



Modello di organizzazione gestione e controllo ai
sensi del D.Lgs 231/2001

Parte Speciale

Sezione

Delitti informatici e trattamento illecito dei dati

Rev. 1.0 06/2019

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
Rev 0.0		Prima emissione	
Rev 1.0	Giugno 2019	Conferma senza variazioni	

INDICE

1.1 Descrizione fattispecie di reato	4
1.2 Processi e attività sensibili	7
1.3 Principi di comportamento	7
1.4 Protocolli Specifici	8

1.1 Descrizione fattispecie di reato

La presente Sezione si riferisce ai delitti informatici e trattamento illecito dei dati.

Si descrivono a seguito le singole fattispecie di reato contemplate dall'art. 24-bis del D.Lgs 231/2001 (articolo aggiunto dalla L. 48/2008).

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

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria (1), si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

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

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio (1). (1) Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, 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 di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 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.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quatet 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 (1). (1) Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.

Installazione di apparecchiature atte ad intercettare, impedire o 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 (1). (1) Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.

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 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.

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 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata. (1)

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

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

(1) Articolo inserito dalla L. 18 marzo 2008, n. 48.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 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.

(1) Articolo inserito dalla L. 18 marzo 2008, n. 48.

Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sè 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.

1.2 Processi e attività sensibili

I processi e le attività sensibili ritenuti più a rischio per Chiari Servizi srl sono principalmente:

Descrizione Reati	Processo	Attività sensibili
art. 615-ter c.p. Accesso abusivo ad un sistema informatico o telematico; art. 635-bis c.p. Danneggiamento di informazioni dati e programmi informatici; art. 635-quater c.p. Danneggiamento di sistema informatici o telematici; art.635-ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da un altro ente pubblico o comunque di utilità pubblica.	Gestione sistema informatico e telematico	Sicurezza e protezione dei dati residenti presso gli archivi della società. Utilizzo di banche dati interne/esterne. Accesso al sistema informatico e telematico. Utilizzo software coperti da licenze/copyright.

I destinatari delle disposizioni contenute nella presente Sezione sono tutti i soggetti coinvolti nei processi sopra identificati ed in particolare:

- Responsabili di sistema;
- Responsabili trattamento dati e incaricati trattamento dei dati (ai sensi del D.lgs 196/03);
- Responsabili ICT.

1.3 Principi di comportamento

I principi di comportamento e le disposizioni della Parte Speciale si applicano a tutti gli amministratori, dipendenti, collaboratori e fornitori / partner di Chiari Servizi srl che intervengono e sono coinvolti nei processi aziendali sopra identificati.

Lo scopo della presente Sezione è di:

- indicare protocolli e procedure da osservare per la corretta applicazione del Modello;
- fornire ai responsabili di area processo o funzione l'elenco dei flussi informativi da trasmettere all'Organismo di Vigilanza incaricato di svolgere le attività di verifica e controllo.

Ai soggetti sopra indicati è richiesto di:

- osservare regole e principi del Codice Etico di Comportamento;
- osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano la gestione dei sistemi informatici e telematici interni ed esterni;
- osservare scrupolosamente tutte le norme volte al mantenimento dell'integrità dei sistemi informatici e agire sempre rispettando le procedure interne che su tali norme si fondano;
- osservare la disciplina in materia di privacy e trattamento dei dati (D.lgs 196/2003).

E' fatto esplicito divieto di:

- manomettere e/o danneggiare i sistemi informatici attuando comportamenti non corretti dal punto di vista normativo;
- falsificare documenti informatici pubblici o aventi efficacia probatoria;
- accedere abusivamente a sistemi informatici o telematici;
- detenere o diffondere abusivamente codici d'accesso a sistemi informatici protetti;
- diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere i sistemi informatici;
- interrompere o impedire illecitamente comunicazioni informatiche interne;
- danneggiare dati, informazioni o programmi informatici (sono inclusi anche quei dati necessari nei rapporti Società-Stato, con altri enti pubblici);
- utilizzare illegalmente password di computer, codici di accesso o informazioni per compiere una delle condotte di cui sopra;
- accedere illegalmente e duplicare banche dati.

1.4 Protocolli Specifici

Ad integrazione del Codice Etico di Comportamento e dei principi sopra elencati sono stati adottati dalla Società alcuni protocolli specifici. I protocolli individuati siano essi formalizzati in apposite procedure aziendali o in norme, condotte, policy, etc. hanno lo scopo di fornire un maggiore dettaglio operativo alle funzioni aziendali che operano nei processi e attività a rischio di commissione dei reati ex. D.Lgs 231/2001.

A seguito per ciascun Processo e Attività sensibile si riporta l'elenco delle funzioni coinvolte, delle procedure e dei protocolli adottati e dei flussi informativi da inoltrare all' Organismo di Vigilanza:

Processo: Gestione sistema informatico e telematico

Attività: Sicurezza e protezione dei dati residenti presso gli archivi della società. Utilizzo di banche dati interne/esterne. Accesso al sistema informatico e telematico. Utilizzo software coperti da licenze/copyright.

Unità organizzativa/ Responsabile interno	Documenti/Procedure	Protocolli	Flussi Odv
Organo amministrativo/ Responsabile Amministrazione e Personale	DPS. Istruzione Operative: IS.ERG.06 Gestione Back up dati informatici	Procedura/istruzioni con regole per utilizzo rete web, posta elettronica, sistemi telematici.	Comunicazione delle violazioni ai protocolli specifici previsti dal DPS e dalle procedure interne.