SAL
Società Acqua Lodigiana srl

PARTE SPECIALE H

Reati informatici e trattamento illecito dei dai dati

Approvato dal Consiglio di Amministrazione di SAL S.r.l. nella seduta del 30/11/2020

Revisione 2 del 30/11/2020

Il Presidente SAL
Giuseppe Negri

Indice

Storico delle modifiche

Versione	Causale	Data
Prima Versione	Emissione	26/02/2014

Revisione corrente:

Versione	Causale	Data
Revisione 1	Aggiornamento	30/11/2020

PARTE SPECIALE "H" – REATI INFORMATICI

1. Le fattispecie dei delitti informatici richiamate dal D.Lgs. n. 231/2001

La legge 18 marzo 2008 n. 48 ha introdotto, nel testo del D.Lgs.231/01 l'art **24 bis** in base al quale:

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)".

Con l'introduzione dei reati sopra citati, il legislatore ha predisposto una duplice tutela che assicura:

- l'*integrità* dei sistemi informatici, ovvero la non alterabilità dei dati, delle informazioni e dei sistemi medesimi;
- la *disponibilità* e confidenzialità, ovvero la possibilità, solo da parte dei soggetti autorizzati, di accedere, disporre e conoscere delle informazioni,e del contenuto delle comunicazione;
- l'*autenticità*, ovvero la certezza, da parte del destinatario della comunicazione, dell'identità del mittente.

Tuttavia, come è stato correttamente osservato, non tutti i comportamenti correlati all'uso del computer, ancorché penalmente rilevanti, possono rientrare nel novero dei reati informatici, dovendo tale qualifica essere riservata, più correttamente, ai soli casi in cui il sistema informatico o altri beni informatici (quali dati o programmi) costituiscano l'oggetto materiale della condotta criminosa.

Nel campo tecnico, è tipico distinguere i **reati informatici in senso stretto** dai **reati commessi attraverso l'uso di un sistema informatico**.

I primi sono reati che hanno come obiettivo il sistema informatico o telematico altrui o i dati, le informazioni e i programmi ad esso pertinenti.
Si tratta dei reati descritti dagli artt. 615-*ter* – 615-*quinquies*, 617-*quater* e 617-*quinquies*, e 635-*ter* – 635-*quinquies* c.p.
Gli artt. 491-*bis* e 640-*quinquies* c.p. prevedono, invece, fattispecie di reato della seconda tipologia, cioè reati compiuti attraverso l'uso di un sistema informatico.
Di seguito si riporta una descrizione dei reati richiamati dall'art. 24-bis.

Documenti informatici (art. 491 -bis del codice penale)

"Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applica le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni";
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffa o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni";
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni";
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.): "Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476";
- Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni";
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.): "Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro";
- Falsità materiale commessa da privato (art. 482 c.p.): "Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un

pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo";

- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.): "Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi";
- Falsità in registri e notificazioni (art. 484 c.p.): "Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00";
- Falsità in scrittura privata (art. 485 c.p.): "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata";
- Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.): "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito";
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.): "Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480";
- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.): "Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private";
- Uso di atto falso (art. 489 c.p.): "Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno";
- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.): "Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente";
- Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.): "Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di

"scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti";

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

2. Le tipologie dei reati informatici (art. 24-bis del Decreto)

I reati informatici così richiamati per comodità espositiva sono raggruppabili nelle seguenti tipologie:

1. Reati informatici
2. Reati commessi attraverso l'uso di un sistema informatico

Qui di seguito è riportata la lettera degli articoli del Codice Penale che vengono in rilievo per la comprensione di ciascuna fattispecie, accompagnata da una sintetica illustrazione del reato e da una descrizione astratta a titolo esemplificativo delle attività potenzialmente a rischio-reato.

2.1. Reati informatici

Accesso abusivo a 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*".

In questo caso l'elemento oggettivo consiste nell'introdursi o mantenersi abusivamente in un sistema informatico o telematico; con il termine "abusivamente" si intende un

comportamento illegittimo del soggetto agente che compie, pertanto, l'azione senza alcun permesso.

Si precisa che il sistema informatico è quello destinato alla elaborazione dei dati e alla loro utilizzazione, mentre il sistema telematico è un mezzo attraverso il quale i sistemi informatici sono gestiti a distanza, mediante reti di comunicazione.

È un reato comune, potendo essere commesso da chiunque, di mera condotta in quanto si perfeziona nella semplice esecuzione dell'azione illecita e a forma libera.

L'elemento soggettivo consiste nel dolo generico, inteso come coscienza e volontà del fatto tipico previsto.

Dal punto di vista del concorso di reati, si può pensare ad una duplice imputazione anche per il reato di frode informatica (art. 640-ter c.p.); questo reato, tuttavia, presuppone necessariamente la manipolazione del sistema, elemento che invece non è necessario per la consumazione del reato in esame.

Si precisa inoltre che il reato presuppone l'accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza, caratteristica che invece non ricorre nel reato di frode informatica.

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda e solo per la seguente attività sensibile:

- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali ed inerenti l'attività contrattuale dell'Ente**
- **Accesso a sistemi informatici e telematici privati es. banca**

Dunque tale reato presupposto verrà successivamente analizzato.

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".

L'interesse tutelato è analogo a quello dell'articolo precedente.

L'elemento soggettivo consiste nel procurarsi abusivamente (ovvero agire per venire a conoscenza in maniera illegittima), riprodurre (ovvero eseguire una copia il più fedele possibile all'originale), diffondere (ovvero mettere a disposizione della collettività generale, attraverso i mezzi di pubblica informazione, la possibilità di percepire la notizia o il dato), comunicare (ovvero trasmettere la notizia o il dato a qualcuno), consegnare

(ovvero dare materialmente la cosa a qualcuno) e fornire indicazioni o istruzioni (ovvero trasmettere a taluno informazioni rilevanti relative ad un determinato dato).

L'oggetto della condotta non si riferisce a qualsiasi dato o notizia, ma in particolare ai codici, parole chiave, o qualunque altro strumento idoneo a permettere al soggetto di entrare in sistemi informatici e telematici protetti da sistemi di sicurezza. Il reato è comune - potendo essere commesso da chiunque - e la condotta è a forma vincolata, ovvero il reato si consuma solo se l'azione si svolge nelle modalità indicate dal legislatore. Il tentativo non è punibile.

L'elemento soggettivo è costituito dal dolo specifico, consistente nella previsione e volontà dell'azione unitamente al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno.

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda e solo per la seguente attività sensibile:

- **Utilizzo e detenzione di ID e/o password di accesso a portali internet o applicativi interni per i quali è necessario avere delle specifiche credenziali.**

Dunque tale reato presupposto verrà successivamente analizzato.

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".*

Il testo opera una significativa riforma del "vecchio" art. 615-quinquies c.p., che puniva (con identica sanzione) "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".

La norma sanziona non soltanto le condotte afferenti ai "programmi informatici", ma anche l'utilizzo illecito di "apparecchiature" e "dispositivi" in grado di danneggiare un sistema informatico, ovvero di alterarne il funzionamento.

Integra dunque il "nuovo" delitto di cui all'art. 615-quinquies c.p. non solo il procurarsi virus e malware in genere, ma anche la produzione, importazione, etc. di dongle, smartcard, skimmer e così via, laddove, naturalmente, si prestino ad un utilizzo illecito.

La nuova formulazione della norma amplia nettamente le condotte perseguibili, sanzionando non, solo chi diffonde, comunica, consegna o mette a disposizione programmi, apparecchiature o dispositivi, ma altresì chi produce, importa, si procura ovvero riproduce tali software o hardware.

Diventano pertanto sanzionabili, in astratto, anche le condotte di mera detenzione di *malware*, coerentemente con l'impianto della Convenzione, che impone, all'art. 6, la punibilità anche "dell'approvvigionamento per l'uso".

All'estensione della portata della norma sotto il profilo oggettivo ha fatto riscontro la riformulazione dell'elemento soggettivo richiesto nei termini del dolo specifico.

Se, infatti, la precedente formulazione richiedeva pacificamente il solo dolo generico (ovvero la consapevolezza che il *malware* fosse in grado di danneggiare o alterare il funzionamento di un sistema informatico o telematico, e la consapevolezza della diffusione, comunicazione o consegna), con la riforma l'elemento soggettivo viene ad essere esteso anche al dolo specifico, in quanto il fatto è punibile laddove sia commesso "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".

Si ritiene che le condotte previste dal reato precedentemente presentato non siano neppure astrattamente realizzabili nell'ambito dell'azienda e pertanto tale reato presupposto non verrà successivamente analizzato.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 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*".

La norma ha struttura e contenuto pressoché identici a quelli di cui all'articolo 617 c.p., volendo il legislatore soltanto colmare il vuoto normativo con riferimento alle intercettazioni attraverso elaboratori elettronici.

L'interesse tutelato rimane, pertanto, quello della segretezza e inviolabilità delle comunicazioni. Il reato è di mera condotta - a forma vincolata – ed è comune. È previsto il dolo generico, essendo sufficiente la coscienza e la volontà del fatto tipico previsto dalla norma.

Si ritiene che le condotte previste dal reato precedentemente presentato non siano neppure astrattamente realizzabili nell'ambito dell'azienda e pertanto tale reato presupposto non verrà successivamente analizzato.

Installazione di apparecchiature atte a 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".

Similarmente all'articolo 617-quater, questo articolo estende la punibilità della condotta illecita prevista dall'articolo 617-bis alle comunicazioni effettuate tramite un sistema informatico o telematico.

L'elemento oggettivo consiste nell'installare ovvero nel mettere in opera strumenti tecnici atti ad intercettare (inserirsi in una comunicazione e riceverla all'insaputa del mittente e del destinatario), impedire o interrompere comunicazioni informatiche o telematiche.

È un reato comune, di pericolo e di mera condotta - a forma vincolata, perché la condotta è prestabilita dal legislatore. L'elemento soggettivo è il dolo specifico, perché oltre alla coscienza e alla volontà del fatto tipico, è necessario l'ulteriore scopo di intercettare, impedire o interrompere le comunicazioni.

Si ritiene che le condotte previste dal reato precedentemente presentato non siano neppure astrattamente realizzabili nell'ambito dell'azienda e pertanto tale reato presupposto non verrà successivamente analizzato

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".

La disposizione è stata novellata dalla legge 18 marzo 2008 n. 48, recante la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla crimionalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.

Il testo precedentemente in vigore, rubricato "Danneggiamento di sistemi informatici o telematici" così disponeva: "*Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici 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".

Con le modifiche apportate dalla L. 18 marzo 2008 n. 48, il legislatore ha, per un verso, introdotto una condizione di procedibilità (proposizione della querela da parte della persona offesa) nell'ipotesi semplice di reato (in passato si procedeva d'ufficio); per altro verso, ha precisato con maggior chiarezza le modalità della condotta di danneggiamento, includendovi anche la cancellazione, alterazione o soppressione di informazioni dati e programmi (attività che avrebbero comunque potuto essere ricomprese, in via interpretativa, tra le condotte penalmente sanzionate).

Il reato comune - potendo essere commesso da chiunque - di mera condotta in quanto si perfeziona nella semplice esecuzione dell'azione illecita e a forma libera. Si tratta, inoltre, di una fattispecie sussidiaria, perché sussiste qualora non sia configurabile un reato più grave. Anche nel testo modificato, il reato prevede il mero dolo generico, ovvero la previsione e la volontà del fatto tipico previsto dalla norma incriminatrice.

Si ritiene che le condotte previste dal reato precedentemente presentato non siano neppure astrattamente realizzabili nell'ambito dell'azienda e pertanto tale reato presupposto non verrà successivamente analizzato

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".

Il reato in esame punisce il danneggiamento di dati, informazioni e programmi "pubblici". Si ricorda che tali condotte erano sanzionate dall'art. 420 comma 2 c.p. (abrogato dalla stessa legge che introduce il nuovo reato), ove il delitto fosse delineato quale reato a consumazione anticipata, in termini di attentato a impianti di pubblica utilità (ed alle informazioni ivi contenute).

Il legislatore ha mantenuto tale caratteristica di consumazione anticipata, in termini di attentato, nonostante la Convenzione non lo richiedesse espressamente.

L'attuale norma prevede invece un reato comune, di mera condotta - a forma libera - dove l'eventuale evento si configura quale elemento aggravante. Vengono quindi puniti i fatti diretti a distruggere, deteriorare, cancellare, deteriorare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

In questo caso, si assiste ad un ampliamento evidente delle condotte punibili, in primo luogo sotto il profilo dell'oggetto materiale; il precedente testo normativo sanzionava, infatti, soltanto i danneggiamenti riguardanti i dati contenuti o pertinenti a "sistemi informatici o telematici di pubblica utilità", mentre, attualmente, è sufficiente che i dati siano "utilizzati dallo Stato o da altro ente pubblico".

Sono ricomprese pertanto le condotte riguardanti

1) dati, informazioni e programmi utilizzati dagli enti pubblici;
2) dati informazioni e programmi di pubblica utilità (e dunque sia pubblici che privati, purché siano destinati a soddisfare un interesse di natura pubblica).

Trattandosi di reato aggravato dall'evento, il fatto sussiste anche in assenza di qualunque effettivo deterioramento o soppressione dei dati, pur dovendosi necessariamente richiedere l'idoneità dell'azione a produrre tale effetto.

L'effettiva distruzione, cancellazione, alterazione o deterioramento è invece contemplata come circostanza aggravante (art. 635-ter comma 2 c.p.).

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda e solo per la seguente attività sensibile :

- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali ed inerenti l'attività contrattuale dell'Ente**

Dunque tale reato presupposto verrà successivamente analizzato.

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

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

Se ricorre la circostanza di cui al numero 1) 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 danneggiamento di sistemi informatici o telematici non di pubblica utilità ha mantenuto la caratteristica di reato di evento, e pertanto richiede espressamente che il sistema venga danneggiato, reso in tutto o in parte inservibile, ovvero ne venga ostacolato gravemente il funzionamento.

Sarà pertanto integrata la fattispecie di cui all'art. 635-quater, laddove il danneggiamento del sistema sia cagionato mediante

1) la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi; ovvero
2) l'introduzione o la trasmissione di dati, informazioni o programmi.

Le condotte punibili sono inoltre ampliate rispetto all'originaria dizione (il reato era previsto dall'art. 635-bis c.p.), in quanto è sufficiente la prova che la condotta abbia alterato (ancorché gravemente, nell'espressione ne ostacola gravemente il

funzionamento) il funzionamento del sistema, mentre fino alla recente riforma era necessaria la dimostrazione della distruzione, del deterioramento, ovvero del fatto che il sistema fosse reso, in tutto o in parte, inservibile.

La distinzione tra il danneggiamento di dati (ora punito dal nuovo art. 635-bis c.p.) e il danneggiamento del sistema è pertanto legata alle conseguenze che la condotta assume: laddove la soppressione o l'alterazione di dati informazioni e programmi renda inservibile, o quantomeno ostacoli gravemente il funzionamento del sistema, ricorrerà la più grave fattispecie del danneggiamento di sistemi informatici o telematici, prevista appunto dall'art. 635-quater c.p.

È un reato comune di mera condotta - a forma libera. Si tratta, peraltro di una fattispecie sussidiaria, perché sussiste qualora non sia configurabile un reato grave. È previsto il dolo generico, ovvero la previsione e la volontà del fatto tipico descritto dalla norma incriminatrice.

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda e solo per la seguente attività sensibile

- **Accesso a sistemi informatici e telematici privati es. banca**

Dunque tale reato presupposto verrà successivamente analizzato.

Danneggiamento di sistemi informatici e 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".

L'art. 635-quinquies c.p. corrisponde, anche sotto il profilo sanzionatorio, al "vecchio" reato, previsto dall'abrogato art. 420 c.p. commi 2 e 3 c.p., rubricato "Attentato a sistema informatico o telematico di pubblica utilità".

Rispetto a tale reato, per analogia con quello previsto dall'articolo precedente, si amplia la sfera delle condotte punibili, prevedendo che il fatto possa essere diretto non solo a danneggiare o a distruggere il sistema, ma anche a renderlo inservibile, ovvero ad ostacolarne gravemente il funzionamento.

Si tratta di un reato a consumazione anticipata, che non richiede l'avverarsi dell'evento di danneggiamento.

L'effettivo danneggiamento del sistema, la sua distruzione, o il fatto che venga reso in tutto o in parte inservibile è considerato un'ulteriore circostanza aggravante, che aumenta significativamente la sanzione (reclusione da tre a otto anni). D'altra parte non

è indicato tra le circostanze aggravanti il fatto che il funzionamento del sistema venga gravemente ostacolato.

Allo stesso modo non è più ricompresa nella fattispecie aggravata la circostanza che dal fatto derivi l'interruzione (anche parziale) del funzionamento, prevista dall'art. 420 comma 3 c.p. (ora appunto abrogato).

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

Non è sufficiente quindi, per la sussistenza del reato, che i sistemi siano utilizzati dagli enti pubblici, ma occorre che gli stessi siano di pubblica utilità.

L'articolo in questione estende ai documenti informatici, che abbiano efficacia probatoria, la punibilità prevista dai reati di cui al Capo III dei delitti contro la fede pubblica, ovvero ai delitti di falsità negli atti.

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda e solo per la seguente attività sensibile :

- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali ed inerenti l'attività contrattuale dell'Ente.**

Dunque tale reato presupposto verrà successivamente analizzato.

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

"*Il soggetto che presta servizi di certificazione di firma elettronica 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*".

L'aggiunta dell'articolo 640–quinquies è opportuna, stante la potenziale maggiore offensività della condotta compiuta dal certificatore ed il ruolo svolto. Il reato proprio dell'ente certificatore prevede una condotta che sembra rientrare, comunque, nella fattispecie di cui all'art. 640 c.p., con cui si porrebbe quindi in rapporto di specialità.

Si osserva infine che, a differenza del nuovo art. 495 bis c.p. (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri), in questo caso, la condotta punita riguarda solo il certificatore "qualificato" (o meglio, il soggetto che presta servizi di certificazione di firma elettronica qualificata). Per completezza, si segnala che l'articolo 495-bis c.p., inserito dalla stessa legge, non è contemplato tra i reati presupposto di cui al Decreto Legislativo 231/2001.

In termini sanzionatori, oltre alle sanzioni pecuniarie, l'art. 24-bis prevede la possibilità di comminare all'ente le sanzioni interdittive descritte dall'art. 9.

In particolare, si prevede che nell'ipotesi di condanna dell'ente a seguito della commissione del reato – di accesso abusivo a sistema informatico o telematico (615-ter c.p.), di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-quater c.p.), di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico(617-quinquies c.p.), di danneggiamento di informazioni, dati e programmi informatici (635-bis c.p.), di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-ter c.p.), di danneggiamento di sistemi informatici o telematici (635-quater c.p.) e di sistemi informatici o telematici di pubblica utilità (635-quinquies c.p.) - saranno applicabili le sanzioni dell'interdizione dall'esercizio dell'attività, della sospensione o della revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e, infine, del divieto di pubblicizzare beni o servizi.

Si applicheranno, invece, le sanzioni interdittive della sospensione o della revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e il divieto di pubblicizzare beni o servizi in caso di commissione del reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-quater c.p.) e di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (615-quinquies c.p.).

Infine per i reati previsti dal terzo comma dell'art. 24-bis, e quindi di falsità in documenti informatici (491-bis c.p.) e di frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640-quinquies c.p.) si applicheranno le sanzioni interdittive del divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un servizio pubblico); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi ed, ancora,il divieto di pubblicizzare beni o servizi.

Si ritiene che le condotte previste dal reato precedentemente presentato non siano realizzabili nell'ambito dell'azienda, ma si è comunque prestata attenzione alla:

- **gestione delle firme elettroniche**

3. Le "attività sensibili" ai fini del d.lgs n. 231/2001

L'art. 6, comma 2, lett. a) del d.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal d.lgs. n. 231/2001.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui al precedente punto 1, le attività "sensibili" di SAL S.r.l., di seguito elencate:

1) **Gestione dei sistemi informativi e della sicurezza informatica**: riguarda le attività di gestione dei profili utente e del processo di autenticazione, creazione, trattamento, archiviazione di documenti elettronici con valore probatorio, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno, gestione e protezione delle reti e degli output di sistema e dei dispositivi di memorizzazione, nonché della sicurezza fisica (cablaggi, dispositivi di rete, ecc.).
2) **Accesso a sistemi informatici e telematici privati es. banca**
3) **Utilizzo e detenzione di ID e/o le password di accesso a portali internet o ad applicativi interni per i quali è necessario avere delle specifiche credenziali.**
4) **gestione delle firme elettroniche**

4. Destinatari della Parte Speciale

Sono destinatari (di seguito i "Destinatari") della presente Parte Speciale del modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/01 di S.A.L. (di seguito l'"Azienda") e si impegnano al rispetto del contenuto dello stesso:

- l'amministratore e i dirigenti dell'azienda (cosiddetti soggetti apicali);
- i dipendenti dell'azienda (cosiddetti soggetti interni sottoposti ad altrui direzione).
- In forza di specifica accettazione o in forza di apposite clausole contrattuali possono essere destinatari di specifici obblighi per il rispetto del contenuto del Codice di Condotta i seguenti soggetti esterni (di seguito i "Soggetti Esterni"):
- i collaboratori, i consulenti e in generale i soggetti che svolgono attività di lavoro autonomo;
- i fornitori, clienti di S.A.L.

5. Il sistema dei controlli

Il sistema dei controlli, perfezionato dalla Società sulla base delle indicazioni fornite dalle principali associazioni di categoria, quali le Linee Guida Confindustria, nonché dalle "best practice" internazionali, prevede con riferimento alle attività sensibili e ai processi strumentali individuati:

- Principi generali degli standard di controllo relativi alle attività sensibili;
- Standard di controllo "specifici" applicati alle singole attività sensibili.

5.1 Principi generali degli standard di controllo relativi alle attività sensibili

Gli standard di controllo specifici sono fondati sui seguenti principi generali:

- **Procedure**: gli standard si fondano sull'esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: gli standard si fondano sul principio secondo cui: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.
- **Segregazione dei compiti**: gli standard si fondano sulla separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Procure e deleghe**: gli standard si fondano sul principio secondo il quale i poteri autorizzativi e di firma assegnati debbano essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese.

5.2 Standard di controllo specifici

Qui di seguito sono elencati gli standard di controllo specifici relativi alle singole attività sensibili individuate:

1) Gestione dei sistemi informativi e della sicurezza informatica

- *Procedure:* l'attività sensibile è regolata dalla procedura "Gestione dei sistemi informativi e della sicurezza informatica" che prevede la descrizione di ruoli, responsabilità, modalità operative e controlli con riferimento alle seguenti aree:
  - Sicurezza del sistema informativo;
  - Organizzazione della sicurezza per gli utenti interni ed esterni;
  - Classificazione e controllo degli asset aziendali ivi inclusi dati ed informazioni;
  - Sicurezza fisica e ambientale (locali e beni in essi contenuti);
  - Gestione delle comunicazioni e dell'operatività;
  - Controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni;
  - Gestione degli incidenti e dei problemi di sicurezza informatica;
  - Attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica;
  - Controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche;

- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi;
- Valutazione e formazione degli amministratori di sistema.

Per i controlli aggiuntivi associati all'attività sensibile in oggetto, si rimanda a quanto previsto all'interno della "Parte Speciale F – Delitti in violazione del diritto d'autore".

6. I flussi informativi in favore dell'Organismo di Vigilanza

Al fine di fornire all'Organismo di Vigilanza gli strumenti per esercitare le sue attività di monitoraggio e di verifica dell'efficace esecuzione delle procedure, dei regolamenti e dei controlli previsti dal Modello e, in particolare, dalla presente Parte Speciale è necessario che tutta la documentazione prodotta nell'ambito delle attività disciplinate nella presente Parte Speciale sia conservata da ciascun Destinatario coinvolto nel processo per le attività di propria competenza e messa a disposizione, su richiesta dell'Organismo di Vigilanza.

I Destinatari interni, sulla base delle verifiche effettuate, provvedono a inviare all'Organismo di Vigilanza, i documenti da lui richiesti in apposito documento riassuntivo dei flussi.

I Destinatari interni sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.

L'Organismo di Vigilanza richiede ai Destinatari del Modello di comunicare il rispetto dei principi e dei protocolli di controllo sanciti nella presente Parte Speciale nello svolgimento dei compiti loro assegnati.

Lo strumento di comunicazione è rappresentato da un messaggio di posta elettronica corredato dal flusso informativo cui si riferisce la comunicazione da inviarsi, a cura dell'interessato, all'indirizzo di posta elettronica appositamente creato per tale fine.