MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

(D.LGS. 231/2001)

PARTE SPECIALE

LIBELLULA ONLUS COOPERATIVA SOCIALE

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DELL'ART. 6 D.LGS 231/01

PARTE SPECIALE
Sezione
Reati Informatici

Revisione	Data	Elaborato da	Approvato da
Prima stesura	05/02/2019	Commissione Qualità	Cda
Revisione		Commissione Qualità	Cda

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

(D.LGS. 231/2001)

PARTE SPECIALE

INDICE

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

(D.LGS. 231/2001)

PARTE SPECIALE

1.1 Descrizione fattispecie di reato

La presente Sezione si riferisce ai reati Informatici.

*

L'art. **24 bis D.LGS 231/2001** è dedicato a "*Delitti informatici e trattamento illecito dati" e così recita: <<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. 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.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, e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all'ente la sanzione pecuniaria sino a quattrocento quote. 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)>>*.

*

I reati richiamati dalla norma sono in sintesi:

- **Art. 491*bis* c.p. Falsità in un documento informatico pubblico o avente efficacia probatoria. <<*Se alcuna delle falsità previste dal presente capo [ndr Falsità in atti] 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 fattispecie in questione punisce le condotte di falsità di cui agli artt. 476-493 c.p.aventi ad oggetto documenti informatici pubblici o privati aventi efficacia probatoria.La norma punisce sia la falsità c.d. materiale che la falsità ideologica; nel primo caso sifa riferimento all'ipotesi di un documento contraffatto nell'indicazione del mittente o nellafirma stessa, o ancora all'ipotesi di alterazione del contenuto dopo la sua formazione.L'ipotesi di falsità ideologica attiene, invece, alla non veridicità delle dichiarazioni contenute nel documento stesso;

- **Art. 615*ter* c.p. Accesso abusivo ad un sistema informatico o telematico. <<*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.***

  La pena è della reclusione da uno a cinque anni:

- ***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;***
- ***se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;***
- ***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 fattispecie di reato prevede e punisce chi si introduce o permane abusivamente in unsistema informatico o telematico protetto.

Fondamentale per la configurabilità del reato è che il sistema attaccato (anche se adibito ad un uso individuale) risulti protetto da "misure di sicurezza", che devono intendersi anche come misure genericamente di carattere organizzativo, che cioè disciplinino semplicemente le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo. Possono rilevare, esemplificando, la sistemazione dell'impianto all'interno di un locale munito di serrature, la prescrizione di una *password* di accesso, l'esclusione del personale impiegatizio, attraverso la rete interna del sistema, dall'accesso ai comandi centrali per intervenire sui dati, ecc. Si prescinde dall'accertamento del fine specifico di lucro o di danneggiamento del sistema.

E ' prevista la punibilità di due tipologie di condotte:

- introduzione abusiva (cioè senza il consenso del titolare dello *ius excludendi*) in un sistema informatico o telematico munito di sistemi di sicurezza;
- la permanenza in collegamento con il sistema stesso, continuando a fruire dei relativi servizi o ad accedere alle informazioni ivi contenute, nonostante vi sia stato il dissenso anche tacito del titolare (che è dimostrato anche dalla predisposizione di misure di protezione del sistema nel senso sopra descritto).

Si tratta di una fattispecie perseguibile a querela della persona offesa, salvo che non si verifichino le aggravanti di cui al comma 2 (danneggiamento/distruzione di dati, di programmi o del

sistema; interruzione totale o parziale del funzionamento del sistema; abuso della funzione di pubblico ufficiale, investigatore, operatore del sistema; utilizzo di violenza; accesso a sistemi di interesse pubblico).

- **Art. 615*quater* c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. <<*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, 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*>>.**

  Il reato in questione punisce le condotte di procacciamento, riproduzione, diffusione, comunicazione o consegna di codici, parole-chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto, con il fine di procurarsi un profitto o di arrecare un danno. Rispetto alla disposizione prevista dall'art. 615 ter c.p. vi è anticipazione della soglia di tutela poiché il reato sanziona condotte che riguardano i codici d'accesso e non direttamente i sistemi informatici che con tali codici possono essere aggrediti. Di qui la natura di reato di pericolo che va attribuita alla fattispecie in esame, che si consuma nel momento in cui l'agente, alternativamente, si procura o diffonde i codici di accesso ovvero fornisce indicazioni utili a tal fine, indipendentemente dall'effettivo danno o turbamento del sistema (ad esempio, a prescindere dall'effettivo utilizzo dei codici per accedere abusivamente nel sistema).

  Il reato è perseguibile d'ufficio e la condotta criminosa può limitarsi alla mera detenzione di mezzi o dispositivi idonei all'accesso abusivo (*virus*, *spyware)* e comunque è sanzionata la condotta di chi illegittimamente operi su codici di accesso, parole chiave o altri mezzi di accesso a sistemi informatici protetti da misure di sicurezza.

- **Art. 615*quinquies* c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. <<*Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, 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.*>>**

  Il reato punisce il procacciamento, la produzione, la riproduzione, l'importazione, la diffusione, la comunicazione, la consegna o la messa a disposizione in qualsiasi modo di programmi o dispositivi

volti a danneggiare sistemi informatici o telematici, o dati e programmi ivi contenuti, o comunque volti ad alterare il loro funzionamento.

Le condotte tipiche si realizzano mediante l'introduzione di *virus*, *worms*, programmi

contenenti le c.d. bombe logiche ecc. Potrebbe, pertanto, ipotizzarsi una responsabilità della società nel caso in cui tali condotte siano poste in essere ad esempio con la finalità di distruggere dati, documenti o evidenze di attività ipoteticamente illecite in vista di un controllo/ispezione delle autorità competenti.

Rispetto alla fattispecie precedente, questo reato richiede già la realizzazione di una condotta attiva idonea a realizzare il danneggiamento. Il reato è perseguibile d'ufficio.

- **Art. 617*quater* c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. <<*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da 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:***
    - ***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;***
    - ***da chi esercita anche abusivamente la professione di investigatore privato.>>***

Il reato in esame è inserito nella sezione V (delitti contro l'inviolabilità dei segreti), del capo III (delitti contro la libertà individuale), del titolo XII (delitti contro la persona) del libro secondo del codice penale.

L'articolo prevede tre ipotesi criminose:

1. il fatto di chiunque fraudolentemente intercetta una comunicazione proveniente da un sistema informatico o telematico o da più sistemi fra loro collegati;

2. il fatto di chiunque fraudolentemente interrompe o impedisce tali comunicazioni;

3. il fatto di chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni informatiche o telematiche di cui fraudolentemente abbia pre-

so conoscenza. Tale ipotesi è sussidiaria, infatti è prevista autonomamente solo se non costituisce un più grave reato.

Il tentativo di reato nei casi previsti dall'articolo in esame è ipotizzabile. Si tratta di un reato comune perchè può essere commesso da chiunque. La responsabilità è esclusivamente dolosa. Il dolo richiesto è quello generico, consistente nella coscienza e volontà di commettere una delle fattispecie previste. Le condotte consistono nell'intercettazione, impedimento o interruzione fraudolenta di comunicazioni relative ad un sistema informatico, nonché nella rivelazione all'esterno delle comunicazioni in tal modo raccolte. Si tratta di una fattispecie perseguibile a querela della persona offesa, salvo che non si verifichino le circostanze aggravanti di cui al comma 4 (danneggiamento di un sistema pubblico; abuso o violazione dei doveri della funzione di pubblico ufficiale, o della qualità di operatore del sistema).

- **Art. 617*quinquies* c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. <<*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.*>>**

  Trattasi di reato, perseguibile d'ufficio, che punisce la mera installazione di strumenti volti a rendere possibile l'intercettazione, l'impedimento o l'interruzione di comunicazioni telematiche o informatiche. Si prescinde dunque dalla realizzazione dell'intercettazione in concreto. Si tratta di una norma a tutela anticipata che mira a tutelare la riservatezza e la libertà delle comunicazioni con l'incriminazione di fatti prodromici rispetto all'effettiva lesione del bene giuridico.

  Il dolo è generico e consiste nella coscienza e volontà di installare apparecchiature in grado di intercettare comunicazioni informatiche o telematiche.

- **Art. 635*bis* c.p. Danneggiamento di informazioni, dati e programmi informatici. <<*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se 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.*>>**

  La condotta punita si concretizza nelle attività di distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui.

Il reato è punibile a querela della persona offesa, a meno che non ricorra una delle circostanze aggravanti previste dalla norma (violenza o minaccia contro persone o abuso della qualità di operatore del sistema).

- **Art. 635*ter* c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. <<*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se 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.*>>**

  La fattispecie punisce i fatti di danneggiamento previsti nel precedente art. 635*bis* c.p. riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

  Il reato è sempre perseguibile d'ufficio e per la sua realizzazione è sufficiente porre inessere "atti diretti" a realizzare gli eventi dannosi previsti, a prescindere dal loro concreto verificarsi.

- **Art. 635quater c.p. Danneggiamento di sistemi informatici o telematici. <<*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se 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.*>>**

  Il sistema sanzionatorio dei reati informatici è completato con l'introduzione di due fattispecie incriminatrici dirette a punire le condotte di danneggiamento che abbiano ad oggetto non singoli documenti o dati informatici, bensì il funzionamento di un sistema informatico.Il reato *de quo* punisce l'introduzione o la trasmissione di dati, informazioni o programmiche causino la distruzione, il danneggiamento, l'inservibilità o il grave malfunzionamentodi sistemi informatici o telematici. E' necessario che l'evento dannoso si verifichi in concreto.

- **Art. 635*quinquies* c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità. <<*Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il*

funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se 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.>>

L'articolo in questione punisce le stesse condotte criminose di cui all'art. 635*quater* c.p., anche se gli eventi dannosi, aventi come oggetto materiale sistemi informatici o telematici di pubblica utilità, non si realizzino concretamente.

- **Art. 640*quinquies* c.p. Frode informatica del certificatore di firma elettronica. <<*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>>.***

  Si tratta di un reato proprio che può essere commesso dal soggetto che presta servizi di certificazione di firma elettronica. Le condotte di reato si concretizzano nella generica violazione degli obblighi di legge per il rilascio di un certificato qualificato, con il dolo specifico di procurare a sé un vantaggio o un danno ad altri.

*

1.2 Processi e attività sensibili

I processi e le attività sensibili ritenuti più a rischio per la Cooperativa sono principalmente:

Processo	Attività sensibili
Gestione sistemi informativi e tutela della privacy	Sicurezza e protezione dei dati. Gestione delle password di accesso alle postazioni. Utilizzo di internet e posta elettronica. Gestione accessi ai sistemi telematici della PA. Gestione licenze e copyright programmi. Trattamento dati e autorizzazioni

I destinatari delle disposizioni contenute nella presente Sezione sono tutti i soggetti coinvolti nei processi sopra identificati.

*

1.3 Principi di comportamento

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

Lo scopo della 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;
- 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 (GDPR 679/2016).

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 e dei principi sopra elencati sono stati adottati dalla Cooperativa 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:

Unità organizzativa/ Responsabile interno	Documenti/Procedure	Protocolli	Flussi Odv
Responsabile Sistema Informativo/ Responsabile Privacy	INFRASTRUTTURE: SISTEMA INFORMATIVO REGOLAMENTO STRUMENTI INFORMATICI E POSTA ELETTRONICA - MANSIONARIO / DOTAZIONI / COMPUTER - ISTRUZIONI OPERATIVE	Adozione Registro Privacy in assenza di obbligo Adozione già dal 2016 di Regolamento Strumenti informatici in linea con Garante Privacy Autorizzazioni specifiche al trattamento dati Informative privacy secondo GDPR	Segnalazione violazioni Attività di report

		Accesso banche dati PA a persone autorizzate Accorgimenti per accesso alla struttura ai soli autorizzati. Sistemi di controllo Licenze e programmi fornite da Ente esterno Utilizzo sistemi di salvataggio file e archiviazione a tutela dei dati Diffusione ai dipendenti del Modello e Codice Etico e periodica formazione D.lgs. 231/01.	