano come incaricati di un pubblico servizio.

La definizione di "***documento informatico***" si rinviene all'art. 1 del D.Lgs. 7 marzo 2005, n. 82, c.d. *Codice dell'Amministrazione Digitale* a norma del quale lo stesso consiste nella *rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti*.

Perché la falsità del documento informatico assuma rilevanza penale ai sensi dell'art. 491 *bis* c.p. occorre che lo stesso sia dotato di efficacia probatoria.

[1] In tal senso si è espressa l'ANAC nell'ambito delle Linee Guida n. 3 di attuazione del D.Lgs. 18 aprile 2016 n. 50 recanti "*nomina, ruolo e compiti del Responsabile Unico del Procedimento per l'affidamento di appalti e concessioni*", indicazione confermata nell'ambito dei Piani Nazionali 2019 e 2022. La valutazione non cambia a seguito dell'entrata in vigore del D.Lgs. 31 marzo 2023 n. 36.

Occorre pertanto distinguere tra:

- Documenti informatici privi di sottoscrizione: gli stessi hanno una valenza probatoria incerta e costituiscono piena prova riguardo ai fatti ed alle cose in esso rappresentati soltanto nell'ipotesi in cui colui nei confronti del quale vengono prodotti non ne disconosca la conformità. Al riguardo, ad esempio, il Giudice per l'Udienza preliminare presso il Tribunale di Brescia, con sentenza n. 348 dell'11 marzo 2008, ha escluso la configurabilità del reato di falso in atto pubblico con riferimento ad un messaggio di posta elettronica "semplice" ritenendo che lo stesso non possa fornire certezza riguardo la provenienza e l'identità del sottoscrittore. Al documento privo di sottoscrizione è assimilato, ai sensi dell'art. 21 comma 3 Codice dell'Amministrazione Digitale, il documento informatico sottoscritto con firma elettronica qualificata basato su un certificato revocato, scaduto o sospeso.
- Documento informatico sottoscritto con firma elettronica semplice di cui all'art. 1 lett. q) del Codice dell'Amministrazione Digitale che, ai sensi dell'art. 21 del medesimo Codice, "sul piano probatorio è liberamente valutabile in giudizio tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e modificabilità". Detto documento, in concreto, potrà quindi essere dotato di rilevanza probatoria come non esserlo.
- Documento informatico sottoscritto con firma elettronica qualificata, avanzata o digitale di cui all'art. 1 lett. q) *bis*, lettera r) e lettera s) del Codice dell'Amministrazione Digitale che soddisfa il requisito della forma scritta, risulta riconducibile al titolare fino a prova contraria ed ha il valore probatorio di cui all'art. 2702 c.c.

Il reato di falso ideologico di documento informatico pubblico è stato riconosciuto integrato, ad esempio, in ipotesi di inserimento di dati relativi al superamento di esami mai sostenuti nell'ambito di un supporto informatico con funzione vicaria dell'archivio dell'Università[2]. È stato riconosciuto integrato, invece, il reato di falsità materiale di documento informatico pubblico in ipotesi di falsificazione di atti contenuti nei supporti del sistema informatico di un Ente pubblico (in particolare nell'ambito di un caso di alterazione del contenuto di un referto medico conservato nel sistema informatico di un Ospedale)[3].

I delitti di falso richiamati dall'art. 491 *bis* c.p. sono puniti a titolo di dolo generico, ravvisabile nella coscienza e nella volontà di immutare il vero mediante una falsa rappresentazione della realtà.

b) Accesso Abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.):

"*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da 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"

La norma è posta a tutela della riservatezza dei dati e dei programmi contenuti in un sistema informatico.

[2] Cass. Pen. Sez. V, 15 aprile 2008, udienza 6 marzo 2008, n. 15535.

[3] Cass. Pen. Sez. VI, 23 febbraio 2009, udienza 16 gennaio 2009, n. 7752.

Per "***sistema informatico***" deve intendersi qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compie l'elaborazione automatica di dati[4].

Un sistema informatico può ravvisarsi tanto in un *computer* quanto in ogni dispositivo di elaborazione elettronica, magnetica, ottica o similare di dati.

Il sistema informatico assume la denominazione di "*sistema telematico*" nel caso in cui l'elaboratore sia collegato a distanza con altri elaboratori attraverso sistemi di telecomunicazione. Nonostante il Legislatore abbia voluto separare le due definizioni non vi è dubbio che i "sistemi telematici" siano ricompresi nella generale definizione di "sistemi informatici".

Attraverso l'art. 615 *ter* c.p. si reprimono l'accesso e la permanenza abusivi nel sistema informatico altrui in quanto tipicamente pericolosi per la riservatezza dei dati e dei programmi che vi sono contenuti.

Per essere penalmente rilevante, l'indebita intromissione o permanenza deve riguardare un sistema informatico o telematico "protetto da misure di sicurezza" per tali intendendosi tutte le protezioni al cui superamento è possibile subordinare l'accesso ai dati ed ai programmi contenuti nel sistema (ad esempio una *password* da digitare sulla tastiera ovvero un codice di accesso alfanumerico memorizzato sulla banda magnetica di una tessera da introdurre in un apposito lettore).

Ai fini dell'integrazione del reato, tuttavia, non è necessario che l'accesso abusivo sia stato conseguito attraverso un aggiramento di tali misure; la norma, infatti, trova applicazione anche nel caso in cui l'introduzione si verifichi in una situazione di temporanea disattivazione delle stesse (ad esempio in quanto in corso di manutenzione) di cui l'agente sia a conoscenza ovvero nell'ipotesi, come si vedrà, di permanenza in sistema informatico altrui contro la volontà del titolare a fronte di un'introduzione inizialmente legittima o casuale.

Si ha "*introduzione*" in un sistema informatico o telematico protetto allorché si siano superate le barriere che presidiano l'accesso alla memoria interna del sistema e si sia quindi in condizione di poter richiamare i dati ed i programmi che vi sono contenuti; in questo momento, infatti, si realizza quella situazione di pericolo per la riservatezza dei dati e dei programmi che giustifica l'intervento della sanzione penale.

L'introduzione può avvenire sia "da lontano", per via elettronica servendosi di altro elaboratore, sia "da vicino" da parte di chi si trovi a diretto contatto con l'elaboratore ove sono custoditi i dati o i programmi di interesse.

Sussisteranno quindi gli estremi del reato di accesso abusivo ad un sistema informatico sia nel caso in cui, ad esempio, un dipendente della Società si introduca nel sistema informatico di Finaosta S.p.A., di Aosta Factor S.p.A. (credenziali in possesso di determinati dipendenti di Finaosta S.p.A. nell'esercizio dell'attività di direzione e coordinamento come meglio precisato nel prosieguo), di un fornitore della stessa o, ancora, di Banca d'Italia alla cui vigilanza la Società è soggetta in assenza di autorizzazione, sia nell'ipotesi in cui – approfittando della qualità di utente legittimato ad accedere ad uno dei citati sistemi – si introduca in settori della memoria interna o partizioni del *server* cui non è abilitato ad accedere tramite le credenziali d'accesso che gli sono state fornite (superando quindi le misure di sicurezza a tutela di dette partizioni del *server*/della memoria).

L'introduzione deve essere abusiva, vale a dire non accompagnata dal consenso di colui il quale, titolare dei dati e dei programmi immagazzinati nel sistema o comunque garante della loro riservatezza, ha il potere di attribuire la legittimazione dell'accesso.

Oltre all'introduzione abusiva il reato di cui all'art. 615 *ter* punisce anche l'ipotesi del "*mantenimento*" in un sistema protetto contro la volontà, espressa o tacita, del titolare dei dati o dei programmi ivi contenuti.

Il reato risulterà pertanto integrato nell'ipotesi in cui l'agente permanga in un sistema informatico altrui a seguito di un'introduzione casuale ovvero inizialmente autorizzata e nonostante il dissenso di colui che ha interesse alla riservatezza dei dati e dei programmi ivi contenuti.

[4] Secondo la definizione fornita dalla Convenzione di Budapest sulla criminalità informatica ratificata dall'Italia mediante la Legge n. 48 del 2008.

Recentemente le Sezioni Unite della Corte di Cassazione (con sentenza del 18 maggio 2017, ricorrente Savarese) hanno ritenuto integrato il reato di accesso abusivo ad un sistema informatico (nell'ipotesi aggravata di cui al comma 2 n. 1, fatto commesso da un Pubblico Ufficiale o da un Incaricato di un pubblico servizio) nel caso di un soggetto, abilitato ad accedere ad un sistema informatico, il quale si era mantenuto all'interno dello stesso per ragioni ontologicamente estranee o comunque diverse da quelle per le quali gli era stata attribuita la facoltà di accesso[15].

Il secondo comma della disposizione prevede tre circostanze aggravanti.

La circostanza di cui al n. 1 potrebbe assumere rilevanza nel caso in cui il reato venisse commesso da un dipendente della Società con la qualifica di Incaricato di Pubblico Servizio e Pubblico Ufficiale; circostanza rilevante per Finaosta S.p.A. sia con riferimento ai dipendenti chiamati a svolgere attività strumentali per conto del Socio Regione Autonoma Valle d'Aosta (i quali assumono, nell'esercizio di tali funzioni, la qualifica di incaricati di un pubblico servizio) sia con riferimento a chi svolge funzioni di Responsabile di Progetto (RUP).

La circostanza di cui al n. 3 si riferisce all'eventualità che dall'accesso abusivo sia derivato il danneggiamento del sistema nel suo complesso o di singole sue componenti.

Ricadono nell'ambito di tale circostanza tutte quelle ipotesi in cui il danneggiamento sia una conseguenza dell'accesso abusivo e non il mezzo necessario o agevolatore per realizzarlo, nel qual caso troverà applicazione la circostanza di cui al n. 2.

Dovrà trattarsi altresì di una conseguenza non voluta, essendo altrimenti applicabile la norma sul danneggiamento informatico di cui all'art. 635 *bis* c.p. in concorso con quella di accesso abusivo.

Il reato è punito a titolo di dolo generico, ravvisabile nella coscienza e volontà di introdursi o mantenersi nella memoria interna di un elaboratore in assenza del consenso del titolare dei dati ivi contenuti e con la consapevolezza che quest'ultimo ha predisposto delle misure per proteggere detti dati.

Lo scopo perseguito dall'agente nel commettere l'accesso o la permanenza abusivi è irrilevante.

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

"*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.*

La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui al quarto comma dell'art. 617 quater*".*

Attraverso tale disposizione il Legislatore ha inteso rafforzare la tutela della riservatezza dei dati e dei programmi contenuti in un elaboratore (già assicurata dall'incriminazione delle condotte di accesso e di permanenza abusivi di cui all'art. 615 *ter* c.p.) reprimendo una serie di condotte prodromiche alla possibile realizzazione dell'accesso abusivo.

In particolare, la norma vieta di procurare a sé o ad altri, abusivamente, "*codici, parole chiave o altri mezzi idonei all'accesso*" ad un sistema informatico che sia protetto da misure di sicurezza nonché di fornire "*indicazioni o istruzioni idonee al predetto scopo*".

Oggetto della condotta può essere innanzitutto il "*codice di accesso*" o la "*password*" che consentono l'accesso ai dati ed ai programmi contenuti nella memoria interna.

Più in generale può trattarsi di "*qualsiasi mezzo idoneo all'accesso*" come, ad esempio, una chiave che consenta l'accensione dell'elaboratore o una scheda magnetica, da introdursi in un apposito lettore, sulla quale sono registrati i dati che legittimano l'utente all'accesso.

[5] Orientamento ormai consolidato e confermato, ad esempio, dalla recente sentenza della V Sezione Penale, n. 8541 del 27 febbraio 2019.

La giurisprudenza[6] ha applicato tale fattispecie di reato anche all'ipotesi di indebita acquisizione/diffusione di codici di accesso a conti correnti bancari o postali, a condizione che l'accesso al sistema informatico per la gestione *on–line* del conto, realizzabile tramite detti codici, consenta non solo di effettuare operazioni economiche, ma anche di acquisire informazioni relative al conto stesso (quali il saldo disponibile, i movimenti del mese, ecc.).

Oltre agli strumenti logici (come una *password*) e fisici che consentono direttamente l'accesso ad un sistema informatico protetto, la norma menziona anche le "*indicazioni o istruzioni idonee al predetto scopo*", vale a dire le informazioni sul modo di eludere o neutralizzare le misure che proteggono il sistema altrui dagli accessi non autorizzati.

Diversamente da quanto indicato nella rubrica, la norma non punisce la detenzione dei codici di accesso (o strumenti simili) da parte di chi non sia autorizzato a farne uso, ma soltanto:

- l'*acquisizione* (che consiste nel procurarseli, in qualsiasi modo, anche mediante autonoma elaborazione);
- la *detenzione*;
- la *riproduzione* (effettuando una o più copie);
- la *diffusione* (consistente nel rendere disponibile un codice di accesso ad un numero indeterminato di soggetti);
- la *comunicazione* (consistente nel rendere disponibile un codice di accesso ad una cerchia determinata di persone);
- la *consegna* (che diversamente dalla comunicazione e dalla diffusione può riguardare solo cose materiali, quali una scheda magnetica o la chiave che consente l'accesso ad un *computer*) di tali strumenti.

Il reato è punito, al tempo stesso, a titolo di dolo generico – consistente nella volontà di procurarsi, riprodurre, diffondere, comunicare o consegnare codici, parole chiave o mezzi similari che si sa essere idonei a consentire l'accesso ad un sistema informatico protetto ovvero di fornire indicazioni o istruzioni utili per conseguire tale accesso – e di dolo specifico, individuabile nel fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.

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

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

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

La norma è volta a tutelare dati e programmi, vale a dire le componenti immateriali di un sistema informatico.

Per "*dati*" si intendono quelle rappresentazioni di informazioni o concetti che, essendo destinate all'elaborazione da parte di un *computer*, sono codificate in una forma (elettronica, ottica o similare) non percettibile visivamente.

Suscettibili di danneggiamento informatico possono essere dati e programmi immagazzinati nella memoria interna dell'elaboratore, su un supporto esterno come un disco magnetico o una chiavetta *usb*, ovvero memorizzati sulla banda magnetica di una carta di pagamento.

Non rileva il contenuto dei dati oggetto di aggressione: può trattarsi anche di dati personali, ossia di dati contenenti informazioni su una determinata persona fisica, giuridica, Ente o Associazione.

L'art. 635 *bis* c.p. richiede, ai fini dell'integrazione del reato di danneggiamento informatico, che i beni oggetto di aggressione siano "*altrui*"; l'altruità deve essere valutata con riferimento all'esistenza o meno di un interesse all'integrità dei dati in capo ad una persona diversa dall'aggressore.

Di conseguenza il reato potrà essere integrato anche dal soggetto, proprietario di dati registrati, con il proprio consenso, su un supporto altrui, il quale distrugga detto supporto.

La norma prevede diverse ipotesi di "danneggiamento":

[6] In particolare, la pronuncia del G.I.P. presso il Tribunale di Milano del 28 luglio 2006, D.M., pubblicata sulla rivista *D. Internet* 2007, pag. 62.

- la distruzione: rilevante con riferimento ai supporti fisici su cui siano incorporati i dati ed i programmi e consistente nel completo annientamento del bene nella sua funzione strumentale di soddisfacimento delle esigenze di chi ha diritti su di esso;
- il deterioramento: non avendo i dati ed i programmi una consistenza fisica, il loro deterioramento consiste in un'apprezzabile diminuzione del loro valore e della loro utilizzabilità che, pur non risolvendosi nella distruzione o nella cancellazione, ne pregiudichi ugualmente l'essenza (ossia le caratteristiche intrinseche) e non soltanto la funzionalità;
- la cancellazione: trattasi dell'ipotesi più frequente di distruzione di dati e programmi. La stessa può essere conseguenza, ad esempio, di un comando impartito all'elaboratore in cui siano immagazzinati (attraverso, ad esempio, l'utilizzo dell'apposito comando "cancella"), dell'inserimento di un *virus* predisposto a cancellare i dati immagazzinati nell'elaboratore, della smagnetizzazione del supporto, della sostituzione con nuovi dati contenutisticamente diversi. Non si ha cancellazione penalmente rilevante nell'ipotesi in cui i dati siano recuperabili in qualche zona della memoria dell'elaboratore o qualora la vittima possegga una copia di riserva dati o dei programmi cancellati (purché la stessa sia immediatamente disponibile e consenta di rimpiazzare i dati con facilità ed in brevissimo tempo);
- l'alterazione: nell'ipotesi in cui dati e programmi vengano modificati in maniera tale da renderne impossibile il normale utilizzo per un lasso di tempo apprezzabile (ad esempio in caso di conversione dei dati o dei programmi in un linguaggio cifrato di cui la vittima non sia a conoscenza ovvero in caso di sovvertimento di uno schedario elettronico);
- la soppressione: nell'ipotesi in cui i dati o i programmi vengano sottratti alla disponibilità dell'avente diritto con mezzi diversi dalla materiale distruzione o cancellazione, purché gli stessi vengano resi irreperibili nella loro materialità ovvero ne venga impedita la lettura attraverso manipolazioni che li rendano definitivamente illeggibili.

Il reato è punibile a titolo di dolo generico, ravvisabile nella volontà di distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici con la consapevolezza che si tratti di beni altrui, ossia di beni la cui integrità costituisce oggetto di un altrui interesse di protezione.

e) 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.):

"*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".

La norma è volta a tutelare l'integrità di dati, informazioni e programmi di rilevante importanza pubblica e prevede, per tali beni, una tutela rafforzata rispetto a quella apprestata dall'art. 635 *bis* c.p., tramite sanzioni più elevate e la punibilità anche della mera predisposizione di atti idonei alla distruzione, al deterioramento, alla cancellazione, all'alterazione o alla soppressione degli stessi.

I beni informatici tutelati dal presente reato si distinguono da quelli tutelati dall'art. 635 *bis* c.p. per essere di pubblica utilità, vale a dire posti a servizio di una collettività indifferenziata di persone ovvero utilizzati dallo Stato o da altro Ente pubblico.

È indifferente che i beni oggetto di danneggiamento appartengano a privati o a Enti pubblici, in quanto la norma predispone una tutela ampia per dati e programmi che siano in qualsiasi modo utilizzati per finalità pubbliche.

La mancata previsione del requisito dell'altruità fa ritenere che il reato possa essere commesso anche dal proprietario dell'oggetto del danneggiamento in considerazione della funzione sociale dell'oggetto del danneggiamento.

Il secondo comma dell'art. 635 *ter* c.p. prevede una pena più grave nell'ipotesi in cui l'azione sia giunta a compimento ed il danneggiamento si sia effettivamente verificato.

Il reato è punito a titolo di dolo generico, ravvisabile nella volontà di distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici accompagnata dalla

consapevolezza del fatto che si tratta di beni di pubblica utilità ovvero utilizzati dallo Stato o da altro Ente pubblico.

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

"*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 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".

La norma integra la tutela dei "beni informatici" approntata dall'art. 635 *bis* c.p. punendo le condotte che comportino un pregiudizio per il funzionamento dei sistemi informatici nel loro complesso.

Per "*sistema informatico*" deve intendersi qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compie l'elaborazione automatica di dati[7].

Un sistema informatico può ravvisarsi tanto in un *computer* quanto in ogni dispositivo di elaborazione elettronica, magnetica, ottica o similare di dati.

Il sistema informatico assume la denominazione di "*sistema telematico*" nel caso in cui l'elaboratore sia collegato a distanza con altri elaboratori attraverso sistemi di telecomunicazione. Nonostante il Legislatore abbia voluto separare le due definizioni non vi è dubbio che i "sistemi telematici" siano ricompresi nella generale definizione di "sistemi informatici".

Costituisce sistema informatico rilevante ai sensi della fattispecie anche la carta di pagamento a microprocessore (non la carta a banda magnetica).

L'art. 635 *quater* c.p. richiede, ai fini dell'integrazione del reato di danneggiamento di sistemi informatici o telematici, che i beni oggetto di aggressione siano "*altrui*"; l'altruità deve essere valutata con riferimento all'esistenza o meno di un interesse all'integrità del sistema informatico in capo ad una persona diversa dall'aggressore.

Il Legislatore ha predeterminato le condotte di aggressione ad un sistema informatico penalmente rilevanti identificandole nella distruzione, nel deterioramento, nella cancellazione nell'alterazione e nella soppressione di informazioni, dati o programmi nonchè, infine, nella introduzione o trasmissione di dati.

L'ipotesi di aggressione mediante il "*danneggiamento di programmi informatici*", ed in particolare mediante la loro cancellazione, pare essere la più rilevante; ad essa è riconducibile la cancellazione di programmi necessari al funzionamento del sistema, come i programmi facenti parte del c.d. sistema operativo, in assenza dei quali l'elaboratore non è in grado di svolgere alcuna operazione, e la cancellazione di programmi applicativi che, pur non interrompendo del tutto il funzionamento del sistema, lo rendano inutilizzabile allo scopo cui è preposto.

Si ha "*danneggiamento dei dati*" nell'ipotesi di cancellazione di quei *file* che, pur non essendo programmi eseguibili, sono comunque indispensabili al funzionamento dell'elaboratore.

Ricorre l'ipotesi dell'introduzione della "*introduzione*" nel caso di installazione all'interno del sistema informatico di programmi *virus* o c.d. *worm* (la cui peculiarità consiste nella capacità di riprodursi incessantemente all'interno della memoria dell'elaboratore in cui vengono inseriti causando il rallentamento o l'arresto delle normali funzioni del sistema, per il progressivo esaurimento della capacità di memoria).

L'ipotesi della "*trasmissione*" ricorre invece nel caso di aggressione al sistema informatico realizzata attraverso reti di comunicazione, senza un contatto diretto con l'elaboratore (ad esempio nel caso di invio di un programma *virus* attraverso la posta elettronica).

Ai fini dell'integrazione del reato di cui all'art. 635 *quater* c.p. è necessario che le condotte appena elencate abbiano portato alla distruzione, all'inservibilità, al danneggiamento o all'ostacolo al funzionamento del sistema informatico.

Mentre la distruzione di un sistema informatico, da intendersi come eliminazione materiale, pare di difficile realizzazione, di maggiore rilevanza pare il concetto di "*inservibilità totale o parziale*" dello stesso.

---

[7] Secondo la definizione fornita dalla Convenzione di Budapest sulla criminalità informatica ratificata dall'Italia mediante la Legge n. 48 del 2008.

Si avrà inservibilità ogniqualvolta l'intervento aggressivo porti al malfunzionamento del sistema o di una sua parte.

Affinché il pregiudizio arrecato alla funzione strumentale del sistema informatico assuma rilevanza penale è necessario che l'impossibilità di utilizzare, in tutto o in parte, il sistema informatico si protragga per un lasso di tempo apprezzabile ovvero che il ripristino della funzionalità originaria del sistema richieda spese non irrilevanti.

Per "*danneggiamento*" deve intendersi il deterioramento del sistema, vale a dire la diminuzione del suo valore nelle ipotesi in cui questa non si accompagni alla distruzione o all'inservibilità.

L'evento dannoso del "*serio ostacolo al funzionamento*" costituisce una formula di chiusura con la quale si rendono penalmente rilevanti tutte le condotte di aggressione al sistema diverse dalle precedenti; a tale ipotesi può ricondursi, ad esempio, il caso dei c.d. *denial of service*, vale a dire attacchi realizzati mediante l'invio al sistema di un numero elevato di richieste, tale da sopraffare le capacità di elaborazione o di comunicazione.

Il reato è punito a titolo di dolo generico, ravvisabile nella volontà di distruggere, danneggiare, rendere inservibili sistemi informatici ovvero ostacolarne gravemente il funzionamento con la consapevolezza che si tratti di beni altrui.

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

"*Se il fatto di cui all'art. 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".

La norma è volta a tutelare l'integrità di sistemi informatici e telematici di rilevante importanza pubblica e prevede, per tali beni, una tutela rafforzata rispetto a quella apprestata dall'art. 635 *quater* c.p., prevedendo la punibilità anche della mera predisposizione di atti idonei alla distruzione, al danneggiamento, all'inservibilità, totale o parziale, o al grave ostacolo al funzionamento degli stessi.

La disposizione prevede poi, al secondo comma, un aumento di pena nell'ipotesi in cui l'azione sia giunta a compimento ed i suddetti eventi si siano effettivamente verificati.

La condotta punita dalla norma consiste nel compimento di atti idonei e diretti al danneggiamento di un sistema informatico di pubblica utilità.

L'oggetto della condotta (sistemi informatici o telematici), le modalità di aggressione e gli eventi dannosi previsti sono gli stessi previsti dal reato di cui all'art. 635 *quater* c.p. appena trattato e cui si rimanda per la loro interpretazione.

I sistemi oggetto dell'attività aggressiva possono essere esclusivamente quelli di *pubblica utilità*, vale a dire messi al servizio di una collettività indifferenziata di persone. Gli stessi possono appartenere indifferentemente a privati o ad Enti pubblici. Non rilevano, ai fini dell'integrazione del reato, gli atti che, pur finalizzati al danneggiamento, non siano idonei al raggiungimento dello scopo.

Il reato è punito a titolo di dolo generico, ravvisabile nella volontà di distruggere, danneggiare, rendere inservibili i sistemi o ostacolarne gravemente il funzionamento con la consapevolezza che si tratta di sistemi di pubblica utilità.

2. PROCESSI SENSIBILI E FUNZIONI COINVOLTE NELL'AMBITO DELLE ATTIVITÀ SVOLTE DA FINAOSTA S.P.A.

Il Sistema Informativo di Finaosta S.p.A. è schematizzabile in:

- **infrastruttura tecnologica interna**: costituita dalla LAN di Sede (*server*, *personal computer*, *hub*, *switch*, *router*, gruppi di continuità, cablaggi, ecc), da tutte le informazioni residenti sugli elaboratori presenti presso la Società e dalle applicazioni in uso;
- **Utenti**: utilizzatori delle funzioni e delle applicazioni.

La struttura prevede la presenza di un presidio organizzativo interno, il Servizio Sistemi Informativi, chiamato a svolgere attività di coordinamento e gestione del Sistema Informativo e di sicurezza dei dati.

Prima di procedere con l'individuazione dei processi sensibili si evidenzia ancora si che Finaosta S.p.A. ha:

1. designato un Responsabile della Protezione Dati (DPO) esterno ai sensi degli articoli 37 – 39 del Regolamento (UE) 2016/679;
2. adottato una Politica aziendale in materia di c.d. *disaster recovery*;
3. adottato una procedura per la gestione di eventuali perdite o indisponibilità di dati (c.d. *Data breach*);
4. Individuato e designato gli Amministratori di Sistema disciplinandone ruolo e funzioni nell'ambito di apposita procedura;
5. Adottato una procedura di *Change Management* riferita agli applicativi gestiti dal Servizio Sistemi Informativi;
6. Adottato una procedura per la gestione delle credenziali e dei profili di accesso degli utenti;
7. Adottato una procedura in materia di gestione del sistema informativo aziendale;
8. Adottato una procedura in materia di *backup Restore*.

Quanto sopra consente di limitare i rischi di integrazione delle fattispecie di reato presupposto di responsabilità per l'Ente indicate nel capitolo che precede. In ogni caso, all'esito dell'attività di analisi funzionali alla stesura del presente documento, i processi ritenuti potenzialmente a rischio di integrazione dei reati di cui agli artt. art. 491 *bis*, 615 *ter*, 615 *quater*, 635 *bis*, 635 *ter*, 635 *quater* e 635 *quinquies* c.p. nell'ambito delle attività svolte da Finaosta S.p.A. sono risultati essere i seguenti:

a) Gestione operativa dei sistemi informativi aziendali (sistemi di rete, applicazioni, postazioni di lavoro e *device mobili*)

Attività sensibili:

- Gestione del patrimonio informativo;
- Attribuzione Conti ed autorizzazioni;
- Gestione processo di *change management* del gestionale aziendale;
- Manutenzione dei *server* della Società;
- Gestione dei *software* applicativi installati;
- Utilizzo dei *computer* ed in generale degli strumenti informatici di proprietà di Finaosta S.p.A.;
- Gestione delle credenziali di accesso al *server*, ai PC ed agli strumenti informatici;
- Utilizzo della posta elettronica aziendale;
- Utilizzo della rete *internet* e dei relativi servizi;
- Accesso ai gestionali.

Nell'ambito di tali attività si profila un rischio, potenziale, di integrazione di diversi reati previsti dalla presente Parte Speciale, tra cui quelli di accesso abusivo ad un sistema informatico, di

danneggiamento di dati o documenti ovvero di danneggiamento di sistemi informatici nell'ipotesi in cui esponenti della Società dovessero:

- cancellare o alterare informazioni a valenza probatoria presenti nel sistema informatico allo scopo di eliminare le prove di un altro reato o illecito;
- cancellare o alterare dati rilevanti ai fini della formazione del bilancio;
- validare una prestazione mai ricevuta al fine di permettere il pagamento della relativa fattura (operazione inesistente a fini, ad esempio, corruttivi);
- diffondere all'interno del sistema informatico un *virus* idoneo a danneggiarne o ad interromperne il funzionamento al fine di distruggere/alterare documenti rilevanti nell'ambito di un'indagine penale;
- accedere abusivamente a partizioni non accessibili al fine di commettere uno degli atti di cui sopra.

Funzioni coinvolte:

- Servizio Sistemi Informativi (gestione patrimonio informativo, manutenzione dei *server* della Società, attribuzione conti, gestione credenziali di accesso al *server* ed agli strumenti informatici, gestione dei *software* applicativi installati, utilizzo dei computer e degli strumenti informatici di proprietà di Finaosta S.p.A., utilizzo posta elettronica, utilizzo rete *internet* e relativi servizi);
- Componenti il Consiglio di Amministrazione (gestione patrimonio informativo, gestione credenziali di accesso al *server* ed agli strumenti informatici qualora rilasciate, utilizzo posta elettronica);
- Direzione Generale, Direzione Operativa, tutte le Aree, i Servizi, gli Uffici di cui all'Organigramma nonché *Chief Risk Officer*, Funzione Antiriciclaggio e Funzione *Risk Management (*gestione patrimonio informativo, gestione credenziali di accesso al *server* ed agli strumenti informatici, gestione dei *software* applicativi installati, utilizzo dei computer e degli strumenti informatici di proprietà di Finaosta S.p.A., utilizzo posta elettronica, utilizzo rete *internet* e relativi servizi)

b) Elaborazione e gestione di documenti informatici:

Attività sensibili:

- elaborazione buste paga, cedolini, modello CU, ecc. e trasmissione della stessa ai dipendenti;
- elaborazione e gestione della documentazione relativa alle procedure di gara d'appalto gestite telematicamente tramite *software* o portali informatici *ad hoc* secondo quanto previsto dal D.Lgs. 31 marzo 2023 n. 36

Nell'ambito di tali attività si ravvisa un rischio, potenziale, di integrazione dei reati di falsificazione di un documento informatico avente efficacia probatoria al fine di procurare a sé o ad altri un vantaggio in ipotesi di alterazione dei dati trasmessi ai dipendenti ovvero di dati o documenti informatici di cui alle procedure di rilevanza pubblica.

Funzioni coinvolte:

- Direzione Amministrazione Personale e Acquisti, Ufficio Amministrazione del Personale (quanto all'elaborazione buste paga, cedolini, modello CU, ecc.);

- Responsabile Unico di Progetto (Direttore Generale o la persona di volta in volta nominata) ovvero chiunque svolga funzioni di RUP nell'ambito di una procedura di rilevanza pubblica (con riferimento alla gestione della relativa documentazione);
- Amministratori di Sistema (designati nell'ambito del Servizio Sistemi Informativi).

c) Gestione dei rapporti con Banca d'Italia.

Attività sensibili:

- Accesso al portale *Infostat – UIF* al fine di procedere alla comunicazione delle operazioni registrate nell'Archivio Unico Informatico ed alla segnalazione di Operazioni Sospette;
- Accesso alla Centrale dei Rischi per effettuare le segnalazioni periodiche previste dalla normativa di riferimento (segnalazione mensile antiriciclaggio aggregata SARA, basi segnaletiche 3 – 4 – YF – COREP/Q2 – LGD e 7, eventuali ulteriori segnalazioni richieste dall'Autorità).

L'accesso al portale *Infostat – UIF* ed alla Centrale dei Rischi è limitato ai soggetti abilitati e dotati di credenziali di accesso (*username* e *password*) ovvero a soggetti appositamente delegati.

Nell'ambito delle attività sopra indicate si profila un rischio, potenziale, di integrazione dei reati di falso ideologico o materiale di documento informatico da parte del privato o di uso di atto informatico falso (nell'ipotesi in cui, ad esempio, venissero comunicati all'UIF o alla Centrale Rischi dati falsi ovvero inviati come allegati documenti contraffatti a fronte di un vantaggio per Finaosta S.p.A.); di accesso abusivo ad un sistema informatico (nell'ipotesi in cui, ad esempio, l'accesso avvenga da parte di un utente non abilitato ovvero non delegato secondo la procedura prevista da parte di Banca d'Italia, oppure da parte di un soggetto abilitato il quale si trattenga per svolgere attività ontologicamente diverse rispetto a quelle per cui è stato autorizzato nell'interesse o a vantaggio di Finaosta S.p.A.), di diffusione abusiva di codici d'accesso (nell'ipotesi, remota e di fatto quasi solo teorica, in cui, ad esempio, le credenziali dell'utente autorizzato di Finaosta S.p.A. venissero cedute a terzi a fronte di un corrispettivo per la Società).

Può ravvisarsi altresì un rischio potenziale di integrazione dei reati di danneggiamento di dati o documenti ovvero di danneggiamento di sistemi informatici nell'ipotesi in cui l'utente abilitato dovesse porre in essere condotte aggressive avverso i suddetti beni (ad esempio inviando a Banca d'Italia programmi *virus* o *worm* al fine di eliminare dati precedentemente inviati ovvero di coprire il mancato adempimento di un obbligo gravante sulla Società).

Funzioni coinvolte:

- Funzione Antiriciclaggio (quanto all'invio delle comunicazioni alla Centrale dei Rischi, alla verifica di corretta trasmissione dei dati nell'Archivio Standardizzato ed all'invio delle segnalazioni SARA);
- *Chief Risk Officer* (quanto alla segnalazione di Operazioni sospette);
- Amministratori di Sistema (Servizio Sistemi Informativi).

d) Gestione dell'Archivio Standardizzato:

Attività sensibili:

- Utilizzo del *software* per la gestione dell'Archivio Standardizzato:

  a) Inserimento nuove registrazioni in archivio Unico provvisorio;
  b) Correzione scritture in anomalia in ambiente AUI provvisorio (senza necessità di rettifica);

c) Correzione – mediante rettifica – delle scritture passate nell'Archivio Unico Definitivo;
d) Verifica dei tracciati dei diagnostici effettuati;
e) Monitoraggio attività svolta dagli Utenti.

Un apposito modulo predisposto dal *software* in base ai dati inseriti dall'Utente produce il flusso SARA da inviare all'UIF.

L'accesso al programma è limitato agli utenti abilitati, dotati di *Username* e *password*.

Nell'ambito di tale attività si profila un rischio, potenziale, di integrazione del reato di accesso abusivo ad un sistema informatico (nell'ipotesi in cui, ad esempio, l'accesso avvenga da parte di un utente non abilitato ovvero da parte di un soggetto abilitato il quale si trattenga per svolgere attività ontologicamente diverse rispetto a quelle per cui è stato autorizzato nell'interesse o a vantaggio di Finaosta S.p.A.), di diffusione abusiva di codici d'accesso (nell'ipotesi, remota e di fatto quasi meramente teorica, in cui, ad esempio, le credenziali dell'utente autorizzato di Finaosta S.p.A. venissero cedute a terzi a fronte di un corrispettivo per la Società), del reato di falso ideologico o materiale di documento informatico da parte del privato o di uso di atto informatico falso (nell'ipotesi in cui, ad esempio, venissero inseriti nell'Archivio Unico dati falsi o allegati documenti contraffatti a fronte di un vantaggio o di un interesse di Finaosta S.p.A.).

Può ravvisarsi altresì un rischio potenziale di integrazione dei reati di danneggiamento di dati o documenti ovvero di danneggiamento di sistemi informatici nell'ipotesi in cui l'utente abilitato dovesse porre in essere condotte aggressive avverso i suddetti beni programmi *virus* o *worm* al fine di eliminare dati precedentemente inviati ovvero di coprire il mancato adempimento di un obbligo gravante sulla Società).

Funzioni coinvolte:

- Funzione Antiriciclaggio
- Amministratori di Sistema (Servizio Sistemi Informativi).

e) Accesso agli applicativi di Aosta Factor S.p.A. nell'esercizio delle attività di direzione e coordinamento:

Attività sensibili:

- Possibilità di accesso ai sistemi informativi di Aosta Factor S.p.A.

Nell'ambito di tali attività si profila un rischio, potenziale, di integrazione del reato di accesso abusivo ad un sistema informatico (nell'ipotesi in cui, ad esempio, l'accesso avvenga da parte di un utente non abilitato ovvero da parte di un soggetto abilitato il quale si trattenga per svolgere attività ontologicamente diverse rispetto a quelle per cui è stato autorizzato nell'interesse o a vantaggio di Finaosta S.p.A.), di diffusione abusiva di codici d'accesso (nell'ipotesi in cui, ad esempio, le credenziali dell'utente autorizzato di Finaosta S.p.A. venissero cedute a terzi a fronte di un corrispettivo per la Società) nonché dei reati di danneggiamento di dati o documenti ovvero di danneggiamento di sistemi informatici nell'ipotesi in cui l'utente abilitato dovesse:

- cancellare o alterare informazioni a valenza probatoria presenti nel sistema informatico allo scopo di eliminare le prove di un altro reato o illecito nell'interesse di Finaosta S.p.A. quale Capogruppo;
- cancellare o alterare dati rilevanti ai fini della formazione del bilancio nell'interesse di Finaosta S.p.A. quale Capogruppo;
- validare una prestazione mai ricevuta al fine di permettere il pagamento della relativa fattura (operazione inesistente a fini, ad esempio, corruttivi);

- diffondere all'interno del sistema informatico della controllata un *virus* idoneo a danneggiarne o ad interromperne il funzionamento al fine di distruggere/alterare documenti rilevanti nell'ambito di un'indagine penale;
- accedere abusivamente a partizioni non accessibili al fine di commettere uno degli atti di cui sopra.

Funzioni coinvolte:

- Amministratori di Sistema (Servizio Sistemi Informativi)
- Tutti gli esponenti di Finaosta S.p.A. abilitati all'accesso al sistema informatico di Aosta Factor S.p.A. (elenco tenuto dal Servizio Sistemi Informativi cui si rimanda)

3. PRINCIPI GENERALI DI COMPORTAMENTO:

I seguenti divieti di carattere generale si applicano in via diretta a tutti i destinatari del presente Modello di organizzazione, gestione e controllo compresi i soggetti terzi individuati secondo quanto indicato nell'ambito della parte generale.

A tutti i suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti che, singolarmente o cumulativamente, integrino, direttamente o indirettamente, le fattispecie di cui agli artt. 491 *bis*, 615 *ter*, 615 *quater*, 615 *quinquies*, 617 *quater*, 617 *quinquies*, 635 *bis*, 635 *ter*, 635 *quater* e 635 *quinquies* c.p.

In particolare, coerentemente con le procedure di sicurezza del sistema informativo di Finaosta S.p.A., sono adottate le seguenti misure:

- l'accesso alle informazioni che risiedono sui server e sulle banche dati aziendali, ivi inclusi i *client*, è limitato da strumenti di autenticazione;
- gli Amministratori di sistema e gli addetti alla manutenzione sono muniti di credenziali di autenticazione;
- I log di accesso ai sistemi di elaborazione ed agli archivi elettronici effettuati dagli Amministratori di Sistema sono conservati per 6 mesi; decorso tale periodo vengono definitivamente cancellati;
- Il Servizio Sistemi Informativi deve provvedere a catalogare tutte le macchine informatiche presenti, evidenziando il *software* caricato, l'eventuale data di scadenza delle singole licenze e la persona autorizzata all'utilizzo. Tale documento deve essere costantemente aggiornato, con indicazione della data dell'ultimo aggiornamento e della firma di chi lo ha redatto. Il documento dovrà essere trasmesso all'Organismo di Vigilanza a semplice richiesta, al fine di consentire la verifica della corrispondenza tra i programmi dichiarati, quelli effettivamente caricati su PC, le rispettive licenze e le persone che hanno diritto di utilizzo;
- il personale dipendente è munito di univoche credenziali di autenticazione per l'accesso ai *client*;
- l'accesso alle applicazioni da parte del personale è garantito attraverso strumenti di autorizzazione;
- tutti i *server* e i *laptop* aziendali sono aggiornati periodicamente sulla base delle specifiche necessità;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (*firewall* e *proxy*);
- i dispositivi telematici di instradamento sono collocati in aree dedicate e protetti al fine di renderli accessibili al solo personale autorizzato;
- il personale deve astenersi dal diffondere le informazioni ricevute dalla Società per l'uso dei mezzi informatici aziendali e l'accesso a dati, sistemi e applicazioni aziendali;
- il personale deve attuare i comportamenti richiesti dalla Società e necessari per proteggere il sistema informativo, diretti ad evitare che terzi possano accedervi in caso di allontanamento dalla postazione di lavoro;
- il personale deve accedere al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla modifica periodica;
- il personale deve astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui;
- il personale deve conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi che in tal modo potrebbero accedere abusivamente a dati aziendali riservati.

È fatto divieto di:

- installare programmi senza aver preventivamente informato il Servizio Sistemi Informativi, preposto alla gestione della sicurezza informatica;
- utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa;
- porre in essere condotte finalizzate ad alterare o falsificare documenti informatici;

- accedere abusivamente a sistemi informatici o telematici, detenere, diffondere e utilizzare abusivamente codici di accesso a sistemi informatici e telematici, intercettare, impedire, danneggiare e interrompere illecitamente comunicazioni informatiche verso e tra soggetti terzi, danneggiare dati, programmi informatici o telematici di proprietà di soggetti terzi e quelli utilizzati dallo Stato da enti pubblici o comunque di pubblica utilità. installare apparecchiature che potrebbero intercettare, danneggiare e interrompere comunicazioni informatiche e telematiche verso e tra terzi.

  I soggetti coinvolti devono adempiere alle disposizioni di legge e dei regolamenti vigenti e in particolare, al fine di evitare comportamenti illeciti da parte degli utilizzatori dei sistemi informatici e telematici, **devono**:
- attuare procedure di controllo;
- effettuare ricognizioni sistematiche sull'attività informatica e telematica aziendale e sui programmi informatici utilizzati;
- informare prontamente il Responsabile della protezione dei dati ("DPO"), gli Amministratori di Sistema e l'Organismo di Vigilanza laddove vengano a conoscenza di un trattamento illecito di dati o di altre situazioni o condotte, anche di terzi, che violino le regole di comportamento sopra indicate.

4. REGOLE SPECIFICHE DI COMPORTAMENTO.

Attribuzione dei conti

- L'attribuzione dei diritti e dei conti (utente o amministratore) deve rispettare il principio del privilegio minimo: un conto dispone esclusivamente dei diritti strettamente necessari al suo utilizzo (personale) o al suo funzionamento (processi).
- L'attribuzione dei conti è riservata al personale ed ai processi che ne hanno strettamente bisogno.
- La trasmissione del nome utente e della *password* iniziale avviene attraverso dei canali diversi.
- La trasmissione della *password* iniziale deve avvenire per mezzo di un canale sicuro (ad esempio una *mail* criptata).
- È necessario che i processi di gestione degli accessi separino con chiarezza i ruoli di:
    - richiedente (persona che richiede il diritto);
    - validatore (persona che conferma la necessità di attribuire il diritto richiesto).
    - controllore (persona che verifica periodicamente i diritti degli utenti).

Gestione degli ID

- Gli ID sono una parte fondamentale della gestione dei conti e dei diritti di accesso. In tal senso, la loro gestione non deve essere trascurata, soprattutto quella dei conti condivisi.
- Gli accessi al Sistema Informatico di Finaosta S.p.A. sono, qualora ciò sia tecnicamente possibile:
    - individuali e non condivisi: un conto deve essere collegato a una sola persona o a un solo processo automatico di tipo *webservice*, *script*, ecc.
    - nominali: un conto deve disporre di una denominazione chiara che permetta di individuare la persona o il processo dietro l'utilizzo di tale conto.
- Quando non sia possibile definire per un'applicazione o una risorsa un conto che rispetti i principi definiti sopra (conto individuale e nominale), deve essere richiesta una deroga per la creazione di un conto condiviso. Tale deroga deve essere giustificata e validata.

Gestione delle autenticazioni

- A ciascun conto che può accedere al Sistema Informatico deve essere associata una credenziale (quale per esempio una *password*);
- L'insieme delle abilitazioni alle risorse del sistema informativo attribuite ad un utente costiuisce il profilo di accesso di quest'ultimo.
- Ciascuna *password* deve avere una durata di vita massima.
- Un conto utente deve essere temporaneamente bloccato dopo 10 tentativi falliti di accesso con *password*.
- I privilegi di accesso devono prevedere diversi livelli di abilitazione quali:
    - *Full*: accesso alla risorsa con privilegi di Amministratore;
    - *Input*: accesso con privilegio di lettura, modifica e cancellazione dei dati;
    - *Input* condizionato: accesso con privilegio di lettura, modifica e cancellazione dei dati sulla base di una specifica condizione quale l'appartenenza ad un'Area o un Servizio;
    - *Read*: accesso in sola lettura
    - Disabilitato: nessuna possibilità di acceso.
- Con cadenza annuale il Servizio Sistemi Informativi effettua un'elaborazione volta a verificare la congruità dei privilegi assegnati ad un operatore secondo il principio del minimo privilegio.
- Ogni responsabile di un'unità organizzativa ha a disposizione un *report* relativo ai privilegi di accesso alle risorse assegnate all'Unità organizzativa medesima;
- Detto report contiene l'elenco dei profili di accesso a ciascuna risorsa censita con evidenza di eventuali situazioni di incongruità (quali l'accesso ad una risorsa da parte di operatori non

appartenenti all'Unità organizzativa) al fine di consentire a ciascun responsabile di formulare eventuali proposte di intervento.

Gestione del *server* e delle dotazioni informatiche dei dipendenti:

- Ogni postazione di lavoro (*hardware*) messa a disposizione dei propri dipendenti da Finaosta S.p.A., la strumentazione informatica ed il complesso delle applicazioni e dei programmi che la Società installa sulla medesima (*software*) sono di proprietà esclusiva di Finaosta S.p.A.
- I dipendenti sono responsabili del corretto utilizzo delle apparecchiature *hardware* e *software* assegnate. Gli stessi sono tenuti a custodirle in modo appropriato e dare tempestiva comunicazione all'Amministratore di Sistema, al Direttore Generale ed al Responsabile della Protezione Dati di eventuali furti, danneggiamenti, smarrimenti o indisponibilità dei dati.
- Tanto l'*hardware* quanto i programmi *software* sono esclusivamente strumenti di lavoro e debbono essere utilizzati secondo questa unica finalità.
- La navigazione *internet* e l'utilizzo della posta elettronica sono possibili mediante accesso con un codice identificativo (*account*) al quale l'utente stesso deve associare una componente riservata (*password*). La *password* è nota al solo utente, ma consente all'*account* l'accesso o la creazione di ambienti condivisi eventualmente con altri utenti e certamente con l'Amministratore di Sistema.
- Il Dipendente si impegna:
    - a non scrivere/appuntare le credenziali di accesso su alcun supporto, a memorizzarle o, eventualmente, conservarle in luogo separato e non accessibile a terzi (compresi altri dipendenti della Società);
    - a non procedere al salvataggio automatico delle stesse;
    - a modificarle con regolarità ed in ogni caso entro il 90° giorno di validità;
    - ad utilizzare *password* alfanumeriche con lunghezza minima individuata dalla "*Politica Sistema Informativo*" non riconducibili in alcun modo al di lui nome ovvero al nome di propri famigliari, al numero di telefono o ad ogni altra informazione allo stesso facilmente riconducibile;
    - a non utilizzare *password* corrispondenti a parole presenti in un dizionario (italiano o di lingue straniere) neppure in senso inverso;
    - a non utilizzare credenziali di accesso utilizzate, in tutto o in parte, per altri *account*;
    - a comunicare immediatamente all'Amministratore di sistema l'eventuale furto, smarrimento, perdita o appropriazione a qualsivoglia titolo da parte di terzi delle credenziali d'accesso;
    - a non utilizzare le credenziali d'accesso per scopi diversi rispetto a quelli inerenti la gestione dell'*account* attribuitogli (ed in particolare *social network*, *forum* o qualsivoglia attività non riconducibile a Finaosta S.p.A.).
    - A non modificare le impostazioni di blocco schermo della postazione assegnata.
    - A segnalare all'Amministratore di Sistema ogni anomalia, errore, tentativo di violazione o illecito riscontrato.
- Finaosta S.p.A. ha facoltà procedere alla disattivazione delle credenziali di accesso:
    - decorsi 6 mesi senza che le stesse vengano utilizzate;
    - qualora l'Utente perda la qualità che gli consentiva di accedere al Sistema Informatico;
    - qualora vengano accertati:
        a) un uso non corretto - ovvero estraneo all'attività lavorativa - del sistema o degli strumenti informatici da parte dell'Utente;
        b) manomissioni e/o interventi sull'*hardware* e/o sul *software*;
        c) la diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di *password*, procedure di connessione, indirizzo IP ed altre informazioni tecniche riservate;

d) l'accesso doloso dell'utente a *directory*, a siti e/o *file* e/o servizi cui lo stesso non è autorizzato ad accedere.

- il contenuto dei messaggi di posta elettronica (*mail*), come pure i *file* agli stessi allegati nonché le eventuali estensioni sono considerati documenti di lavoro e di proprietà di Finaosta S.p.A.;
- Tanto l'*account* quanto la *password* possono essere in qualunque momento disattivati dall'Amministratore di Sistema.
- I Dipendenti non possono installare sul *computer*, sugli strumenti informatici o sui *server* accentrati alcun tipo di programma o applicazione, salvo esplicita autorizzazione della Direzione Generale ovvero dell'Amministratore di Sistema; l'installazione non autorizzata di programmi e applicazioni aumenta notevolmente il rischio di introdurre nei sistemi informatici aziendali programmi dannosi e auto replicanti (*virus*) e può alterare la stabilità delle applicazioni del *personal computer* e dei *server*.
- I Dipendenti non possono utilizzare programmi non distribuiti o autorizzati dalla Società tramite l'Amministratore di Sistema o la Direzione Generale.
- I Dipendenti non possono duplicare programmi, *file* e applicazioni residenti sul personal *computer* o sui *server*; parimenti non è consentito un utilizzo personale degli stessi.
- I Dipendenti non possono utilizzare strumenti *software* e/o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
- I Dipendenti non possono modificare le configurazioni impostate sul proprio *personal computer* o sugli strumenti informatici in dotazione salvo esplicita autorizzazione dell'Amministratore di Sistema.
- I Dipendenti non possono installare alcun sistema di comunicazione personale.
- I Dipendenti non possono, anche se i supporti *hardware* e *software* in loro possesso lo consentono, utilizzare i sistemi per l'ascolto di programmi, *file* audio o musicali, ecc, per finalità extra lavorative, personali o illecite, ma solo nell'ambito delle mansioni affidate.
- I *personal computer* portatili e gli altri strumenti informatici utilizzati al di fuori dei locali della Società, non devono essere lasciati incustoditi e l'accesso ai documenti ivi contenuti deve essere subordinato all'inserimento di credenziali di accesso.
- In caso di assenza dalla postazione di lavoro e in caso di allontanamento, anche temporaneo, dalla macchina i dipendenti devono attivare i sistemi di protezione e di blocco.
- Finaosta S.p.A. si riserva la facoltà di procedere alla rimozione dagli archivi di ogni applicazione o programma che riterrà non necessari all'attività lavorativa, anche con modalità automatizzate, ma comunque tali da non consentire in alcun modo di venire a conoscenza della qualità e del contenuto dei file aperti in esecuzione dei medesimi programmi/applicazioni.
- I supporti mobili (CD, DVD, USB, *Floppy*, ecc.), così come i *cloud computing* esterni, rappresentano un potenziale veicolo per l'intrusione di programmi pericolosi, conseguentemente devono essere osservate le seguenti regole:
  - il Dipendente non può utilizzare alcun tipo di supporto mobile o *cloud* non fornito dalla Società, salva esplicita autorizzazione da parte del diretto responsabile;
  - il Dipendente non può scaricare *file* contenuti in supporti magnetici, ottici e *on-line*, non aventi alcuna attinenza con la propria prestazione lavorativa;
  - il Dipendente deve sottoporre al controllo e alla relativa autorizzazione all'utilizzo da parte dell'Amministratore di Sistema i *file* di provenienza incerta;
  - il Dipendente deve custodire i supporti mobili autorizzati con modalità sicure, ponendo particolare attenzione alla custodia delle chiavi *USB*.
- Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi; pertanto, qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
- La Società si riserva la facoltà di procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione della presente procedura.
- Finaosta S.p.A. si riserva la facoltà di procedere alla rimozione dagli archivi di ogni *file* o applicazione che riterrà non necessari all'attività lavorativa.

Utilizzo della posta elettronica

- Per finalità esclusivamente lavorative, la Società può dotare il proprio personale dipendente di una o più caselle di posta elettronica, anche condivise fra componenti del medesimo ufficio o Funzione. Oltre all'utente e/o agli utenti assegnatari, alla casella di posta elettronica ed ai relativi archivi (es. messaggi ricevuti, messaggi inviati) può altresì accedere l'Amministratore di sistema, con proprie credenziali di autenticazione, per le sole finalità di gestione delle caselle stesse e con i limiti previsti dalla normativa sulla protezione dei dati personali.
- La casella di posta elettronica è di proprietà di Finaosta S.p.A. ed all'utente ne è consentito il mero utilizzo per le finalità di cui alla presente procedura; è fatto divieto di utilizzare la casella di posta elettronica per finalità private, personali o comunque non riconducibili all'attività lavorativa.
- In particolare, la casella di posta elettronica è utilizzabile per soli fini riconducibili all'attività della Società o alle mansioni che l'utente svolge all'interno della stessa e pertanto:
    - è vietato utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate e/o per contatti interpersonali tra i dipendenti non inerenti all'uso d'ufficio;
    - è vietato accedere al servizio di posta elettronica *internet* attraverso mezzi (*mobile* o altro) diversi dal collegamento alla rete informatica della Società, salvo diversa abilitazione concessa dall'Amministratore di Sistema;
    - non è consentito l'uso di comunicazioni via *e-mail* che non sfruttino il sistema di posta della Società.
- Il Dipendente non può inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, pertanto, il Dipendente non può inviare ad un indirizzo estraneo alla rete informatica aziendale documenti dal contenuto riservato salva autorizzazione da parte del diretto responsabile.
- Il Dipendente non può utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, *forum* o *mail-list*, ecc., salvo diversa ed esplicita autorizzazione da parte della Direzione.
- Non devono essere aperti i messaggi provenienti da mittenti sconosciuti, oppure conosciuti ma con oggetto non chiaro o tale dal sollevare dubbi sulla loro legittimità. In casi dubbi è necessario contattare il mittente se conosciuto e/o l'Amministrazione di Sistema per le valutazioni del caso.
- I messaggi di posta elettronica devono essere inviati con i formati definiti, non possono essere utilizzati formati personalizzati.
- L'archivio dei messaggi di posta elettronica dei singoli utenti residente sui *server* di posta non deve eccedere la capienza definita dalla Società, la detenzione di archivi personali di maggiore capacità deve essere autorizzata dal Direttore Generale o dall'Amministratore di Sistema. In caso di raggiungimento della massima capienza prevista la Società si riserva la facoltà:
    - di bloccare il caricamento dei nuovi messaggi, eliminandoli automaticamente non appena arrivino, senza aprirli e senza controllarne il mittente;
    - di eliminare dagli archivi residenti sui *server* di posta i messaggi memorizzati, eventualmente copiandoli su supporti mobili.
- È cura dell'utente fare in modo che nessuno abbia ragione o motivo di ritenere che la casella di posta assegnata dalla Società sia o possa essere utilizzata per fini o comunicazioni personali.
- Finaosta S.p.A. riconosce che l'utilizzo della posta elettronica rappresenta in misura sempre maggiore il principale veicolo di informazioni aziendali, sia internamente, sia verso l'esterno; in questo contesto, fermo il divieto di lettura sistematica, occorre apprestare misure organizzative che consentano di far fronte all'eventualità di assenze programmate, improvvise o prolungate del lavoratore al quale sia assegnato l'utilizzo di una casella di posta elettronica.
- In caso di assenza programmata, eccedente i due giorni lavorativi, il lavoratore deve impostare la funzione di risposta automatica della casella di posta elettronica che invia al mittente la comunicazione dell'assenza del destinatario comunicando le coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.
- In caso di assenza non programmata la comunicazione dell'assenza del destinatario e delle coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura, può essere attivata dall'Amministratore di Sistema, indicando come destinatario di

contatto la figura gerarchicamente e immediatamente superiore del lavoratore assente o il sostituto del lavoratore assente, ove nominato, o in modo più generico i recapiti dell'area di appartenenza.

- In caso di cessazione del rapporto di lavoro, l'Amministratore di Sistema provvederà a bloccare la casella di posta elettronica e ad impostare la funzione di risposta automatica che invia al mittente la comunicazione dell'assenza del destinatario, comunicando le coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura, al fine di non interrompere le comunicazioni relative alle attività professionali svolte dal titolare della casella. Conformemente ai principi di necessità, pertinenza e non eccedenza, Finaosta S.p.A. determina in mesi tre il periodo di mantenimento della casella di posta elettronica. Allo scadere del periodo si provvederà alla cancellazione definitiva della stessa.

Navigazione in internet

- Finaosta S.p.A. riconosce che la possibilità di navigare in *internet* può costituire un idoneo mezzo per il reperimento delle informazioni funzionali allo svolgimento dell'attività lavorativa; tuttavia, l'utilizzo imprudente o non necessario di alcuni servizi della rete può esporre la Società ad attacchi informatici o ad un rallentamento della velocità di connessione; per questi motivi di sicurezza e di organizzazione la Società può distinguere tre diversi casi:
    - Livello 1 – personale al quale non è data la possibilità di navigare in *internet*, ma solamente la possibilità di consultare la rete extranet e *intranet*;
    - Livello 2 – personale al quale è consentito navigare in *internet*, con restrizioni in ordine ai siti visitabili ed ai *download* possibili, solo nell'ambito delle mansioni affidate ed in ogni caso non per finalità extra lavorative;
    - Livello 3 – personale al quale è consentito navigare in *internet* senza restrizioni in ordine ai siti visitabili, ma con restrizioni in ordine ai *download* possibili nonché all'accesso ai *social network*; navigazione senza restrizioni, e comunque non per finalità extra lavorative, personali o illecite ma solo nell'ambito delle mansioni affidate.
- La classificazione in ordine al livello 2 viene svolta in relazione a siti di diffusa conoscenza che rappresentino un concreto strumento di arricchimento delle informazioni necessarie per un più agevole svolgimento delle mansioni affidate.
- Le restrizioni di *download* mirano ad evitare che possano essere scaricati, anche inconsapevolmente, *file* portatori di potenziali attacchi informatici o che possano rappresentare uno strumento di violazione della vigente normativa.
- La classificazione e le restrizioni sono determinate dall'Amministratore di Sistema su indicazione della Società.

Misure organizzative per la navigazione internet

- Il Dipendente non può effettuare sul *web* alcun genere di transazione finanziaria, acquisti *on-line* e simili per finalità *extra* lavorative salvo casi espressamente autorizzati. Sono altresì vietate le operazioni personali di *trading-on-line*. Sono ammesse, limitatamente alle urgenze, operazioni personali effettuate tramite *internet banking*.
- Il Dipendente non può scaricare *software* gratuiti (*freeware)* e *shareware* prelevato da siti *internet* se non espressamente autorizzato e previa valutazione da parte dell'Amministratore di Sistema.
- Il Dipendente non può registrarsi a siti i cui contenuti non siano legati all'attività lavorativa.
- Il Dipendente non può partecipare, per motivi non professionali, a *Forum, chat line,* bacheche elettroniche e/o registrarsi in *guest book* anche utilizzando pseudonimi (*nicknames*).
- Il Dipendente non può scaricare *file* non aventi alcuna attinenza con la propria prestazione lavorativa. I *file* di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'Amministratore di Sistema.
- Il Dipendente non può connettersi ad *internet* senza transitare dalla rete aziendale, così come non può collegare alla rete aziendale apparati non autorizzati dall'Amministratore di Sistema. Infatti, una non adeguata tipologia di collegamento espone l'apparato al rischio di attacco da parte di

hacker esterni con la possibilità di causare un punto di accesso alla rete. Restano salve le *Virtual Private Network* (VPN) autorizzate.

Utilizzo applicativi gestionali e banche dati:

- L'accesso agli applicativi gestionali ed alle banche dati da parte dei Dipendenti di Finaosta S.p.A. è subordinato ad espressa autorizzazione che si concretizza attraverso la concessione delle credenziali di accesso.
- Tutti gli utenti, prima di poter utilizzare detti applicativi devono procedere alla funzione di identificazione fornendo al sistema le credenziali di accesso.
- Queste ultime attribuiscono le abilitazioni strettamente necessarie allo svolgimento delle funzioni spettanti al Dipendente.
- I destinatari di credenziali d'accesso ai suddetti ovvero ad ulteriori applicativi gestionali utilizzati da Finaosta S.p.A. sono tenuti a custodirle diligentemente, evitando che altri esponenti della Società ovvero soggetti terzi possano conoscerle.
- L'utilizzo dei *software* perdura per il tempo necessario allo svolgimento delle attività previste dalla licenza o dalla normativa di riferimento.
- Non possono essere effettuate operazioni diverse da quelle previste dalla licenza.
- All'uscita dai programmi deve essere effettuato il *logout*.
- Durante il periodo di utilizzo del *software* non è consentito abbandonare la postazione di lavoro ed in ipotesi di allontanamento occorre effettuare il *logout* dal programma.

Gestione dei rapporti con Banca d'Italia:

- Le credenziali di accesso al portale *Infostat – UIF* ed alla Centrale dei Rischi sono consegnate alle sole funzioni autorizzate alla comunicazione delle operazioni registrate nell'Archivio Unico Informatico, alla segnalazione di operazioni sospette e ad effettuare le segnalazioni periodiche previste dalla normativa di riferimento (segnalazione mensile antiriciclaggio aggregata SARA, basi segnaletiche 3 – 4 – YF – COREP/Q2 – LGD e 7) oltre che al Direttore Generale.
- Gli stessi sono tenuti a custodirle adeguatamente evitando che altri esponenti della Società o soggetti terzi possano conoscerle.
- L'accesso ai portali da parte di persone diverse deve essere espressamente autorizzato da parte del Direttore Generale;
- Il soggetto autorizzato secondo quanto previsto nel punto che precede dovrà altresì ricevere espressa delega se prevista dalle procedure di accesso ai portali (come nel caso di *Infostat – UIF*).
- La permanenza all'interno del portale perdura per il tempo necessario allo svolgimento delle attività che rendono necessario l'accesso.
- Durante la permanenza nel portale non possono essere compiute operazioni diverse da quelle normativamente previste.
- All'uscita dal portale deve sempre essere effettuato il *logout*.
- Durante il periodo di connessione al portale non è consentito abbandonare la postazione di lavoro; in ipotesi di allontanamento occorre uscire dal programma effettuando il *logout*.
- Banca d'Italia procede autonomamente al *backup* dei dati inseriti nel portale; detta operazione si aggiunge a quelle effettuate da Finaosta S.p.A.

Accesso agli applicativi di Aosta Factor S.p.A. nell'esercizio delle attività di direzione e coordinamento.

- L'accesso agli applicativi di Aosta Factor S.p.A. da parte dei Dipendenti di Finaosta S.p.A. è subordinato ad espressa autorizzazione che si concretizza attraverso la concessione delle credenziali di accesso.
- L'elenco del personale in possesso delle credenziali è conservato dal Servizio Sistemi Informativi.
- L'accesso è volto esclusivamente all'esercizio di funzioni di controllo nell'ambito dell'attività di direzione e coordinamento.

- Tutti gli utenti, prima di poter utilizzare detti applicativi devono procedere alla funzione di identificazione fornendo al sistema le credenziali di accesso.
- Queste ultime attribuiscono le abilitazioni strettamente necessarie allo svolgimento delle funzioni attribuite.
- I destinatari di credenziali d'accesso sono tenuti a custodirle diligentemente, evitando che altri esponenti della Società ovvero soggetti terzi possano conoscerle.
- L'accesso ai sistemi informativi di Aosta Factor S.p.A. è limitato al solo periodo di tempo necessario allo svolgimento delle attività di controllo programmate.
- Terminate le attività deve essere effettuato il *logout*.
- Durante il periodo di accesso agli applicativi della controllata non è consentito abbandonare la postazione di lavoro; in ipotesi di allontanamento occorre effettuare il *logout*.