# ECOSAVONA S.R.L.

# PARTE SPECIALE - 8-

## Reati informatici e Trattamento illecito dei dati

**Aggiornato il 4 Ottobre 2019**

## CAPITOLO 1.
## Funzione della presente Parte speciale-8-

Il legislatore, mediante la previsione dell'art. 24-*bis*, ha esteso l'ambito di applicazione della responsabilità amministrativa degli enti, prevista dal D.lgs. n. 231/2001, ai reati informatici e al trattamento illecito dei dati, a seguito del recepimento, ad opera della legge 18.03.2008, n. 48, della "*Convenzione del Consiglio d'Europa sulla criminalità informatica*", redatta a Budapest il 23.11.2001.
La presente Parte Speciale-8- è destinata a tutti i soggetti operanti presso ECOSAVONA, siano essi Amministratori, Dirigenti, Dipendenti, Consulenti esterni e/o Collaboratori, soggetti a vigilanza, (di seguito, indicati quali "*Destinatari*").
I predetti "Destinatari", nell'ambito delle rispettive funzioni, dovranno conformarsi ai principi di comportamento ivi delineati al fine di prevenire la commissione dei reati espressamente considerati dall'art. 24-*bis*, D.lgs. n. 231/2001.
In relazione all'attività aziendale svolta nello specifico da ECOSAVONA, i reati di cui all'art. 24-bis del D.Lgs. n. 231/2001, sono da ritenersi in effetti solo astrattamente configurabili.
Al fine di rispondere alle esigenze penal-preventive di cui al D.Lgs. n. 231/2001, la Società ha tuttavia ritenuto opportuno disciplinarli nella presente Parte Speciale-6- con il fine specifico di evitare che eventuali condotte, poste in essere da soggetti operanti presso ECOSAVONA, possano concretare le condotte tipiche previste in materia di reati informatici.

Il perseguimento delle finalità di prevenzione dei reati richiede – come già ampiamente evidenziato nella Parte Generale del presente Modello – una ricognizione dei meccanismi di funzionamento e di controllo esistenti all'interno della società, nonché la verifica dell'adeguatezza dei criteri di attribuzione dei poteri di rappresentanza e delle responsabilità connesse.

In tal senso si sono individuati i principali presidi per l'attuazione delle vigenti previsioni normative costituiti da:
- Modello di organizzazione, gestione e controllo;
- Codice Etico;
- Sistema disciplinare e sanzionatorio;
- Sistema di formazione e comunicazione;
- Documento Programmatico di Sicurezza ex D. Lgs. 196/2003.

Nelle pagine che seguono, verranno pertanto individuate:

- le fattispecie dei reati di cui all'art. 24 *bis* D.Lgs. n. 231/01, con analisi delle modalità di condotta prese in considerazione dalle norme in oggetto;
- le attività sensibili di ECOSAVONA relative ai reati informatici e al trattamento illecito dei dati che, nell'ambito della società potrebbero risultare a rischio di commissione di reati;
- i principi di riferimento in attuazione dei quali devono essere adottate le procedure aziendali che tutti i Destinatari sono chiamati ad osservare, ai fini della corretta ed effettiva applicazione del Modello di Organizzazione, gestione e controllo;
- i principi di riferimento che devono presiedere alle attività di controllo, monitoraggio e verifica dell'Organismo di Vigilanza e dei responsabili delle altre funzioni aziendali che con lo stesso cooperano, debitamente formalizzate in apposite procedure e/o regolamenti interni da adottare ai fini della corretta applicazione del presente Modello.

## CAPITOLO 2.
## Le fattispecie dei reati informatici (art. 24-*bis*, D.Lgs. n. 231/01)

### 2.1. Definizioni

Come dinnanzi esposto, l'art. 7 della legge 18.03.2008, n. 48, ratificando la Convenzione del Consiglio d'Europa sui reati informatici, ha introdotto nel D.lgs. n. 231/2001, tramite l'art. 24-*bis*, alcune ipotesi di reato in materia di criminalità informatica, già disciplinate nel codice penale.

Per "**crimine informatico**" si intende ogni comportamento previsto e punito dal codice penale o da leggi speciali in cui qualsiasi strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione del fatto-reato.

Si utilizza il termine "**reato informatico**" per indicare qualsiasi condotta realizzata per mezzo di nuove tecnologie o comunque rivolta contro beni informatici, sanzionata dall'ordinamento penale.

In sostanza, ricorre un crimine informatico quando un sistema di elaborazione, o ciò che viene prodotto dall'elaboratore, è usato come mezzo per commettere frodi, sabotaggi o falsificazioni.
In ordine alle sanzioni poste a carico delle società in caso di commissione, consumata o tentata, di uno dei reati ivi contemplati, l'art. 24 *bis* precisa quanto segue:
«***Articolo 24-bis.*** *– (**Delitti informatici e trattamento illecito di dati**). – 1. In relazione alla commissione dei delitti di cui agli articoli **615-ter**, **617-quater**, **617-quinquies**, **635-bis**, **635-ter**, **635-quater** e **635-quinquies** del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*
*2. In relazione alla commissione dei delitti di cui agli articoli **615-quater** e **615-quinquies** del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*
*3. In relazione alla commissione dei delitti di cui agli articoli* **491-bis e 640-quinquies** *del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*
*4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».*

Si procede, di seguito, ad una breve descrizione normativa delle singole fattispecie di reato previste dall'art. 24-*bis*, D. Lgs. n. 231/01.

## 2.2. Falsità in un documento informatico pubblico o privato (491-*bis* c.p.)

*"Se alcuna delle falsità previste dal presente capo (Capo III c.p.) 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. A Tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".*

L'esame delle disposizioni penali in materia di reati informatici, prende le mosse dall'art. 491-*bis* c.p., che opera una definizione tecnico-giuridica di "documento informatico".
La norma in oggetto opera un rinvio diretto ai reati contro la "falsità in atti", previsti dal Capo III del c.p., estendendo la tutela penale a tutte le ipotesi in cui la falsità riguarda un documento informatico pubblico o privato, avente efficacia probatoria.
Ne consegue che, la falsificazione del documento informatico assume rilevanza penale quando:

a) l'oggetto su cui cade la condotta è un documento informatico pubblico o privato;
b) la condotta di falso è riconducibile, presentandone tutti i requisiti, a una delle ipotesi di reato previste nel Capo III sulla falsità in atti (ex artt. 476 e ss c.p.).

Le condotte prese in considerazione possono riguardare la "contraffazione" o "alterazione" di un documento ovvero "dichiarazioni false" o "menzognere" trasposte in un documento.
Soggetti attivi di tali reati possono essere soggetti privati, pubblici ufficiali o incaricati di un pubblico servizio nell'ambito delle rispettive funzioni.
In relazione al documento oggetto di falsificazione, può, a sua volta, essere un atto pubblico o una scrittura privata.
Le condotte punibili riguardano, altresì, tutti quei casi in cui venga utilizzato un atto che si sa, a priori, essere falso, o i casi in cui un soggetto distrugge, sopprime od occulta un atto vero.
**Le condotte di falsificazione esaminate devono ricadere, ai sensi dell'art. 491-*bis*, c.p., su un documento informatico pubblico o privato avente "efficacia probatoria".**
Per "**documento informatico**" deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti a tutti gli effetti di legge. La norma, dunque, prende in considerazione qualunque supporto informatico contenente dati o

informazioni o programmi specificamente destinati a elaborarli, in relazione al loro "contenuto rappresentativo".
Il supporto informatico viene, infatti, indicato quale equivalente informatico del tradizionale foglio di carta, sul quale può essere impresso un qualsiasi contenuto rappresentativo che può essere oggetto di condotte di falsificazione da parte dei Destinatari.
La norma in oggetto sanziona altresì le ipotesi di uso abusivo della firma digitale (es., l'utilizzo abusivo della chiave privata, preposta alla digitalizzazione della firma, da parte di persona diversa dal titolare e, in ogni caso, ogni atto di falsificazione di firma elettronica).
Data l'eterogeneità delle condotte penalmente rilevanti in materia di "falsità in atti", si riportano, di seguito, altri esempi: l'inserimento di dati falsi nell'archivio elettronico da parte di un dipendente; la alterazione o la manomissione di un atto pubblico o privato (es. documenti per accedere a un bando del Comune o per partecipare ad una gara pubblica); l'inserimento di informazioni della società non corrispondenti al vero (es, in sede di dichiarazione dei redditi compilata on line, o di altri documenti compilati on line a fini amministrativi, attestazione di conformità di un atto, falsità in un verbale di riunione assembleare); la distruzione, l'occultamento o manomissione di un documento per favorire, in qualunque modo la società (es, in caso di ispezioni o perquisizioni, per accedere a convenzioni, agevolazioni, o per richiedere sovvenzioni).
In ogni caso, le condotte sono sanzionate, ai sensi del D.lgs. n. 231/2001, nella forma consumata o tentata, qualora siano commesse al fine di procurare un vantaggio, un interesse o un profitto, diretto o indiretto, alla società.

## 2.3. Accesso abusivo ad un sistema informatico o telematico (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".*

Il reato in oggetto, posto a tutela della riservatezza delle comunicazioni e delle informazioni, incrimina due differenti condotte:

a) L'introduzione abusiva in un sistema informatico o telematico protetto;
b) L'atto di mantenersi nel sistema protetto contro la volontà del titolare.

Nella prima ipotesi considerata, il delitto punisce la condotta di chi si introduce abusivamente, ovvero eludendo una qualsiasi forma, anche minima, di barriera ostativa all'accesso in un sistema informatico o telematico protetto da misure di sicurezza.

.

Con la nozione di misure di sicurezza si intendono diversi tipi di strumenti: misure fisiche (servizi di vigilanza, porte blindate), logiche (password), biometriche (lettura dell'iride o dell'impronta digitale) ovvero il superamento di ogni barriera di protezione del sistema che renda possibile il dialogo con il medesimo in modo che l'agente venga a trovarsi nella condizione di conoscere dati, informazioni o programmi.

La conoscenza dei dati, evidentemente, può avvenire sia con la semplice lettura, sia con la copiatura degli stessi.

Le modalità delle condotta, ai fini del D.lgs. n. 231/2001, possono riguardare soggetti che si introducono nel sistema informatico della società per effettuare operazioni portatrici di un interesse o un vantaggio per la società stessa (es, diminuzione del credito dei clienti, maggiorazione dei costi dei servizi erogati, fatturazioni non richieste). Oppure soggetti che si introducono abusivamente in sistemi informatici esterni (accesso abusivo al sistema informatico di una società concorrente per conoscere informazioni riservate, es portafoglio clienti, Know-how, e qualsiasi altra informazione riservata sulla vita della società).

Possono integrare la condotte di "introduzione e "mantenimento" nel sistema, ex art. 615 *ter* c.p., l'installazione di virus e di *software* spia, ma anche l'installazione di *data-logs* o l'invio di *cookies* in un sistema protetto, senza il consenso del titolare del sistema stesso (*data logs* e *cookies* infatti, sono tecniche che, anche in maniera occulta ed automatica, consentono di acquisire informazioni relative al sistema (ubicazione dell'utente, dati relativi al traffico telematico, username, password).

La seconda ipotesi presa in considerazione dall'art. 615-*ter*, c.p., è quella di colui che si mantiene all'interno del sistema informatico o telematico contro la volontà di chi ha diritto di escluderlo.

Dunque, chi è autorizzato all'accesso per una determinata finalità, ma utilizza il consenso per una finalità diversa, e quindi non ne rispetta le condizioni, risponderà della condotta vietata.

Il reato si perfeziona sia nel caso in cui il soggetto nel momento di introdursi nel sistema informatico, abbia già maturato la decisione di duplicare abusivamente i dati in esso contenuti, sia nel caso in cui, possedendo per ragioni di servizio una duplicazione di quei dati, decida di farne uso, pur conoscendo la contraria volontà del titolare del diritto.
Il dolo richiesto per la consumazione del reato, in entrambe le ipotesi, è generico.

### 2.4. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (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, 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 è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater".*

La fattispecie in oggetto è un reato di pericolo volto a prevenire la consumazione di più gravi delitti contro la tutela della riservatezza (es., art. 615-*ter*) o contro il patrimonio (es: art. 640-*ter*, frode informatica).
E' noto che a protezione dell'accesso a programmi riservati sono previsti le c.d. "password" (codici di accesso riservati, nominativi o numerici) la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico.
Le condotte incriminate si riferiscono a soggetti che si procurano codici di accesso ai sistemi informatici al fine di accedere ad un sistema (interno o esterno) per effettuare operazioni a vantaggio o interesse della società.
Il *dolo è specifico* dovendo essere la condotta diretta a procurare un profitto a sé o ad altri ovvero ad arrecare ad altri un danno.
Il delitto si consuma al momento del compimento della condotta; il tentativo appare configurabile in tutte le forme di condotta.
Ai sensi del secondo comma dell'art. 615-*quater* c.p. il delitto è aggravato se il fatto è commesso:

- 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;
- 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.

## 2.5. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico (615-*quinquies* c.p.).

*“ 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”.*

L’art. 615- *quinquies* c.p. punisce chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare illecitamente un sistema informatico o telematico o di alterarne, seppur parzialmente, il funzionamento.

Con tale norma si mira reprimere la diffusione dei c.d. “virus” informatici, forieri di gravi danni ai sistemi informatici e telematici, utilizzati spesso per scopi di sabotaggio.

Dalla lettera dell’articolo si deduce che il reato è configurabile sia in caso di messa in circolazione di programmi virus, sia in caso di produzione degli stessi. Quanto all’elemento soggettivo, il reato è punibile a titolo di dolo generico, consistente nella coscienza e volontà della condotta con la consapevolezza dell’idoneità del virus a danneggiare un sistema informatico o telematico, a prescindere dalla finalità dell’agente.

Più pesante, dunque, la nuova formulazione dell’articolo 615-*quinquies* che, oltre a punire la diffusione di software, o comunque codice maligno, diretto a danneggiare il flusso dati o un intero sistema telematico, estende le condotte tanto da includere il procurarsi, l’importare software e hardware adatti allo scopo.

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

*“Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.*

*Tuttavia si procede d'ufficio e la pena è della reclusione da 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".*

L'art. 617-*quater*, c.p. e il successivo art. 617-*quinquies*, c.p. tutelano la libertà e la riservatezza delle comunicazioni informatiche o telematiche, al fine di garantirne la riservatezza e l'autenticità dei contenuti.
La condotta materiale prevista dal I comma dell'art. 617- *quater*, c.p. (intercettazione abusiva) è autonoma rispetto alla condotta prevista nel comma II dello stesso articolo (rivelazione), di talché, può benissimo sussistere il delitto di divulgazione di comunicazioni intercettate senza che sussista quello di intercettazione fraudolenta.
Infatti, con la fattispecie in oggetto, il legislatore ha inteso circoscrivere il divieto di divulgazione alle comunicazioni che per poter essere conosciute, a cagione del mezzo di comunicazione utilizzato, hanno bisogno di essere intercettate - c.d. "comunicazioni chiuse" - mentre tale divieto non è previsto per le comunicazioni che, per il mezzo usato, possono essere legittimamente conosciute da un numero imprecisato di persone.
Sotto tale profilo, la materialità della condotta di cui al I comma (intercettazione abusiva) è più ristretta, nel senso che è punibile soltanto chi abbia intercettato una comunicazione in modo fraudolento, essendo irragionevole punire chi sia venuto a conoscenza di una comunicazione in modo casuale, per effetto, ad esempio, di inconvenienti o interferenze che a volte si verificano nei sistemi di trasmissione delle comunicazioni stesse.
E' perseguibile, invece, ai sensi dell'art. 617-*quater*, II comma, chi divulga comunicazioni intercettate delle quali sia comunque in possesso, per la semplice ragione che la divulgazione di comunicazioni intercettate c.d. "chiuse" non è legittima.
Di talché, i responsabili delle due violazioni possono essere anche soggetti del tutto diversi, proprio per l'autonomia delle due ipotesi di reato, desumibile anche dallo stesso tenore letterale della norma.
In conclusione, il legislatore, con la fattispecie in oggetto, ha inteso circoscrivere il novero delle comunicazioni non divulgabili.

### 2.7. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (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.*

Anche la fattispecie in oggetto è posta a tutela della riservatezza delle comunicazioni.
La lettera dell'art. 617-*quinquies* c.p., concerne in genere le apparecchiature atte ad "intercettare le comunicazioni relative al sistema".
Il termine "intercettare" vuoi dire all'evidenza "inserirsi nelle comunicazioni riservate, traendone indebita conoscenza".
La digitazione indebita di un codice di accesso, proprio perché attua la prima comunicazione di qualsiasi utente con un sistema informatico o telematico viene sanzionata.
Di talché, anche la copiatura abusiva di dati di accesso riservati rientra nel concetto di intercettazione di comunicazioni telematiche.
L'attività illecita di intercettazione può essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico; tale è la digitazione da parte dell'operatore del codice di accesso di un sistema informatico.
Il recente indirizzo giurisprudenziale ritiene applicabile alla fattispecie in oggetto anche la forma del tentativo, essendo ben possibili atti idonei e diretti in modo non equivoco a cagionare un pericolo che invece, di fatto non sorge.
In conclusione, l'acquisizione di codici di accesso, qualunque sia l'obiettivo di profitto dell'agente, non esclude la configurabilità del reato di cui all'art. 617-*quinquies* c.p., nel caso di installazione non consentita di apparecchiature di intercettazione di comunicazioni con un sistema telematico o informatico.

## 2.8. Danneggiamento di informazioni, dati e programmi informatici (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 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".*

## 2.9. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (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 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".*

### 2.10 Danneggiamento di sistemi informatici o telematici (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) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".*

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

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

I reati di danneggiamento informatico di cui agli artt. 635-bis, 635-ter, 625-quater e 625-quinquies c.p., presentando caratteristiche comuni, vengono trattati cumulativamente nel presente paragrafo.
Per danneggiamento informatico si intende un comportamento diretto a cancellare, distruggere, deteriorare, rendere in tutto o in parte inservibili sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui.
L'evento offensivo è rappresentato proprio dal danneggiamento dei predetti beni.
Per distruzione si intende l'eliminazione "fisica", totale o quantomeno tale per cui la parte residua non possa più essere utilizzata. Il deterioramento, trattandosi di un attacco alla funzionalità, invece lo compromette solo in parte.
Quando si parla di danneggiamento bisogna distinguere tra il danneggiamento che ha come fine la distruzione di sistemi informatici o telematici, quindi programmi,

informazioni o dati, e quello che invece ha come obiettivo il deterioramento degli stessi.
Se il danneggiamento è operato su sistemi informatici dello Stato o di altro ente pubblico o su sistemi di pubblica utilità le pene sono aumentate così come previsto dagli articoli che precedono.
Il reato di danneggiamento prevede anche la forma del tentativo nell'ipotesi, per esempio, in cui un soggetto, avviando un programma con il fine specifico di danneggiarlo o di deteriorarlo, non riesce a raggiungere tale obiettivo per cause a lui indipendenti (perché, ad esempio, i mezzi di "protezione" del sistema riescono a disattivare o comunque a neutralizzare l'operatività del virus).
Il dolo nei reati in oggetto è generico e deve essere diretto a distruggere, deteriorare o rendere in tutto o in parte inservibili sistemi informatici o telematici, o programmi, dati, informazioni altrui.
Il reato, tuttavia, è perfezionato anche dal soggetto che decide di agire nel dubbio della realizzazione dell'evento dannoso (es., l'agente è a conoscenza del fatto che l'installazione di un particolare software o il compimento di determinate operazioni meccaniche su un dato computer possa provocare danni a dati o informazioni in esso contenute e nonostante tale consapevolezza decide di procedere).

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

*"Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro".*

Definizioni:
**Firma elettronica:** è definita all'art. 1 del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, così come recentemente modificato dal D. Lgs. 159/2006): *insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.*
Questa definizione di firma elettronica *tout-court,* chiamata dalla dottrina firma "debole", si ispira all'art. 2 del d.lgs. 10/2002, con la sola modifica della locuzione 'autenticazione informatica' che ora è sostituita con 'identificazione informatica'. Non esistendo tuttora norme che disciplinino con chiarezza cosa si debba fare in pratica per ottenere una firma cd. "debole", occorre riferirsi all'art. 2 della Direttiva 1999/93/CE e al suo all'allegato III, che disciplina i requisiti dei dispositivi atti a creare una firma "sicura", e ragionare per esclusione. Mentre nella categoria di firme avanzate appare possibile far rientrare la firma digitale e, per via della loro robustezza, tutti i sistemi di crittazione asimmetrica, nell'altra categoria sembrerebbero essere compresi tutti gli altri metodi, a cominciare dagli algoritmi simmetrici, che non sembrano soddisfare i requisiti di "firma sicura".

**Firma elettronica qualificata**: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati *successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma".*
Viene ricompresa in questo campo sia quella che prima di tale provvedimento era chiamata "firma elettronica avanzata" e la vecchia "firma elettronica qualificata", con l'aggiunta però dei requisiti del certificato qualificato e del dispositivo sicuro.
**Firma digitale***: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".*
**Certificatore:** *il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.*
Il delitto di frode informatica molto spesso concorre con altri delitti informatici, quali l'accesso informatico abusivo e il danneggiamento informatico in conseguenza a detenzione e diffusione abusiva di codici di accesso a sistemi informatici o a diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.
Il profitto dell'agente può anche "non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale".

## CAPITOLO 3.
## *Ratio* della disciplina introdotta dall'art. 24-bis D.Lgs. n. 231/2001 e aree di rischio correlate.

Una funzione preventiva efficace si rivela la sensibilizzazione delle aziende a potenziare una politica di sicurezza informatica, atteso che qualsiasi reato tecnologico può essere impedito soltanto con adeguate contromisure tecnologiche.
Gran parte delle aziende, oggi, sono criticamente dipendenti dall'efficace gestione delle informazioni e delle relative tecnologie informatiche, dipendenza che porta però ad una crescente vulnerabilità ad un ampio spettro di minacce, quali cyber attacchi, gravi incidenti aziendali causati dal malfunzionamento dei sistemi, ecc., anche considerando la notevole complessità portata dal moltiplicarsi di protocolli di accesso e comunicazione (UMTS, WiMax, ecc.), dei canali di trasmissione dei dati (ADSL, fibra, satellite, bluetooth, ecc), dei contenuti e delle applicazioni multimediali e on-line, dell'hardware disponibile per accedere ai dati (palmare, PC, notebook).

Per quanto riguarda i crimini informatici, i rischi riguardano soprattutto l'area dei dati; è dunque possibile ricondurre alle seguenti categorie le condotte che comportano seri rischi per la sicurezza:

1. eventi cagionati dai dipendenti, che possono consistere in: sottrazione di credenziali di autenticazione, distruzione o perdita di dati, trattamento dei dati non consentito, disattenzione o incuria, comportamenti sleali o fraudolenti, errore materiale;
2. eventi determinati dall'utilizzo di strumenti: azione di virus informatici, spamming, malfunzionamento, indisponibilità o degrado degli strumenti, utilizzo di codici di accesso non autorizzati, accessi esterni non autorizzati, intercettazione di informazioni in rete;
3. eventi relativi al contesto fisico-ambientale: ingressi non autorizzati a locali/aree ad accesso ristretto, sottrazione di strumenti contenenti dati, eventi distruttivi, naturali o artificiali nonché dolosi, accidentali o dovuti ad incuria, guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.), errori umani nella gestione della sicurezza fisica.

## CAPITOLO 4.
## Le Attività Sensibili di ECOSAVONA con riferimento ai reati informatici

Come rilevato in precedenza, in relazione all'attività aziendale svolta nello specifico da ECOSAVONA, i reati di cui all'art. 24-bis del D.Lgs. n. 231/2001, sono da ritenersi solo astrattamente configurabili.
In ogni caso sono state individuate le seguenti attività sensibili:

- Gestione dei sistemi informatici;
- Gestione circolazione dei dati informatici;
- Gestione utilizzo di informazioni, dati e programmi informatici;
- Gestione del trattamento dei dati personali.

Eventuali segnalazioni circa aree di attività a rischio specifiche potranno essere eventualmente individuate ed integrate nel presente documento dal Consiglio di Amministrazione anche su segnalazione dell'Organismo di Vigilanza, al fine di definire gli opportuni provvedimenti operativi.

## CAPITOLO 5.

## Definizione delle procedure per la prevenzione dei reati di cui all'art. 24-*bis* D.Lgs. n. 231/2001

ECOSAVONA ha adottato specifiche procedure per la formazione e l'attuazione delle decisioni societarie.
La formazione e l'attuazione delle decisioni degli Amministratori sono disciplinate oltre che dai principi e dalle prescrizioni contenute nelle disposizioni di legge vigenti, anche dai principi codificati nello Statuto Sociale e nel Codice Etico.

Si deve osservare che l'utilizzo degli strumenti informatici - coerentemente ai principi del D.Lgs. n. 231/01 - deve avvenire seguendo le procedure interne e nel rispetto del DPS ex D. Lgs. n. 196/2003; di ogni contatto/passaggio deve essere data debita evidenza e conservata traccia.

Il Responsabile Interno della Funzione Sistemi Informativi (di seguito anche: SI) dovrà presidiare e monitorare costantemente le attività a rischio nonché l'adeguamento e il rispetto dei presidi in materia di reati informatici.

Inoltre il Responsabile della Funzione SI deve:
- comunicare - attraverso la redazione di *report* informativi – all'AD ed all'Organismo di Vigilanza qualunque anomalia o criticità riscontrata nel corso dello svolgimento dell'attività nell'ambito della funzione di competenza;
- verificare la concreta ed efficace attuazione – nell'ambito delle funzioni di competenza – delle procedure aziendali e dei principi di cui al presente Modello di Organizzazione e Gestione.

### 5.2. I principi generali di comportamento

Agli Organi Sociali e ai Dirigenti di ECOSAVONA, in via diretta, nonché a lavoratori Dipendenti, Collaboratori e i Consulenti, soggetti a vigilanza, è fatto divieto di:

- alterare/manomettere/danneggiare il funzionamento di sistemi informatici o telematici al fine di procurare un vantaggio o un interesse per la società;
- intervenire illegalmente con qualsiasi modalità su dati, informazioni o programmi informatici, al solo fine di procurare un vantaggio o un interesse per la società;
- intercettare, impedire o interrompere illecitamente o diffondere comunicazioni informatiche o telematiche al fine di procurare un vantaggio o un interesse per la società;

- Installare nella rete aziendale un proprio software che non rientri nello scopo per cui il sistema informatico è stato assegnato all'utente per evitare che possa interrompere, danneggiare, manomettere, o impedire le comunicazioni informatiche aziendali;
- Prestare o cedere a terzi qualsiasi apparecchiatura informatica senza la preventiva autorizzazione del Responsabile interno;
- Evitare di trasferire all'esterno dell'azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'azienda stessa o di altra società collegata a ECOSAVONA, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del Responsabile interno;
- Astenersi dall'effettuare copie non autorizzate di dati o di software;
- Evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile dei Sistemi Informatici;
- Alterare, contraffare, documenti informatici, pubblici o privati;
- Accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati, in ogni caso di soggetti "esterni" al fine di manomettere dati o carpire informazioni riservate;
- Accedere abusivamente al sistema informatico o telematico della società al fine di alterare e/o cancellare dati o informazioni;
- Detenere e/o utilizzare abusivamente codici di accesso di società o soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- Svolgere attività di intercettazione, impedimento, interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti pubblici o privati, al fine di acquisire informazioni riservate;
- Modificare, cancellare, danneggiare, distruggere dati, informazioni, programmi di soggetti privati, o soggetti pubblici o comunque di pubblica utilità.

## CAPITOLO 6.
## I Protocolli di controllo comuni nell'ambito dei reati informatici

In materia di reati informatici e trattamento illecito dei dati, occorre garantire la protezione del patrimonio informativo da parte delle Direzioni e delle singole Unità organizzative e assicurare il corretto utilizzo delle risorse tecnologiche, nonché disporre di evidenze che documentino l'efficacia dei controlli implementati.

I protocolli di controllo comuni alle attività a rischio reato devono essere volti a:

- definire politiche di sicurezza delle informazione attraverso la corretta gestione e uso delle password, prevedendone anche l'aggiornamento periodico obbligatorio a tutti gli utenti;
- stabilire l'obbligo di mantenere la riservatezza della password;
- prevedere controlli sulla rete aziendale e sulle informazioni che vi transitano;
- prevedere corsi di aggiornamento/formazione sui principali pacchetti informativi in dotazione (in particolare sul corretto utilizzo delle posta elettronica), e la distribuzione di un breviario sul corretto utilizzo delle dotazioni informatiche a ciascun dipendente;
- limitare l'accesso internet a siti aziendalmente utili e moralmente leciti;
- inibire, come policy aziendale, l'utilizzo delle e-mail spamming;
- prevedere l'inventario aggiornato dell'hardware e del software in uso agli utenti;
- prevedere il tracciamento degli accessi degli utenti alla rete aziendale;
- prevedere l'adozione di meccanismi di segregazione delle reti:
- prevedere la sicurezza fisica dei siti ove risiedono i sistemi IT;
- prevedere una politica per l'uso di controlli crittografici per la protezione delle informazioni;
- prevedere procedure che regolamentano la firma digitale dei documenti, disciplinando il responsabile, i livelli autorizzativi, l'utilizzo del sistema di certificazione, eventuale utilizzo e invio di documenti;
- creare una struttura di esperti informatici (di riporto diretto al presidente del C.d.A. o alla Direzione del Personale) che monitorano l'adempimento alle prescrizioni aziendali in materia di sicurezza informatica ed aggiornano i sistemi di sicurezza alla luce delle nuove forme di "invasione";
- prevedere l'aggiornamento del sistema antivirus/antispamming periodico;
- controllare il regolare aggiornamento del Documento programmatico sulla sicurezza;

- stabilire l'assegnazione nominale di PC aziendali (non lasciare mai la disponibilità dei PC aziendali ad outsoucer etc. se non si crea una identificazione dell'utilizzatore);
- prevedere il rispetto delle leggi e dei regolamenti applicabili in tema di protezione e sicurezza dei dati informatici, di cui al D.lgs. n. 196/2003.

ECOSAVONA ha definito ed attuato un'apposita procedura per la gestione della privacy, in conformità al Regolamento UE 679/2016 (GDPR), che stabilisce le misure di sicurezza, tecniche ed organizzative, che la Società ha adottato per garantire un'adeguata protezione dei dati personali trattati, a seguito dell'effettuazione della valutazione dei rischi che incombono sui trattamenti di dati personali, in funzione della relativa probabilità e gravità di verificarsi.
Tali misure di sicurezza comprendono le modalità di trattamento dei dati personali sia su supporto cartaceo, sia su supporto digitale, mediante strumenti elettronici, che tutto il personale si impegna ad adottare per garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

La procedure permettono, altresì, di portare a conoscenza di tutti i Dipendenti e dei Collaboratori i limiti di utilizzo delle risorse informatiche assegnate per lo svolgimento delle mansioni lavorative, nonché di informare gli utilizzatori stessi circa la possibilità che l'azienda effettui dei controlli sulle corrette modalità di utilizzo dei beni con il solo fine di assicurare e preservare l'integrità degli strumenti stessi, evitare la commissione di illeciti e verificare la funzionalità del sistema.

La società, ha individuato le varie figure preposte al trattamento dei dati ("Titolare", "Responsabile" e "Incaricati) e sono analizzate le situazioni aziendali e le misure che la stessa ha adottato, ed adotterà, a garanzia della sicurezza nel trattamento dei dati.