



**Modello di Organizzazione, Gestione e Controllo ai
sensi del Decreto Legislativo 231/01
Parte Speciale B - Reati Informatici e trattamento illecito
dei dati**

Rev. 04 del 17.04.2025

**approvato dal Presidente (Legale rappresentante e Amministratore Unico) con
Atto n°44 del 17.04.2025**

	Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01 Parte Speciale B - Reati Informatici e trattamento illecito dei dati	Rev. 04 del 17.04 2025
---	--	-----------------------------------

Sommario

1. Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01 – Parte Speciale B – Reati Informatici e trattamento illecito dei dati.....	3
2. Le tipologie dei reati informatici (art. 24-bis del Decreto).....	3
2.1 Reati informatici.....	4
2.2 Reati commessi attraverso l'uso di un sistema informatico	11
2.3 Cyberterrorismo.....	12
3. Le attività sensibili ex art. 24-bis del Decreto	13
4. Destinatari della Parte Speciale	13
5. Principi generali di comportamento e i protocolli di controllo	13
6. I flussi informativi in favore dell'Organismo di Vigilanza.....	14

1. Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01 – Parte Speciale B – Reati Informatici e trattamento illecito dei dati

L'art. 7 della Legge 18 marzo 2008, n. 48 ha introdotto nel D.Lgs. 231/01, l'articolo 24-bis in materia di delitti informatici e trattamento illecito dei dati, ampliando così le fattispecie che possono generare la responsabilità dell'Ente.

L'articolo citato dispone che:

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 duecento a settecento quote.

1-bis. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e ((635-quater.1)) del codice penale, si applica all'ente la sanzione pecuniaria ((sino a quattrocento 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, 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.

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 il delitto indicato nel comma 1-bis si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni)).

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 comunicazioni;
- 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**.

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.

	Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01 Parte Speciale B - Reati Informatici e trattamento illecito dei dati	Rev. 04 del 17.04 2025
---	--	-----------------------------------

2.1 Reati informatici

ALER Pavia Lodi gestisce buona parte dei servizi di SAP attraverso procedure informatiche e l'utilizzo del sistema informativo. I reati inclusi nella presente famiglia sono trasversali a tutti i processi e le attività dell'Ente. Al fine del concretizzarsi della responsabilità amministrativa è necessario che si configuri un interesse o un vantaggio per l'Ente, aspetto che riduce notevolmente la probabilità di applicazione nella fattispecie di ALER.

Art. 615-ter. 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 due a dieci anni (1):

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 minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato (2);

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 ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati, delle informazioni o dei programmi in esso contenuti (3).

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 tre a dieci anni e da quattro a dodici anni (4).

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.

Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi, per prendere cognizione di dati riservati altrui nell'ambito per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse dell'ente stesso.

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 all'attività contrattuale dell'Ente (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel etc.).**
- **Accesso a sistemi informatici e telematici privati (es. banca)**

Dunque, tale reato presupposto verrà successivamente analizzato.

Art. 615-quater. Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici.

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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 a due anni e con la multa sino a euro 5.164 (3).

La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1) (4).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma (5)

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:

- **Gestione sistemi informatici interni (anche gestione internet da parte del personale interno)**

Dunque, tale reato presupposto verrà successivamente analizzato.

Art. 617-quater. 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 un anno e sei mesi a cinque anni. (2)

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 quattro a dieci anni se il fatto è commesso (3):

- 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma (4);
2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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 (5);
[3) da chi esercita anche abusivamente la professione di investigatore privato (6).]".

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 ed a vantaggio dell'Ente e pertanto tale reato presupposto non verrà successivamente analizzato.

Art. 617-quinquies.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche. (1) (2)

Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti 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. (3)

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni (4).

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni (5).".

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.

Il reato si integra, ad esempio, a vantaggio della Società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti a vantaggio dell'Ente.

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

Art. 635-bis. 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 due a sei anni (3).

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato. (2)".

La disposizione è stata novellata dalla legge 18 marzo 2008 n. 48, recante la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità 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.

Tale reato potrebbe ad esempio essere commesso nell'interesse della Società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (ad es. polizia giudiziaria) relativi ad un procedimento penale a carico della Società.

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda ed a vantaggio per l'ente 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 (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, SIMOG e Osservatorio regionale per la codificazione dei contratti, etc.).**

Art. 635-ter.

Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico

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 di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni (3).

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;*

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici (4).

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)

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 ed a vantaggio dell'ente e solo per la seguente attività sensibile:

- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali ed inerenti all'attività contrattuale dell'Ente (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel etc.).**

Dunque, tale reato presupposto verrà successivamente analizzato.

Art. 635-quater. 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 due a sei anni (3).

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato. (2)*

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. 635bis 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.

Art. 635-quater.1.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (1)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.

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

- **Gestione sistemi informatici interni**
- **Accesso a sistemi informatici e telematici esterni privati**
- **Utilizzo di firma digitale**
- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali e connessi all'attività svolta da Aler (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel, Sintel etc.)**

Dunque, tale reato presupposto verrà successivamente analizzato.

Art. 635-quinquies.

Danneggiamento di sistemi informatici o telematici di pubblico interesse (1)

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, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni. La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;*
- 3) 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 quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).

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 ed a vantaggio per l'ente e solo per la seguente attività sensibile:

- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali e connessi all'attività svolta da Aler (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel Sintel etc.)**

Dunque, tale reato presupposto verrà successivamente analizzato.

Art. 629 Estorsione.

3 Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa,

procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità (8).

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

- **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali e connessi all'attività svolta da Aler (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel, Sintel etc.)**

Dunque, tale reato presupposto verrà successivamente analizzato.

2.2 Reati commessi attraverso l'uso di un sistema informatico

Art. 491-bis. Documenti informatici

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.

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.

Il reato può essere compiuto da un qualunque soggetto che accede alla rete aziendale o ad una postazione informatica collegata alla rete esterna al fine di danneggiare informazioni, dati e programmi informatici, sistemi informativi altrui (Es. Catasto, Agenzia delle Entrate, INPS etc.).

Dato però che sono, al di fuori dell'ambito di operatività della responsabilità ex D.Lgs. n. 231/2001 si ritiene poco probabile, ma non impossibile il rischio di commissione di tali fattispecie di reato.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 e connessi all'attività svolta da Aler (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel, Sintel etc.)**
- **Accesso a sistemi informatici e telematici privati (es. banca)**
- **Gestione informazioni e dati ai sensi del GDPR Privacy**

Dunque, tale reato presupposto verrà successivamente analizzato.

Art. 640-quinquies. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

"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 (491bis c.p.) e di frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640quinquies 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**

2.3 Cyberterrorismo

Legge 18 novembre 2019 n 133 "Legge sulla sicurezza cibernetica" introduce la responsabilità amministrativa specificando che "Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote".

Si ritiene che le condotte previste dal reato precedentemente presentato siano difficilmente realizzabili nell'ambito dell'azienda

In base alla direttiva NIS 2 (Direttiva UE 2022/2555), recepita in Italia tramite il decreto legislativo n. 138/2024 del 16 ottobre 2024, sono stati introdotti obblighi specifici per le imprese che operano in settori critici. Questi obblighi mirano a rafforzare la sicurezza informatica e a migliorare la gestione dei rischi.

	Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01 Parte Speciale B - Reati Informatici e trattamento illecito dei dati	Rev. 04 del 17.04 2025
---	--	-----------------------------------

Approfondimenti specifici hanno confermato che Aler non rientra tra gli enti obbligati a registrarsi presso l'Agenzia per la Cybersicurezza Nazionale (ACN).

3. Le attività sensibili ex art. 24-bis del Decreto

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale "B" del Modello, le seguenti:

1. **Accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali e connessi all'attività svolta da Aler (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale, Entratel, Siatel, Sintel etc.).**
2. **Accesso a sistemi informatici e telematici privati (es. banca**
3. **Gestione sistemi informatici interni (anche gestione internet da parte del personale interno)**
4. **Utilizzo firme elettroniche**
5. **Gestione informazioni e dati ai sensi del GDPR Privacy**

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 Aler Pavia Lodi (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 ed altri stakeholders di Aler Pavia Lodi.

5. Principi generali di comportamento e i protocolli di controllo

I Destinatari della presente Parte Speciale del Modello, oltre a rispettare le previsioni di legge esistenti in materia, le norme comportamentali e i principi generali di comportamento richiamati nel Codice etico devono rispettare i protocolli di controllo di cui sono responsabili previsti nel presente paragrafo e nell'ulteriore documentazione adottata in attuazione dei principi di riferimento previsti nella presente Parte Speciale.

1. **Con riferimento all'accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali e connessi all'attività svolta da Aler (es. Regione Lombardia SIRAPER per invio dati patrimonio edilizio, Sportello unico previdenziale etc.).**
2. **Con riferimento all'accesso a sistemi informatici e telematici privati (es. banca)**
3. **Con riferimento alla gestione sistemi informatici interni (anche gestione internet da parte del personale interno)**

In questo ambito, all'interno di Aler Pavia Lodi per la tenuta sotto controllo sia dell'hardware sia dei software installati è presente uno specifico "Elenco hardware ed elenco software in uso" monitorato dalla funzione sistemi informativi.

Per quanto riguarda gli accessi ai Database esterni sia pubblici sia privati e per la loro gestione è stato predisposto un "Elenco accesso Banche dati esterne" con l'identificazione dell'Ente a cui si riferisce la banca dati, della Banca dati esterna, della Descrizione del servizio, degli operatori che accedono e dell'Amministratore delle Utenze.

In merito alla gestione della privacy e presente un Data protection Officer e la documentazione relativa alla Privacy e al rispetto della normativa cogente così composta:

Registro delle attività di trattamento -- Organigramma privacy -- Autorizzazioni al trattamento dati -- Elenco responsabili del trattamento -- Nomine a responsabili del trattamento dati -- Elenco titolari del trattamento (per i quali Aler agisce da Responsabile) -- Informativa Utenti -- Informativa Acquirenti Asta -- Informativa Videosorveglianza -- Informativa Sito Internet -- Censimento Asset -- Atto di designazione DPO -- Data Breach Policy.

4. Con riferimento alla gestione delle firme elettroniche

Aler Pavia Lodi controlla che le smart card o business key per la firma digitale impiegata ai fini aziendali, siano utilizzate dalle sole persone proprietarie.

5. Con riferimento alla gestione informazioni e dati ai sensi del GDPR Privacy

Aler Pavia Lodi ha predisposto adeguata documentazione, recante specifiche procedure per la sicurezza delle informazioni e la tutela dei dati, e contenente le modalità di gestione delle risorse informatiche dell'Azienda, ai sensi del GDPR 2016/679.

È stato inoltre designato il Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679 (GDPR)

È prevista anche la distribuzione in forma controllata dei beni informatici aziendali per i quali è mantenuta la rintracciabilità in appositi moduli.

La documentazione relativa alla Privacy e al rispetto della normativa cogente così composta:

Registro delle attività di trattamento -- Organigramma privacy -- Autorizzazioni al trattamento dati -- Elenco responsabili del trattamento -- Nomine a responsabili del trattamento dati -- Elenco titolari del trattamento (per i quali Aler agisce da Responsabile) -- Informativa Utenti -- Informativa Acquirenti Asta -- Informativa Videosorveglianza -- Informativa Sito Internet -- Censimento Asset -- Atto di designazione DPO -- Data Breach Policy.

Riassumendo, ALER Pavia Lodi ha già adottato i seguenti controlli e misure di prevenzione per la gestione delle attività connesse alla presente area di reato al fine di ridurre i rischi di commissione dei reati presupposto:

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.

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.

	Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01 Parte Speciale B - Reati Informatici e trattamento illecito dei dati	Rev. 04 del 17.04 2025
---	--	-----------------------------------