
**Parte Speciale “H”:**
**I reati informatici**

**MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO**

**AGGIORNATO DA**

**EMAK s.p.a.**

**con delibera del Consiglio di Amministrazione**
**del 31Gennaio 2014**

Parte Speciale “H”

**1. I reati informatici ex art. 24-bis D.Lgs. 231/01**

Il D.Lgs. 231/01 ha recepito con la Legge n. 48, art. 7, del 18 marzo 2008, pubblicata in G.U. n. 80 del 4 aprile 2008, la **Convenzione del Consiglio d’Europa sulla criminalità informatica**, redatta a Budapest il 23 novembre 2001; convenzione suddivisa nei seguiti quattro capitoli:

1. misure normative di diritto penale sostanziale con la precisazione che le sanzioni da adottare da parte degli Stati devono essere effettive, proporzionate, dissuasive e comprendenti anche pene detentive;
2. misure procedurali che riguardano il perseguimento dei reati contenuti nel capitolo primo;
3. norme di coordinamento in tema di cooperazione internazionale;
4. clausole finali.

A seguito della ratifica ed esecuzione della Convenzione suddetta dopo l’art. 24 del D.Lgs. 231/01 è stato inserito l’art. 24bis “*Delitti informatici e trattamento illecito di dati”.*

Il recepimento della convenzione ha esteso la responsabilità amministrativa degli enti ai seguenti reati informatici:

- accesso abusivo ad un sistema informatico o telematico (art. 615ter c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da latro ente pubblico o comunque di pubblica utilità (art. 635ter c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635quinquies c.p.);

con previsione di sanzione pecuniaria da cento a cinquecento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere a), b) ed e).

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater c.p.);
- diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615quinqiues c.p.);

con previsione di sanzione pecuniaria sino a trecento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere b) ed e).

- falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491bis c.p.);
- frode informatica del certificatore di firma elettronica (art. 640quinquies c.p.).

con previsione di sanzione pecuniaria sino a quattrocento quote e sanzioni interdittive previste dall'art. 9 comma 2 lettere c), d) ed e).

***2. Aggiornamento normativo: i nuovi reati presupposto ex D.lgs 231/01 introdotti dal D.L 24 agosto 2013 n. 93 c.d. "Decreto Fare"***

D.L. 24 agosto 2013 n. 93 intitolato "Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province" pubblicato in Gazzetta Ufficiale n. 191 del 16.08.2013 ed entrato in vigore il 17.08.2013 ha ampliato il novero dei reati nell'ambito della criminalità informatica.

Tale novella, all'art. 9 comma II, statuisce infatti che:

*"All'articolo 24-bis, comma 1, del decreto legislativo 8 giugno 2001, n. 231, le parole "e 635-quinquies" sono sostituite dalle seguenti: ", 635-quinquies e 640-ter, terzo comma," e dopo le parole: "codice penale" sono aggiunte le seguenti: "nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231, e di cui alla Parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196."*

Riformulando così l'art. 24-bis DLGS. 231/01 nel modo che segue:

*Art. 24-bis, D.Lgs. 231/2001 - Delitti informatici -*

*1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-ter, terzo comma del codice penale nonché dei delitti di cui agli articoli 55, comma 9, del decreto*

*legislativo 21 novembre 2007, n. 231, e di cui alla Parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196, 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 di delitti di cui agli artt. 491 bis e 640 quinquies del Codice Penale, salvo quanto previsto dall'art. 24 del presente decreto per i casi di frode informatica in danno allo 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).*

***

In seguito all'emanazione del D.L. 93/2013 è stato innanzitutto introdotto nel catalogo dei reati presupposto la nuova aggravante ad effetto speciale del delitto di frode informatica di cui all'art. 640-*ter* comma 3 del codice penale.

Il delitto in oggetto andrà ad integrarsi qualora la frode informatica venga commessa con sostituzione dell'identità digitale in danno di uno o più soggetti. Con tale norma il legislatore ha voluto dunque implementare la tutela dell'identità digitale, punendo più severamente le frodi realizzate mediante l'accesso abusivo ad un sistema informatico attuato attraverso l'indebito utilizzo dell'identità digitale altrui.

- ***Art. 640-ter, terzo comma, c.p. (1)(2)***
  ***"Frode Informatica"***

*1. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

*2. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.*

*3. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti (3).*

*4. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante (4).*

---

*(1) Articolo aggiunto dall'art. 10, L. 23 dicembre 1993, n. 547, che modifica ed integra le norme del codice penale o del codice di procedura penale in tema di criminalità informatica.*
*(2) Per l'aumento della pena per i delitti non colposi di cui al presente titolo commessi in danno di persona portatrice di minorazione fisica, psichica o sensoriale, vedi l'art. 36 della L. 5 febbraio 1992 n. 104, così come sostituito dal comma 1 art. 3 della L. 15 luglio 2009 n. 94.*
*(3) Comma inserito dalla lett. a) del comma 1 dell'art. 9, D.L. 14 agosto 2013, n. 93.*
*(4) Comma così modificato dalla lett. b) del comma 1 dell'art. 9, D.L. 14 agosto 2013, n. 93.*

## 2. Aree di attività a rischio

In considerazione della tipologia di attività svolta da Emak, è astrattamente ipotizzabile la commissione dei seguenti reati:

**Art. 24 bis comma 1 D.Lgs. 231/2001**

- **accesso abusivo ad un sistema informatico o telematico (art. 615ter 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 palesamente armato;*

  *3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.*

  *Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.*

  *Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.*

  La norma non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "*ius excludendi alios*", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati sia che titolare dello "*ius excludendi*" sia persona fisica, sia giuridica, privata o pubblica, o altro ente.

Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi un'effettiva lesione alla stessa.

L'art. 1 della Convenzione di Budapest chiarisce che per "sistema informatico" si considera "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati".

Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di un software che permette il loro funzionamento elaborando delle informazioni (o comandi).

Nel medesimo articolo è contenuta la definizione di "dato informatico", che descrive il concetto derivandolo dall'uso: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informativo di svolgere una funzione".

- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617quater 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*

- **installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617quinquies c.p.)**

  *Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*

  *La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617quater c.p..*

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

  *Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*

  *Se ricorre una o più delle circostanze di cui al 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.*

  Antecedentemente all'entrata in vigore della *legge 23 dicembre 1993 n. 547* (in tema di criminalità informatica), che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi *dell'art. 635 cod. pen.* in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore. (Nell'affermare detto principio, la Corte ha precisato che tra il delitto di cui *all'art. 635 cod. pen.* e l'analoga speciale fattispecie criminosa prevista dall'*art. 9 della legge n. 547 del 1993* - che ha introdotto *l'art. 635-bis cod. pen.* sul danneggiamento di sistemi informatici e telematici - esiste un rapporto di successione di leggi nel tempo, disciplinato *dall'art. 2 cod. pen.).*

- **danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635ter 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, la pena è della reclusione da tre a otto anni.*

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

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

  *Salvo che il fatto non costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, rende, il 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 una o più delle circostanze di cui al secondo comma dell'art. 635 c.p., ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è la reclusione da due a sette anni.*

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

  *Se il fatto di cui all'art. 635quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolare 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'art. 635 c.p. ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

Gli articoli del Codice Penale summenzionati, previsti nel comma 1 dell'art. 24 bis D.Lgs. 231/2001, hanno come fattore comune il "danneggiamento informatico": si parla di danneggiamento informatico quando, considerando la

componente hardware e software, interviene una modifica tale da impedirne il funzionamento, anche solo parziale.

**Art. 24 bis comma 2 D.Lgs. 231/2001**

- **detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater 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 euro 5.164.*
  *La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.*
- **diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615quinqiues c.p.)**
  *Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329.*

Gli articoli del Codice Penale summenzionati, previsti nel comma 2 dell'art. 24 bis D.Lgs. 231/2001, hanno come fattore comune la detenzione o diffusione di codici o programmi atti al danneggiamento informatico. Da un punto di vista tecnico, gli artt. 615quater e 615 quinquies possono essere considerati accessori ai precedenti artt. 615ter, 635bis, 635ter e 635quater: la detenzione o dissezione di codici di accesso o la detenzione o diffusione di programmi o dispositivi diretti a danneggiare o interrompere un sistema telematico, di per sé non compiono alcun danneggiamento, se non utilizzati per un accesso abusivo ad u sistema o nella gestione di un'intercettazione di informazioni.

**Art. 24 bis comma 3 D.Lgs. 231/2001**

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

  *Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, 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*.

  Il reato si configura nella falsità concernente direttamente i dati o le informazioni dotati, già di per sé, di efficacia probatoria relativa a programmi specificatamente destinati ad elaborarli indipendentemente da un riscontro cartaceo. Si chiarisce inoltre nella norma che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.
- **frode informatica del certificatore di firma elettronica (art. 640quinquies c.p.)**

  *Il certificatore che, violando gli obblighi previsti dall'art. 32 del codice dell'amministrazione digitale, di cui al D. Lgs. 82/2005 e suc. Mod., per il rilascio di un certificato, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione fino a tre anni o con la multa fino a 25.000 Euro.*

### *2.1 Aggiornamento normativo: i nuovi reati presupposto ex D.lgs 231/01 introdotti dal D.L 24 agosto 2013 n. 93 c.d. "Decreto Fare"*

D.L. 24 agosto 2013 n. 93 intitolato "Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province" pubblicato in Gazzetta Ufficiale n. 191 del 16.08.2013 ed entrato in vigore il 17.08.2013 ha ampliato il novero dei reati nell'ambito della criminalità informatica.

Tale novella, all'art. 9 comma II, statuisce infatti che:

*"All'articolo 24-bis, comma 1, del decreto legislativo 8 giugno 2001, n. 231, le parole "e 635-quinquies" sono sostituite dalle seguenti: ", 635-quinquies e 640-ter, terzo comma," e dopo le parole: "codice penale" sono aggiunte le seguenti: "nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231, e di cui alla Parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196."*

Riformulando così l'art. 24-bis DLGS. 231/01 nel modo che segue:

*Art. 24-bis, D.Lgs. 231/2001 - Delitti informatici -*

*1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-ter, terzo comma del codice penale nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231, e di cui alla Parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196, 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 di delitti di cui agli artt. 491 bis e 640 quinquies del Codice Penale, salvo quanto previsto dall'art. 24 del presente decreto per i casi di frode informatica in danno allo 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).*

***

In seguito all'emanazione del D.L. 93/2013 è stato innanzitutto introdotto nel catalogo dei reati presupposto la nuova aggravante ad effetto speciale del delitto di frode informatica di cui all'art. 640-*ter* comma 3 del codice penale.

Il delitto in oggetto andrà ad integrarsi qualora la frode informatica venga commessa con sostituzione dell'identità digitale in danno di uno o più soggetti. Con tale norma il legislatore ha voluto dunque implementare la tutela dell'identità digitale, punendo più severamente le frodi realizzate mediante l'accesso abusivo ad un sistema informatico attuato attraverso l'indebito utilizzo dell'identità digitale altrui.

- ***Art. 640-ter, terzo comma, c.p. (1)(2)***

  ***"Frode Informatica"***

*1. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

*2. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.*

*3. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti (3).*

*4. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante (4).*

* * *

Gli articoli del Codice Penale summenzionati, previsti nel comma 3 dell'art. 24 bis D.Lgs. 231/2001, disciplinano illeciti che, a differenza di quelli sopradescritti (veri e propri reati informatici), sono compiuti attraverso l'uso di un sistema informatico.

---

*(1) Articolo aggiunto dall'art. 10, L. 23 dicembre 1993, n. 547, che modifica ed integra le norme del codice penale o del codice di procedura penale in tema di criminalità informatica.*

*(2) Per l'aumento della pena per i delitti non colposi di cui al presente titolo commessi in danno di persona portatrice di minorazione fisica, psichica o sensoriale, vedi l'art. 36 della L. 5 febbraio 1992 n. 104, così come sostituito dal comma 1 art. 3 della L. 15 luglio 2009 n. 94.*

*(3) Comma inserito dalla lett. a) del comma 1 dell'art. 9, D.L. 14 agosto 2013, n. 93.*

*(4) Comma così modificato dalla lett. b) del comma 1 dell'art. 9, D.L. 14 agosto 2013, n. 93.*

**3. Destinatari della parte speciale: Comportamenti vietati e principi generali di condotta**

Nell'espletamento della propria attività per conto di Emak, gli Amministratori, i Sindaci, i soggetti che operano per la Società di revisione, i dirigenti ed i dipendenti di Emak devono rispettare le norme di comportamento di seguito indicate.
A tutti i soggetti sopra indicati è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato richiamate nella presente Parte Speciale "H";
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

In particolare è fatto obbligo:

- all'Amministratore del Sistema di denunciare al DAF eventuali accessi al sistema informatico aziendale da parte di hacker;
- ai dipendenti, dirigenti ed amministratori di attenersi al **Regolamento Aziendale per l'Utilizzo del Sistema Informatico (Codice Procedura PRY01)** relativo a:
  - utilizzo del personal computer;
  - utilizzo della rete Emak;
  - gestione delle password;
  - utilizzo dei supporti magnetici;
  - utilizzo dei pc portatili;
  - uso della posta elettronica;
  - uso della rete Internet e dei relativi servizi;
  - policy in materia di privacy e riservatezza del know-how.
  -

Pertanto, è nello specifico fatto divieto:

- ai dipendenti, dirigenti ed amministratori di installare nella rete aziendale un proprio software che non rientri 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;
- ai dipendenti, dirigenti ed amministratori di installare nella rete aziendale un proprio software che possa impedire o interrompere

o danneggiare le comunicazioni informatiche aziendali ovvero l'intero sistema informatico aziendale.

E', comunque, necessario:

- che sia garantito il rispetto del Codice Etico Emak;
- che tutte le attività e le operazioni svolte per conto di Emak siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza.

Nel **Documento Programmatico sulla Sicurezza (Codice Procedura PRY02)** sono analizzate le situazioni aziendali ed organizzate le procedure a garanzia della sicurezza nei trattamenti dei dati. In particolare, per quel che riguarda il rischio analizzato nel presente capitolo, è volta l'analisi:

- dei server;
- delle misure di sicurezza per i trattamenti informatici;
- degli strumenti antivirus;
- dei sistemi anti-intrusione;
- dei firewall;
- dei piani di Disaster Recovery.

**4. Responsabilità delle Operazioni**

Sono considerati Responsabili per ogni singola operazione a rischio all'interno delle aree sopra individuate i Responsabili delle Funzioni all'interno delle quali vengono svolti i processi a rischio, i Consiglieri di Amministrazione e di Dirigenti.

E' compito dei Responsabili di Funzione, con particolare riferimento al Responsabile della Sicurezza dei Sistemi Informativi, portare a conoscenza dell'OdV, tramite appositi moduli:

a) la piena conoscenza da parte dei vari Responsabili e dei sottoposti del processo da seguire e degli obblighi da osservare nello svolgimento dell'operazione, con dichiarazione di conformità al D.Lgs 231/01;
b) l'elencazione dei principali adempimenti effettuati nell'espletamento dell'attività di controllo e verifica.