PARTE SPECIALE "B"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Entrata in vigore: delibera CdA D_113_23 del 12.12.2023

INDICE

- B.1 ELENCO DEI REATI-PRESUPPOSTO E "CONSIDERAZIONI SPECIFICHE" SULLA RELATIVA STRUTTURA
- B.2 PRINCIPI GENERALI DI COMPORTAMENTO
- B.3 AREE A RISCHIO E PRINCIPI DI CONTROLLO PREVENTIVO

B.1 ELENCO DEI REATI-PRESUPPOSTO E "CONSIDERAZIONI SPECIFICHE" SULLA RELATIVA STRUTTURA

Articolo *615-ter* del codice penale - Accesso abusivo ad un sistema informatico o telematico.

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.

****

Considerazioni specifiche
Si tratta di un reato comune, che può essere compiuto da chiunque, salva l'aggravante di pena prevista alla lettera *a)* del comma secondo, se il fatto viene commesso da un p.u. o da un i.p.s. Le misure di sicurezza (cui fa riferimento la norma) da cui è protetto il sistema sono sia le c.d. misure logiche (ad esempio, *password*), che le c.d. misure fisiche (armadi chiuse, locali non accessibili a tutti, servizi di controllo e vigilanza). Il reato punisce due diverse condotte: l'introduzione abusiva nel sistema protetto e il mantenersi nello stesso contro la volontà del titolare. A quest'ultimo proposito, va sottolineato che il reato può essere commesso anche da chi, autorizzato all'accesso al sistema per una determinata finalità, non rispetti le condizioni a cui era subordinato l'accesso e lo utilizzi per finalità diverse, abusando dell'autorizzazione concessa.

Art. 615-quater del codice penale – Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, 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 5.164 euro.
La pena è della reclusione da uno a tre anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui al quarto comma dell'articolo 617-quater.

****

CONSIDERAZIONI SPECIFICHE

Si tratta di un reato comune di pericolo in quanto il possesso, la comunicazione o la diffusione abusive di mezzi idonei a superare la protezione di un sistema informatico o telematico (*password*, codici di accesso, altri mezzi atti all'accesso, o, semplicemente, informazioni che consentano di eludere le misure di protezione) comportano il pericolo della commissione di un accesso abusivo a detti sistemi. La fattispecie richiede il dolo specifico di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.

Art. 615-quinquies del codice penale – Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

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.

****

CONSIDERAZIONI SPECIFICHE

Si tratta anche in questo caso di un reato comune di pericolo, in quanto il possesso, la comunicazione, la diffusione, o la messa a disposizione di terzi di apparecchiature, dispositivi o programmi informatici rilevano in quanto posti in essere per uno degli scopi indicati nella disposizione, ovvero di danneggiare anche in parte un sistema informatico o telematico o di favorirne l'interruzione anche parziale o l'alterazione del suo funzionamento. La fattispecie è caratterizzata, dunque, dalla presenza del dolo specifico.

Art. 635-bis del codice penale – Danneggiamento di informazioni, dati e programmi informatici

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

****

CONSIDERAZIONI SPECIFICHE

Si tratta di un reato di evento che reprime l'effettivo danneggiamento di informazioni, dati o programmi informatici altrui. La fattispecie è aggravata quando il danneggiamento è commesso con violenza alla persona o minaccia o quando il fatto sia commesso con abuso della qualità di operatore del sistema.

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

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.

****

CONSIDERAZIONI SPECIFICHE

Si tratta di una ipotesi speciale di danneggiamento informatico, che si applica quando le informazioni, i dati o i programmi informatici sono utilizzati dallo Stato o da altro ente pubblico o sono ad essi pertinenti o comunque di pubblica utilità. La fattispecie è strutturata come delitto aggravato dall'evento: se il danneggiamento si realizza si applica la più grave ipotesi prevista dal secondo comma, mentre, ai fini della configurabilità del delitto di cui al comma primo, è sufficiente l'idoneità della condotta a cagionare il danneggiamento. Si applicano le stesse circostanze aggravanti indicate per il reato di cui all'articolo 635-*bis* c.p.

Art. 635-*quater* del codice penale – Danneggiamento di sistemi informatici o telematici

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Se il fatto è commesso con violenza alla persona o con minaccia o con abuso della qualità di operatore del sistema, la pena è aumentata.

****

CONSIDERAZIONI SPECIFICHE

Si tratta di un reato di evento: si richiede espressamente che il sistema venga danneggiato, reso in tutto o in parte inservibile, ovvero ne venga ostacolato gravemente il funzionamento. La fattispecie sarà integrata laddove il danneggiamento del sistema sia cagionato 1) mediante la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi, o 2) mediante l'introduzione o la trasmissione di dati, informazioni o programmi. La distinzione tra danneggiamento di dati e danneggiamento del sistema è legato alle conseguenze della condotta: quando la soppressione o alterazione di dati, informazioni e programmi renda inutilizzabile, o danneggi gravemente il funzionamento del sistema, ricorrerà la fattispecie di cui al presente articolo. Le circostanze aggravanti sono le stesse indicate per il reato dei cui all'articolo 635-*bis* c.p.

Art. 635-*quinquies* del codice penale – Danneggiamento di sistemi informatici o telematici di pubblica utilità

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

****

CONSIDERAZIONI SPECIFICHE

Si tratta di un reato a consumazione anticipata, analogo al precedente art. 635-*ter*, che riguarda in questo caso il danneggiamento di sistemi informatici o telematici di pubblica utilità. La fattispecie è strutturata come delitto aggravato dall'evento: se il danneggiamento si realizza si applica la più grave ipotesi prevista dal secondo comma, mentre, ai fini della configurabilità del delitto di cui al comma primo, è sufficiente l'idoneità della condotta a cagionare il danneggiamento. Si applicano le stesse circostanze aggravanti indicate per il reato di cui all'articolo 635-*bis* c.p.

Art. 617-quater del codice penale – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

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 tre a otto anni se il fatto è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato.

****

CONSIDERAZIONI SPECIFICHE

La disposizione, unitamente a quello previsto dal successivo articolo 617-*quinquies*, è volta a tutelare la libertà e la riservatezza delle comunicazioni informatiche, intendendosi per tali qualunque scambio di dati tra due o più sistemi informatici. Vi rientrano, quindi, gli scambi di *email*, le *mailing list*, i *forum*, le *chat*, i *newsgroup*, ecc.

Si può parlare di intercettazione abusiva (fraudolenta) quando la comunicazione è riservata ad un determinato numero di destinatari: per le comunicazioni a carattere pubblico (ad esempio siti *web*) non è ipotizzabile alcuna riservatezza.

I reati si verificano quando si prende fraudolentemente cognizione del contenuto di un messaggio in corso di trasmissione, ovvero quando si impedisca o interrompa la comunicazione intercettata (comma 1), ovvero il contenuto della comunicazione venga divulgato al pubblico (comma 2).
I reati sono esclusi se c'è stata autorizzazione esplicita preventiva da parte dei soggetti che partecipano alla comunicazione e perseguibili a querela di parte. Se ricorre una delle circostanze indicate al comma terzo, la perseguibilità è d'ufficio e la pena è aumentata.

Art. 617-*quinquies* del codice penale – Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche
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'articolo 617-quater.

****

CONSIDERAZIONI SPECIFICHE
Si tratta di un reato comune di pericolo che si realizza a fronte di condotte idonee al raggiungimento dello scopo che costituisce oggetto di dolo specifico (intercettazione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedimento o interruzione delle stesse).

D) FALSITA' INFORMATICA

491-*bis* del codice penale – Documenti Informatici
Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici.

****

CONSIDERAZIONI SPECIFICHE
L'articolo ha esteso alle falsità riguardanti un documento informatico le disposizioni in tema di falso in atto pubblico.

B.2 PRINCIPI GENERALI DI COMPORTAMENTO

La presente Parte Speciale, ad integrazione/specificazione di quanto previsto nel Codice Etico del Fondo e/o nelle regole generali di condotta indicate nella Premessa della Parte Speciale del Modello, prevede l'espresso divieto a carico dei Destinatari di porre in essere comportamenti:

- tali da integrare le fattispecie di reato previste dall'art. 24-*bis* del D.Lgs. 231/01, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure del Fondo o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico.

Inoltre, per tutti coloro che operano per conto del Fondo, nelle attività relative all'utilizzo ed alla gestione di sistemi, strumenti, documenti o dati informatici, è fatto divieto in particolare di:

- utilizzare gli strumenti, i dati ed i sistemi informatici e telematici in modo da recare danno a terzi, in particolare interrompendo il funzionamento di un sistema informatico o alterando dati o programmi informatici, anche a seguito dell'accesso abusivo, ovvero dell'intercettazione di comunicazioni;
- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- detenere o diffondere indebitamente codici, programmi, parole chiave o altri mezzi atti all'accesso ad un sistema informatico o telematico di soggetti pubblici o privati, al fine di acquisire informazioni riservate;
- detenere o diffondere indebitamente codici, programmi, parole chiave o altri mezzi atti al danneggiamento informatico;
- alterare o falsificare documenti informatici di qualsiasi natura o utilizzare indebitamente la firma elettronica;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o *software* allo scopo di danneggiare un sistema informatico o telematico di soggetti pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

- porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali e sistemi informatici (in particolare, Codice in materia di protezione dei dati personali; provvedimenti del Garante della Privacy, ecc.).

Pertanto, i Destinatari sono tenuti a:

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

Ai fini dell'attuazione dei comportamenti di cui sopra:

- sono predisposti strumenti tecnologici atti a prevenire e/o impedire la realizzazione di illeciti informatici da parte degli esponenti del Fondo attraverso, in particolare, l'uso indebito o non autorizzato delle *password*, la detenzione o installazione di *software* non previsto dalle procedure del Fondo, ivi compresi *virus* e s*pyware* di ogni genere e natura e dispositivi atti all'interruzione di servizi o alle intercettazioni, il collegamento non consentito di *hardware* alla rete del Fondo. Tali misure in particolare prevedono regole in merito:
  - alle restrizioni all'accesso fisico ai luoghi in cui sono collocati gli strumenti informatici/telematici;
  - all'attribuzione e revoca delle *password*, tenendo conto delle mansioni per la quale viene richiesta / concessa;
  - alla rimozione dei diritti di accesso al termine del rapporto di lavoro;
  - al controllo e alla tracciabilità degli accessi;
  - alle modalità di svolgimento delle attività di gestione e manutenzione dei sistemi;

- alla previsione di controlli sulla idoneità della rete del Fondo e sul suo corretto instradamento;

- sono adottate specifiche misure di protezione volte a garantire l'integrità delle informazioni messe a disposizione del pubblico tramite la rete internet;

- sono adottati specifici strumenti per l'individuazione, prevenzione e ripristino dei sistemi rispetto a *virus* ed altre vulnerabilità;

- sono definiti ed implementati controlli specifici per la protezione dei documenti sulla base della loro classificazione, attraverso: la crittografia dei documenti; la restrizione degli accessi in lettura/scrittura sulla base delle liste di distribuzione definite; la corretta conservazione dei file;

- i fabbisogni di materiale IT sono dettagliati nel budget preventivo del Fondo;

- sono previsti e attuati programmi di informazione, formazione e sensibilizzazione rivolti al personale del Fondo al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche in dotazione al Fondo.

B.3 AREE A RISCHIO E PRINCIPI DI CONTROLLO PREVENTIVO

Occorre premettere che tutte le attività implicanti la redazione di un "documento informatico", intendendosi come tale "*qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*", e come "supporto informatico" qualsiasi "*supporto di memoria – sia esso interno o esterno all'elaboratore – sul quale possono essere registrati e conservati per un certo lasso di tempo dei dati, destinati ad essere letti ed eventualmente elaborati da un sistema informatico*", possono essere penalmente rilevanti ai sensi dell'art. 491-*bis* c.p. in chiave di reato presupposto.

Inoltre, assumono rilevanza tutte le attività che si svolgono mediante sistemi informatici adottati dal Fondo (es. comunicazioni, corrispondenza, archiviazione dati,
etc.) e, in particolare, quelle di seguito indicate.

Area a rischio n. 1

GESTIONE E MANUTENZIONE DEGLI APPLICATIVI E DEI SISTEMI INFORMATICI

- RUOLI E FUNZIONI COINVOLTE

Direzione, Area ICT

- ATTIVITÀ SENSIBILI

a) Gestione dello sviluppo e della manutenzione dei *software*;

b) Gestione della sicurezza logica;

c) Gestione della sicurezza fisica;

d) Gestione dei *backup*;

e) Gestione dei fornitori in ambito IT.

- POSSIBILI MODALITÀ DI COMMISSIONE DEI REATI-PRESUPPOSTO

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso l'accesso al sistema informatico di *competitors* o di altri soggetti, mediante l'utilizzo di sistemi informatici aziendali ovvero mediante l'utilizzo di *username* e *password* personali ottenute in maniera fraudolenta e/o per mezzo di tecniche di *hacking* o per appropriazione indebita da parte di utenti/specialisti IT. Il vantaggio può configurarsi, ad esempio, nell'acquisire dati ed informazioni riservate di concorrenti o di altri soggetti, nel manipolare / alterare dati prima o durante il loro inserimento nella memoria del sistema informatico, nell'inserire abusivamente istruzioni in un programma in modo che il sistema informatico operi in modo diverso da quello predeterminato dal legittimo titolare e, in questo modo, procurare vantaggi al Fondo; nell'inserire abusivamente un programma nel sistema informatico per causarne l'arresto attraverso delle istruzioni del tutto incoerenti o contrastanti rispetto a quelle predisposte per il funzionamento del sistema informatico medesimo e, in tal modo, procurare vantaggi al Fondo; nel distruggere, sui sistemi dei concorrenti o di altri soggetti, le informazioni e la documentazione relativa a loro prodotti/progetti e ottenere un vantaggio competitivo;

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- la violazione fisica o logica delle protezioni ai sistemi delle infrastrutture tecnologiche dei concorrenti o di altri soggetti al fine di ottenere, direttamente o indirettamente, un vantaggio economico e/o finanziario e/o impedirne l'attività o danneggiare in altro modo i concorrenti;

- l'alterazione o l'accesso indebito a dati e/o programmi in ambiente di produzione, al fine di produrre dati ed informazioni di bilancio false e conseguire, in genere, un vantaggio economico, patrimoniale e/o finanziario per il Fondo;
- il danneggiamento di informazioni, dati o programmi informatici commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza, al fine di distruggere dati ed informazioni compromettenti che, se diffusi, arrecherebbero un danno al Fondo;

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- L'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;

d) Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 *bis* c.p.)

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, ecc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria.

Area a rischio n. 2

AMMINISTRAZIONE DEL PERSONALE

- RUOLI E FUNZIONI COINVOLTE

Direzione, Area Amministrazione

- ATTIVITÀ SENSIBILI

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

b) immissione/gestione/utilizzo dei dati del Fondo, contabili e sensibili nei sistemi informatici del Fondo;

- POSSIBILI MODALITÀ DI COMMISSIONE DEI REATI-PRESUPPOSTO

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- l'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;
- l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (Ministeri, Agenzie, ANAC, INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, Carabinieri, etc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione.

Area a rischio n. 3

GESTIONE DEI RAPPORTI CON L'AMMINISTRAZIONE FINANZIARIA

➢ RUOLI E FUNZIONI COINVOLTE

Direzione, Area Amministrazione, Affari Legali e Gare

➢ ATTIVITÀ SENSIBILI

a) Installazione, manutenzione, aggiornamento e gestione di *software* di soggetti pubblici utilizzati anche per lo scambio di dati ed informazioni riguardanti tutti gli adempimenti fiscali.

➢ POSSIBILI MODALITÀ DI COMMISSIONE DEI REATI-PRESUPPOSTO

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- l'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;
- l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (Ministero, Agenzie, INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, etc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione.

Area a rischio n. 4

GESTIONE DEI SISTEMI INFORMATIVI

- RUOLI E FUNZIONI COINVOLTE

Direzione, Area ICT

- ATTIVITÀ SENSIBILI

a) Creazione *account* per accesso a sistemi informatici del Fondo;
b) abilitazione all'accesso, manutenzione e custodia della *password*;
c) utilizzo/gestione telefoni cellulari, *tablet* e *notebook*;
d) interruzioni nelle comunicazioni e nelle operazioni d'uso dei PC;
e) scambio di corrispondenza in via telematica;
f) corrispondenza con l'estero tramite posta elettronica;
g) cancellazione dati inseriti da utenti non più nell'organico del Fondo;
h) comunicazioni telematiche o informatiche dirette alla P.A. ed, in generale, ad ogni autorità pubblica che intrattenga rapporti col Fondo;
i) predisposizione, modificazione, trasmissione, archiviazione e custodia di dati, informazioni o documenti riservati per via o su supporto telematico o informatico;

- POSSIBILI MODALITÀ DI COMMISSIONE DEI REATI-PRESUPPOSTO

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso l'accesso al sistema informatico di *competitors* o di altri soggetti, mediante l'utilizzo di sistemi informatici aziendali ovvero mediante l'utilizzo di *username* e *password* personali ottenute in maniera fraudolenta e/o per mezzo di tecniche di *hacking* o per appropriazione indebita da parte di utenti/specialisti IT. Il vantaggio può configurarsi, ad esempio, nell'acquisire dati ed informazioni riservate di concorrenti o di altri soggetti, nel manipolare / alterare dati prima o durante il loro inserimento nella memoria del sistema informatico, nell'inserire abusivamente istruzioni in un programma in modo che il sistema informatico operi in modo diverso da quello predeterminato dal legittimo titolare e, in questo modo, procurare vantaggi al Fondo; nell'inserire abusivamente un programma nel sistema informatico per causarne l'arresto attraverso delle istruzioni del tutto incoerenti o contrastanti rispetto a quelle predisposte per il funzionamento del sistema informatico medesimo e, in tal modo, procurare vantaggi al Fondo; nel distruggere, sui sistemi dei concorrenti o di altri soggetti, le informazioni e la documentazione relativa a loro prodotti/progetti e ottenere un vantaggio competitivo;

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- la violazione fisica o logica delle protezioni ai sistemi delle infrastrutture tecnologiche dei concorrenti o di altri soggetti al fine di ottenere, direttamente o indirettamente, un vantaggio economico e/o finanziario e/o impedirne l'attività o danneggiare in altro modo i concorrenti;
- l'alterazione o l'accesso indebito a dati e/o programmi in ambiente di produzione, al fine di produrre dati ed informazioni di bilancio false e conseguire, in genere, un vantaggio economico, patrimoniale e/o finanziario per il Fondo;
- il danneggiamento di informazioni, dati o programmi informatici commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza, al fine di distruggere dati ed informazioni compromettenti che, se diffusi, arrecherebbero un danno al Fondo;

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

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- l'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;

d) Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 *bis* c.p.)

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, ecc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria.

➢ PRINCIPI DI CONTROLLO PREVENTIVO RELATIVI ALLE AREE A RISCHIO N. 1, 2, 3 e 4

Oltre ai principi generali di comportamento indicati nella presente Parte Speciale "B" del Modello, le attività del Fondo - a mitigazione dei fattori di rischio correlati ai reati informatici di cui all'art. 24-*bis* del Decreto e con riferimento alle aree in oggetto - si ispirano ai seguenti principi di controllo preventivo:

- rispetto dei ruoli, compiti e responsabilità definiti dall'organigramma del Fondo e dal sistema autorizzativo nella gestione di sistemi, strumenti, documenti o dati informatici;
- formale identificazione dei soggetti deputati alla gestione di sistemi, strumenti, documenti o dati informatici;
- corretto e sicuro funzionamento degli elaboratori di informazioni;
- definizione delle modalità di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi;
- rivisitazione periodica dei diritti d'accesso degli utenti;
- accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati (in particolare: se si deve abbandonare la postazione, anche per pochi minuti, è preferibile che l'utente si disconnetta sempre, per poi accedere nuovamente, utilizzando la specifica funzione del sistema operativo; l'utente deve essere ben consapevole che, se abbandona la postazione di lavoro senza essersi disconnesso, è possibile che un terzo non autorizzato compia operazioni vietate dalla legge o dal presente Modello; in questo caso le eventuali conseguenze, penali, civili o disciplinari, ricadranno sul medesimo utente);
- controlli formalizzati sugli accessi atti a presidiare il rischio di accesso non autorizzato alle informazioni, ai sistemi, alle reti e alle applicazioni, nonché atti a prevenire danni ed interferenze ai locali ed ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;
- segregazione delle funzioni al fine di garantire operativamente la separazione del livello esecutivo da quello approvativo;
- segmentazione della rete al fine di assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni utilizzate dal Fondo;
- autenticazione individuale degli utenti tramite codice identificativo dell'utente e *password* o tramite altro sistema idoneo a garantire un adeguato livello di sicurezza (nello specifico: la *password* deve essere composta da caratteri alfanumerici, con alternanza di maiuscole e minuscole e con l'impiego di caratteri speciali; non deve avere senso compiuto, né tantomeno essere basata su informazioni facilmente deducibili, come date di nascita o nomi di familiari);
- modifica al primo accesso, della password attribuita dall'Amministratore di Sistema;
- riservatezza della *password*: non divulgarla a terzi, non permettere ad altri utenti di operare con il proprio identificativo utente, non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi. È essenziale che l'utente riponga la massima cura nella gestione delle *password*, perché un accesso effettuato con la propria password sarebbe irrimediabilmente riconducibile all'utente medesimo, con conseguenti eventuali responsabilità penali, civili e disciplinari. Qualora l'utente ritenga che la segretezza della password sia stata compromessa, deve darne

comunicazione all'Amministratore di Sistema, che provvederà al rilascio di nuova password, che dovrà essere a sua volta modificata;

- assegnazione di una nuova *password* qualora un utente venga a conoscenza della password di un collega, previa tempestiva comunicazione all'Amministratore di Sistema;
- assegnazione di un indirizzo di posta elettronica personale, impiegato unicamente nell'ambito dell'attività svolta per conto del Fondo, ad ogni utente che ne sarà responsabile;
- gestione della casella di posta secondo le direttive organizzative stabilite dal Fondo;
- il controllo della propria casella di posta elettronica privata mediante *webmail*, e rispondere ai messaggi*,* durante l'orario di lavoro, è consentito salvo ciò non pregiudichi il puntuale, tempestivo e corretto svolgimento delle proprie mansioni o, comunque, le obiettive esigenze del Fondo;
- disconnettere l'utenza in caso di abbandono della postazione, anche per pochi minuti, per poi accedere nuovamente, utilizzando la specifica funzione del sistema operativo. L'utente deve essere ben consapevole che, se abbandona la postazione di lavoro senza essersi disconnesso, è possibile che un terzo non autorizzato compia operazioni vietate dalla legge o dal presente Modello. In questo caso le eventuali conseguenze, penali, civili o disciplinari, ricadranno sul medesimo utente;
- segnalazione tempestiva all'Amministratore di Sistema di anomalie, malfunzionamenti, rallentamenti del *computer*: resta fermo che il segnalante/utente non deve intervenire senza l'autorizzazione dell'Amministratore di Sistema.
- spegnere o comunque bloccare tutte le postazioni lavoro, le stampanti, gli scanner, ecc. al termine della giornata lavorativa o in caso di allontanamento prolungato;
- attivazione da parte dell'utente, in caso di assenza programmata, dell'apposita funzione che consente di inviare automaticamente messaggi di risposta che contengano le coordinate di un'altra persona addetta al servizio oppure indichino le modalità per mettersi comunque in contatto col Fondo. Qualora l'attivazione del servizio di risposta automatica non fosse stato attivato, per dimenticanza o per improvvisa assenza, il Fondo si riserva di farlo, tramite una persona di fiducia indicata dall'utente, e con la garanzia della riservatezza. Qualora fosse necessario accedere ai messaggi contenuti nella casella di un lavoratore temporaneamente assente, l'utente ha la possibilità di indicare un altro lavoratore, persona di fiducia, che provvederà ad aprire la casella e ad inoltrare al Fondo i messaggi pertinenti all'attività lavorativa. Di questa attività viene redatto apposito verbale. Al ritorno dell'utente assente, dovrà essergli assegnata una nuova *password*.

- non alterazione, né nella loro configurazione *hardware* né nella loro configurazione *software*, degli strumenti informatici, salvo autorizzazione dell'Amministratore di Sistema. In particolare:

a) non possono essere installati programmi senza l'autorizzazione dell'Amministratore di Sistema, il quale è in possesso dell'elenco delle risorse *software* installate su ogni postazione di lavoro;
b) non possono essere spostate le attrezzature informatiche senza l'autorizzazione dell'Amministratore di Sistema;
c) non possono essere utilizzate e connesse al sistema risorse *hardware* private (a titolo esemplificativo, PC portatili, *Hard disk* esterni, chiavette usb), mentre possono e devono essere utilizzate esclusivamente quelle date eventualmente in uso dal Fondo;

- formale autorizzazione, nel rispetto delle deleghe in essere, all'accesso alle informazioni;
- controlli di sicurezza dedicati a garantire l'integrità, disponibilità e riservatezza delle informazioni sensibili;
- utilizzo di dispositivi *hardware* e *software* dedicati per l'implementazione delle politiche di navigazione in internet e scambio delle informazioni (*firewall*, *proxy server*, ecc.);

- meccanismi di protezione per lo scambio di informazioni tramite *internet*, posta elettronica e dispositivi rimovibili;
- implementazione di misure di sicurezza atte a garantire l'accesso alle informazioni da parte di terze parti solo previa autorizzazione formale e nel rispetto degli accordi di riservatezza e confidenzialità stipulati;
- implementazione di ambienti logicamente e fisicamente separati al fine di controllare e testare le modifiche software fino al rilascio in produzione;
- definizione formale delle modalità di protezione da *software* pericolosi;
- definizione formale delle modalità di gestione dei *back-up* delle informazioni e dei *software*. I supporti vengono conservati per un determinato periodo, al termine del quale vengono riutilizzati per effettuare un nuovo *backup*, tramite il quale vengono sovrascritti e cancellati i dati salvati nel *backup* precedente;
- formale classificazione delle informazioni e dei sistemi informatici gestiti dal Fondo;
- controlli formalizzati atti a presidiare il rischio di appropriazione e modifica indebita delle informazioni di proprietà del Fondo con conseguente perdita di autenticità, riservatezza ed integrità dell'*asset* informativo;
- definizione delle modalità di custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, *hard disk* esterni, ecc.) e previsione di regole di *clear screen* per gli elaboratori utilizzati;
- definizione delle tempistiche per la chiusura delle sessioni inattive;

- formale definizione dei processi di *change management* con indicazione dei ruoli coinvolti nell'*iter* autorizzativo e della segregazione dei compiti garantita nella gestione dei cambiamenti;
- formale definizione delle modalità operative per l'individuazione e la gestione degli incidenti e dei problemi;
- verifica periodica di tutti gli incidenti singoli e ricorrenti al fine di individuarne le relative cause;
- verifica periodica dei *trend* sugli incidenti e sui problemi al fine di individuare le azioni preventive al verificarsi di problemi in futuro;
- valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi e che tenga conto della normativa applicabile in materia e dei principi etici del Fondo;
- formale definizione dei rapporti con gli *outsourcer* in materia informatica, redatti attraverso specifici contratti approvati nel rispetto delle deleghe e procure in essere;
- previsione di specifiche attività di formazione ed aggiornamenti periodici sulle procedure di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
- obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa per i dipendenti e per i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- tracciabilità di tutte le operazioni effettuate per la gestione dei sistemi, strumenti, documenti o dati informatici utilizzati dal Fondo;
- sporgere immediatamente denuncia, da parte dell'utente, alle competenti autorità e inviarne copia al Fondo, specificando quali dati del Fondo erano contenuti negli strumenti smarriti in caso di smarrimento e/o furto degli strumenti portatili in dotazione;
- Il Fondo garantisce che non vengono utilizzati sistemi *hardware* e/o *software* idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:
  - la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per assicurare il servizio e-mail;
  - la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
  - la lettura o la registrazione dei caratteri inseriti, tramite la tastiera e analogo dispositivo;
  - l'analisi occulta del computer portatili affidati in uso.