# Fondazione Bioparco di Roma

# Modello di organizzazione gestione e controllo ai sensi del D.lgs. 8 giugno 2001, n. 231

## PARTE SPECIALE C

## DELITTI INFORMATICI

**Sommario**

## *Definizioni*

**Aree (processi) sensibili**
Insieme di attività correlate e collegate funzionalmente il cui svolgimento determina in termini concreti, un rischio di commissione dei Reati - presupposto del Decreto 231.
**Codice Etico**
Codice di comportamento che riassume gli standard di comportamento e i criteri di svolgimento delle attività al fine di garantire azioni e decisioni in conformità alle prescrizioni di Legge, ai Regolamenti, ai principi etici e ai valori morali propri della Fondazione Bioparco. Costituisce parte integrante del Modello di Organizzazione, gestione e controllo adottato dalla Fondazione con delibera del Consiglio di Amministrazione.
**Decreto 231**
Decreto Legislativo 8 giugno 231, n. 231, dal titolo *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della legge 29 settembre 2000, n. 300”,* pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 231 e successive modifiche ed integrazioni.
**Destinatari**
Tutti i soggetti destinatari del Modello organizzativo e, in particolare, Amministratori, Dipendenti, Collaboratori, ed ogni altro soggetto che opera in nome e per conto della Fondazione, nei limiti di quanto indicato nell’art. 5 del Decreto 231.
**Dipendenti**
Tutti i lavoratori subordinati della Fondazione.
**Area aziendale**
Struttura funzionale, inserita nella complessiva struttura organizzativa, che persegue svolge attività autonome e/o correlate/coordinate con le altre aree funzionali, nell'ambito degli obiettivi generali e della mission istituzionale della Fondazione Bioparco.
**Modello Organizzativo**
Modello di Organizzazione, gestione e controllo ai sensi del Decreto 231. Rappresenta il sistema strutturato formato da un complesso organico di principi, regole, disposizioni, schemi organizzativi e connessi compiti e responsabilità idoneo a prevenire i reati e gli illeciti amministrativi, così come previsto dagli articoli 6 e 7 del Decreto, ad integrazione degli strumenti Organizzativi e di Controllo vigenti nella Fondazione Bioparco.
**Organi di Controllo**
Sono il Comitato di Vigilanza e la Società di revisione della Fondazione.
**Organi Sociali**
Sono il Consiglio di Amministrazione ed il Comitato di Vigilanza della Fondazione.
**Organismo di Vigilanza (OdV)**
Organo previsto dall’art. 6 del Decreto 231, avente il compito di vigilare sul funzionamento e sull’osservanza del Modello Organizzativo, nonché di curarne l’aggiornamento.
**Pubblica Amministrazione**
Qualsiasi Pubblica Amministrazione, inclusi i relativi esponenti nella loro veste di Pubblici Ufficiali o Incaricati di Pubblico Servizio
Per Pubblica Amministrazione si intende, a titolo esemplificativo e non esaustivo: le amministrazioni dello Stato (Amministrazione Finanziaria, Autorità garanti e di Vigilanza, Autorità

Giudiziarie, ecc.), le aziende ed amministrazioni dello Stato, le regioni, le province, i comuni, e loro consorzi e associazioni, le istituzioni universitarie, le camere di commercio, industria, artigianato e agricoltura, gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del servizio sanitario nazionale.

**Responsabile (Direttore o Caposettore/area)**

Soggetto della Fondazione Bioparco a quale viene attribuita la responsabilità, singola o condivisa con altri per le operazioni nelle Aree (Funzioni) Aziendali.

**Soggetti in posizione apicale**

Persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione all'interno delle Società/Enti o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo delle società/Enti medesime.

**Soggetti terzi (Stakeholders)**

Coloro che agiscono in nome e/o per conto della Fondazione sulla base di apposito mandato o di altro vincolo contrattuale.

**Sottoposti (soggetti)**

Soggetti in posizione subordinata, sottoposti alla direzione o alla vigilanza di un soggetto in posizione apicale.

**Violazione (Illecito) disciplinare**

Condotta o omissione dal lavoratore dipendente in violazione delle norme di comportamento previste dal Modello Organizzativo.

**Documento/i Informatico/i**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

**Firma Elettronica**

L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

**Password**

Sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.

**Piano di Sicurezza**

Documento che definisce un insieme di attività coordinate che devono essere intraprese per implementare la politica di sicurezza del sistema.

**Postazione di Lavoro**

Postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.

**Sicurezza Informatica**

L'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.

**Sistemi Informativi**

L'insieme della rete, dei sistemi, dei data base e delle applicazioni aziendali.

## *Premessa*

La presente Parte Speciale C del Modello Organizzativo della Fondazione, recante il titolo "Delitti Informatici", ha l'obiettivo di indirizzare, mediante regole di condotta, le attività sensibili poste in essere dai Destinatari al fine di prevenire il verificarsi dei delitti informatici e di trattamento illecito dei dati di cui all'art. 24 bis del D.Lgs. 231/2001.

In particolare, la Parte Speciale C del Modello Organizzativo della Fondazione ha lo scopo di:

- indicare i Protocolli e le modalità operative che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'OdV, ed alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutti i Destinatari del Modello dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello Organizzativo- Parte Generale;
- Modello Organizzativo - Allegati;
- Modello Organizzativo - Parti Speciali;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto 231.

E' inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di Legge.

# 1 - Delitti Informatici

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei Destinatari qualificati è collegato il regime di responsabilità a carico della Fondazione, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo definito dal Modello.

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi dell'art. 24 bis, introdotto dalla Legge. 18 marzo 2008, n. 48 ("Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", pubblicata in G.U. n. 80 del 4 aprile 2008 e modificato dal D.L. 14/08/2013 n. 93, art. 9), si riporta una breve descrizione dei reati richiamati.

## *1.1 Art. 24 bis D.lgs. 231/2001*

L'art. 24 bis del d.lgs. 231/01, "Delitti informatici e trattamento illecito dei dati" stabilisce che:

1. *In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*
2. 
   *2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*
   *3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*
3. 
   *4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».*

Di seguito si riporta una descrizione dei reati richiamati dall'art. 24 bis.

**<u>Documenti informatici (art. 491-*bis* cod. penale).</u>**

"*Se alcune 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 sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- <u>Falsità materiale commessa dal pubblico ufficiale in atti pubblici</u> (art. 476 c.p.):

"*Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni*";

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

- <u>Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti</u> (art. 478 c.p.): "*Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni*";

- <u>Falsità ideologica commessa dal pubblico ufficiale in atti pubblici</u> (art. 479 c.p.): "*Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476*";

<u>Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative</u> (art. 480 c.p.): "*Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni*";

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

- <u>Falsità materiale commessa da privato</u> (art. 482 c.p.): "*Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo*";

- <u>Falsità ideologica commessa dal privato in atto pubblico</u> (art. 483 c.p.): "*Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi*";

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

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

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

- <u>Falsità in foglio firmato in bianco. Atto pubblico</u> (art. 487 c.p.): "*Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480*";

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

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

- <u>Soppressione, distruzione e occultamento di atti veri</u> (art. 490 c.p.): "*Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente*";

- <u>Copie autentiche che tengono luogo degli originali mancanti</u> (art. 492 c.p.): "*Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti*";

- <u>Falsità commesse da pubblici impiegati incaricati di un pubblico servizio</u> (art. 493 c.p.): "*Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni*".

Tale ipotesi di reato si configura nel caso in cui un dipendente o un rappresentante della Fondazione falsifichi un documento pubblico o privato avente efficacia probatoria.

## <u>Accesso abusivo ad un sistema informatico o telematico – art. 615 ter c.p.</u>

"*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di*

*sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:*
*1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.*
*Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è,rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."*

Il reato incrimina due differenti condotte:

- introduzione abusiva nel sistema protetto;

- l'atto di mantenersi all'interno del sistema contro la volontà del titolare.

Il reato è stato posto dal Legislatore nel capo terzo del libro Secondo del c.p. , intendendo, quindi, che il reato sia una specificazione della violazione di domicilio.
Nel primo caso l'introduzione abusiva è nei confronti del domicilio informatico che il titolare protegge attraverso misure di sicurezza atte ad escludere gli estranei.
Nel secondo caso si fa riferimento all'ipotesi in cui il reato è commesso da chi, autorizzato all'accesso per un determinato scopo, utilizzi tale accesso per finalità diverse da quelle autorizzate.
Affinchè si configuri il reato non è previsto che si configuri lo scopo di lucro o che sia danneggiato il sistema.
Il reato è perseguibile a querela della persona offesa, salvo che sussistano le aggravanti: il soggetto agente riveste una determinata qualifica (es. Pubblico Ufficiale), o se si è usata violenza, o ancora se dal fatto deriva distruzione o danneggiamento del sistema. o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.
Va sottolineato che, all'interno dell'azienda, il reato può essere commesso anche dal dipendente, il quale potrebbe abusivamente accedere utilizzando le proprie credenziali a banche dati dell'azienda per le quali non ha l'autorizzazione utilizzando, eventualmente, le credenziali di colleghi, o le proprie, ma, sconfinando in aree per le quali non è legittimato.

## <u>Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici – art. 615 quarter c.p.</u>

*"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.*
*La pena e' della reclusione da uno a due anni e della multa da 5.164 euro a 10.329*

Riguardo alle condotte criminose:

- per "diffusione" si intende il mettere a conoscenza, di una o più persone indeterminate, i codici di accesso, in qualunque forma, attraverso la disponibilità degli stessi (anche attraverso pubblicazione in Internet);
- Per "riproduzione" si intende la produzione di una copia abusiva di un codice, di una "parola chiave" o di ogni altro mezzo idoneo all'accesso;
- per "consegna" va intesa la cessione materiale del codice a una determinata persona;
- per "comunicazione" invece si intende il mettere a conoscenza di una o più persone determinate dei codici di accesso.

In ordine all'elemento soggettivo è necessario il dolo specifico, ossia il fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno.

Per quanto attiene alle ipotesi aggravate esse sono le medesime indicate all'art. 615 ter c.p., ad esclusione del danneggiamento.

**<u>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- quinquies c.p.)</u>**

*"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329."*

All'art. 615 quinquies sono previste due distinte ipotesi di reato:

1) il fatto di chi diffonde, comunica o consegna un programma informatico di propria redazione o di creazione altrui, volto o atto a danneggiare un sistema informatico/telematico;
2) il fatto di chi diffonde, comunica o consegna un programma di propria o altrui creazione, volto ad interrompere o alterare, seppur parzialmente, il funzionamento di un sistema informatico.

La norma sanziona non soltanto le condotte afferenti ai "programmi informatici", ma anche l'utilizzo illecito di "apparecchiature" e "dispositivi" in grado di danneggiare un sistema informatico, ovvero di alterarne il funzionamento.
Trattasi di reato comune. Il momento consumativo del reato si ha con la messa in atto delle condotte di diffusione, comunicazione o consegna: la mera realizzazione di un virus informatico, infatti, di per sé non ha rilevanza.

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

*“Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, e' punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.*
*Tuttavia si procede d’ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:*
1) *in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;*
2) *da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;*
3) *da chi esercita anche abusivamente la professione di investigatore privato.*

La norma ha struttura e contenuto pressoché identici a quelli di cui all’articolo 617 c.p., volendo il legislatore soltanto colmare il vuoto normativo con riferimento alle intercettazioni attraverso elaboratori elettronici.
L’interesse tutelato rimane, pertanto, quello della segretezza e inviolabilità delle comunicazioni. Il reato è di mera condotta - a forma vincolata – ed è comune. È previsto il dolo generico, essendo sufficiente la coscienza e la volontà del fatto tipico previsto dalla norma.
La norma ha struttura e contenuto pressoché identici a quelli di cui all’articolo 617 c.p., volendo il legislatore soltanto colmare il vuoto normativo con riferimento alle intercettazioni attraverso elaboratori elettronici.

## Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p)

*Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*
*La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.*

Similarmente all’articolo 617-quater, questo articolo estende la punibilità della condotta illecita prevista dall’articolo 617-bis alle comunicazioni effettuate tramite un sistema informatico o telematico.
Affinchè si configuri il reato è sufficiente la mera messa in opera delle apparecchiature, in quanto non si richiede dal Legislatore che esse siano o siano state già in funzione.

## 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 ricorre la circostanza di cui al numero 1) del secondo comma dell’articolo 635 13 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d’ufficio.”*

La configurabilità del reato di danneggiamento informatico non viene preclusa dall'eventuale reversibilità del danno, ritenendosi sufficiente che il bene (ossia il personal computer) sia stato, anche se temporaneamente, oggetto di manomissione o alterazione
Il reato di danneggiamento informatico, infatti, ha argomentato il giudice di legittimità, deve ritenersi integrato dalla manomissione ed alterazione dello stato del computer, rimediabili solo con postumo intervento recuperatorio, che, comunque, non sarebbe reintegrativo dell'originaria configurazione dell'ambiente di lavoro.

**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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 [con violenza alla persona o con minaccia] ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata*

Il precedente testo normativo sanzionava, soltanto i danneggiamenti riguardanti i dati contenuti o pertinenti a "sistemi informatici o telematici di pubblica utilità", mentre, attualmente, è sufficiente che i dati siano "utilizzati dallo Stato o da altro ente pubblico".
Sono ricomprese pertanto le condotte riguardanti 1) dati, informazioni e programmi utilizzati dagli enti pubblici; 2) dati informazioni e programmi di pubblica utilità (e dunque sia pubblici che privati, purché siano destinati a soddisfare un interesse di natura pubblica).
Trattandosi di reato aggravato dall'evento, il fatto sussiste anche in assenza di qualunque effettivo deterioramento o soppressione dei dati, pur dovendosi necessariamente richiedere l'idoneità dell'azione a produrre tale effetto.
L'effettiva distruzione, cancellazione, alterazione o deterioramento è invece contemplata come circostanza aggravante (art. 635-ter comma 2 c.p.).

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

"*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 ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*"

Il danneggiamento di sistemi informatici o telematici non di pubblica utilità ha mantenuto la caratteristica di reato di evento, e pertanto richiede espressamente che il sistema venga danneggiato, reso in tutto o in parte inservibile, ovvero ne venga ostacolato gravemente il funzionamento.

**<u>Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-*quinquies* c. p.)</u>**

"*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 ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata*".

Occorre rilevare che, mentre per quanto riguarda l'art. 635-ter c.p., il danneggiamento può riguardare dati o programmi informatici utilizzati dagli enti pubblici o ad essi pertinenti, o comunque di pubblica utilità, il reato di cui all'art. 635-quinquies c.p. sussiste soltanto laddove la condotta sia diretta a danneggiare, distruggere etc. sistemi informatici o telematici di pubblica utilità.
Non è sufficiente, quindi, per la sussistenza del reato, che i sistemi siano utilizzati dagli enti pubblici, ma occorre che gli stessi siano di pubblica utilità.

# 2 - Processi e attività sensibili ai reati ex art. 24 bis D.lgs. 231/2001

L'art. 6, comma 2, lett. a) del Decreto 231 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Fondazione nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto stesso.
Tuttavia, trattandosi di reati riferibili generalmente alle modalità con le quali vengono, non solo realizzate le attività specifiche dell'azienda, ma anche la gestione della medesima, è evidente che il rischio di commissione dell'illecito è astrattamente configurabile in qualunque contesto aziendale.
Le aree ritenute essere esposte ad un maggior rischio possono essere riconducibili a quelle in cui la frequenza, la complessità e la criticità nell'utilizzo dell'IT è maggiore e in cui le competenze informatiche dei soggetti coinvolti risultano più elevate. Possono tuttavia essere considerati coinvolti nella gestione della sicurezza tutti i dipendenti, collaboratori ecc., a prescindere dalla loro collocazione, dalla forma della loro collaborazione con la Fondazione, dalle mansioni svolte e dal livello gerarchico, in quanto sono obbligati a svolgere le loro attività nel rispetto delle norme di condotta e dei principi di comportamento indicati nel Modello.

## *2.1 Principi generali di condotta e comportamento*

La presente sezione individua i principi di condotta e di comportamento che devono essere rispettati dai Destinatari, affinchè non si incorra nelle ipotesi di reato esposte nella presente parte speciale.
In particolare, tutti i dipendenti e collaboratori della Fondazione sono tenuti a:

• astenersi dal tenere comportamenti tali integrare le fattispecie previste dai suddetti reati di criminalità informatica, ovvero da comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possono potenzialmente diventarlo;

• rispettare le regole di condotta generale, i principi di controllo e le prescrizioni specifiche formulate nel presente Modello;

• rispettare le norme, le policy e le procedure aziendali che disciplinano l'accesso e l'utilizzo dei sistemi e degli applicativi informatici della Fondazione;

• promuovere il rispetto delle suddette norme, regole e principi.

## *2.2 Principi specifici*

Vengono individuati, inoltre, principi specifici di condotta:

• La Fondazione, consapevole dei continui cambiamenti tecnologici e dell'elevato impegno operativo,organizzativo e finanziario necessario, si impegna a mantenere un efficace sistema di sicurezza informatica, in particolare attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi, attraverso l'utilizzo di strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attacchi, (ii) la garanzia della massima continuità del servizio;

• l’assegnazione e la gestione delle credenziali di autorizzazione personale (username e password) e delle credenziali di accesso alle diverse sezioni del sistema informatico della Fondazione e i termini di validità delle medesime sono stabilite secondo idonee policy aziendali;

• l’accesso alle diverse sezioni del sistema informatico della Fondazione e a eventuali dati, informazioni, sistemi informatici e telematici cui la Fondazione abbia accesso è riconosciuto a dipendenti, collaboratori, consulenti e partner nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico e coerentemente con gli obiettivi aziendali;

• ogni singolo utente è personalmente responsabile riguardo l’utilizzo del sistema informatico della Fondazione, inclusi eventuali dati, informazioni, sistemi informatici e telematici cui la Fondazione abbia accesso, nell’ambito dei presidi posti dalla Fondazione a tutela della sicurezza, integrità e riservatezza dei dati.

• è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner che a vario titolo abbiano accesso alla rete aziendale di installare propri software che non rientrino nello scopo per cui il sistema informatico è stato assegnato all’utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale;

• è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner di operare in maniera illecita su sistemi informativi altrui al fine di sottrarre fraudolentemente dati o informazioni riservate o sensibili;

• L’istallazione di nuove apparecchiature IT, strutture e procedure deve essere formalmente approvata. L’approvazione deve includere il parere favorevole del Responsabile della Sicurezza Informatica.

• Il processo di definizione ed approvazione di nuove strutture IT, e della loro modifica, deve essere sempre formalizzato. Il processo di approvazione comprende un’analisi, effettuata dal settore aziendale sulla sicurezza informatica, avente come finalità quella di assicurare che le nuove tecnologie non presentino lacune sotto il profilo della sicurezza e non influenzino negativamente i sistemi e le procedure attualmente presenti.

• è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner che a vario titolo abbiano accesso alla rete aziendale di installare nella rete propri software che possano impedire o interrompere o danneggiare le comunicazioni informatiche aziendali ovvero l’intero sistema informatico aziendale

• qualora si verifichino circostanze non regolamentate, che si prestano a dubbie interpretazioni, tali da originare difficoltà nell’operatività dell’attività, è obbligo di tutti i soggetti coinvolti di ricorrere al proprio responsabile che, sentito l’OdV, assume le decisioni del caso.

Roma, 28/11/2018 Il Presidente