PARTE SPECIALE "I"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

ART 24 *BIS* D.LGS. N. 231/01

ART 24 *BIS* D.LGS 213/01 - REATI PRESUPPOSTO		
CODICE PENALE	**ART 491 BIS**	**Falsità riguardanti un documento informatico**
	ART 615 TER	**Accesso abusivo ad un sistema informatico o telematico**
	ART 615 QUATER	**Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici**
	ART 615 QUINQUIES	**Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi e programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**
	ART 617 QUATER	**Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**
	ART 617 QUINQUIES	**Detenzione, diffusione e Installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedireo interrompere comunicazioni informatiche o telematiche**
	ART 635 BIS	**Danneggiamento di informazioni, dati e programmi informatici**
	ART 635 TER	**Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**
	ART 635 QUATER	**Danneggiamento di sistemi informatici o telematici**
	ART 635 QUINQUIES	**Danneggiamento di sistemi informatici o telematici di pubblica utilità**
	ART 640 QUINQUIES	**Frode informatica del soggetto che presta servizi di certificazione di firma elettronica**

QUADRO NORMATIVO

L'art 24 *bis* del D.lgs. 231/01, introdotto dall'articolo 7 della legge 18 marzo 2008, n. 48, dispone che, in relazione alla commissione dei delitti di cui agli articoli 615 ter, 617 *quater*, 617 *quinquies*, 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies* del codice penale, si applica all'ente la sanzione pecuniaria da 100 a 500 quote.

In relazione alla commissione dei delitti di cui agli articoli 615 *quater* e 615 *quinquies* del codice penale, si applica all'ente la sanzione pecuniaria sino a 300 quote.

In relazione alla commissione dei delitti di cui agli articoli 491 bis e 640 *quinquies* del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a 400 quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e).

Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

I.1. LE FATTISPECIE RILEVANTI

Prima di descrivere le singole fattispecie di reato previste dall'art 24 bis del Decreto, si precisano alcuni concetti richiamati dalle norme in questione:

Per "*sistema informatico*", secondo la ricorrente espressione utilizzata nella L. n. 547/ 1993, si intende un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche che, per mezzo di impulsi elettronici, su supporti adeguati, consentono la trasmissione, registrazione e l'elaborazione automatica dei "dati" (rappresentazioni elementari di un fatto effettuata attraverso simboli – *bit*), in modo da generare "informazioni".

Per "*sistema telematico*" si intende, un insieme combinato di apparecchiature idoneo alla trasmissione a distanza di dati e di informazioni, attraverso l'impiego di tecnologie dedicate alle telecomunicazioni. La definizione di telematica deriva dalla contrazione semantica tra i termini "telecomunicazioni" e "informatica" per indicare la trasmissione a distanza e la circolazione dei dati con i nuovi sistemi di diffusione delle informazioni o con i moderni dispositivi mobili come smartphone e tablet. Nell'ambito dei meccanismi di elaborazione delle informazioni rientrano i sistemi denominati client-server, che indicano una architettura di rete nella quale genericamente un computer client o terminale si connette ad un server per la fruizione di un certo servizio, quale ad esempio la condivisione di una certa risorsa hardware o software, ovvero per consultare, immettere o modificare informazioni rese disponibili ad altri client, appoggiandosi alla sottostante architettura protocollare.

Per "*misure di sicurezza*" si intendono i meccanismi logici, tecnologici ed organizzativi che tendono ad impedire la commissione di reati informatici e a prevenire altri eventi dannosi per la macchina o per i dati (più che mezzi di protezione del luogo ove è collocato il computer, si tratta di strumenti protettivi aventi ad oggetto direttamente ed esclusivamente il sistema informatico).

EVOLUZIONE NORMATIVA

Nel corso dell'anno 2021, la legge n. 238 del 23 dicembre 2021 (c.d. Legge Europea) – entrata in vigore in data 1° febbraio 2022 – recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea, ha apportato – tra le altre – alcune modifiche al c.d. Catalogo dei Reati 231 e, in particolare, sono stati modificati alcuni delitti informatici e trattamento illecito di dati richiamati dall' **24-bis D.Lgs. 231/2001** come segue:

- È stata ampliata la descrizione delle condotte dei reati di: i) detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.); ii) detenzione, diffusione e installazione abusiva diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615 quinquies c.p.) e di iii) detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.) e conseguente modifica della rubrica delle norme;
- Aumentata la pena per il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)

La riforma è, dunque, andata ad ampliare la portata applicativa delle norme penali inserendo

- **DOCUMENTI INFORMATICI (ART. 491 *BIS* C.P.):**

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

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (Art. 1, co. 1, lett. p), D.Lgs.n.82/2005, salvo modifiche ed integrazioni)

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato

- **ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615 *TER* C.P.):**

"…Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) Se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

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

Con tale norma si intende punire colui che viola la riservatezza delle comunicazioni e informazioni trasmesse attraverso sistemi informatici e/o telematici.

Le modalità di commissione del reato in questione possono essere le seguenti:

- Ingresso virtuale nel sistema informatico o telematico, anche attraverso appropriazione di credenziali di autenticazione o simulazione di titolarità;
- Inserimento di programmi "civetta" atti a riprodurre, captare, intercettare dati, codici, contenuti in sistemi informatici o telematici;
- Ingresso materiale nei locali in cui si trova l'elaboratore con la consapevolezza dell'abusività di tale condotta, indipendentemente dalle modalità di accesso e dall'effettiva lesione al sistema.

Elemento soggettivo: il dolo richiesto è generico e consiste nella coscienza e volontà di entrare in un sistema informatico/telematico protetto ovvero di permanervi contro la volontà di chi può escluderlo, con la consapevolezza dell'abusività di tale condotta.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura)

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela

- **DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, CODICI E ALTRI MEZZI ATTI ALL'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, 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 oistruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a 5.164 euro.

La pena è della reclusione da uno a tre anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna

delle circostanze di cui al quarto comma dell'articolo 617 quater".

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'Art. 615-quater, pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (ad esempio, badge, carte di credito, bancomat e smart card)

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet)

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Possesso, distrazione, divulgazione di credenziali di autenticazione – c.d. password - (riservate, nominative, numeriche o di altro tipo), indipendentemente dalle modalità, la cui disponibilità è riservata solo agli utenti del sistema informatico/telematico.
- Agevolazione dell'altrui accesso, mediante indicazioni e istruzioni idonee a raggiungere tale scopo;
- Utilizzo di password di accesso a siti di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate.
- il dipendente di un'azienda autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'azienda oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso

Elemento soggettivo: il dolo è specifico, dovendo essere la condotta diretta a procurare un profitto a sé o ad altri ovvero arrecare un danno.

La legge n.238 del 23 dicembre 2021 ha modificato/integrato le condotte e la durata della reclusione relativa al primo comma

- **DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA 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, 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, èpunito con la reclusione fino a due anni e con la multa sino a euro 10.329…***".

La fattispecie ha l'intento di reprimere la diffusione dei c.d. "virus" informatici (programmi che si attivano da soli in un dato momento temporale o al verificarsi di una certa condizione e che sono forieri di gravi danni ai sistemi informatici/telematici, utilizzati spesso per scopi di sabotaggio).

Questi fatti sono punibili solo nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento. Ciò si verifica, ad esempio, qualora un dipendente introduca un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico di un concorrente

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Fabbricazione, vendita, distribuzione, importazione finalizzata allo smercio, cessione a qualsiasi titolo di apparecchiature o programmi informatici - "virus" – indipendentemente dall'effettiva lesione o concreta idoneità a costituire un danno;

- Fabbricazione, utilizzo o acquisizione di malware, dongle, stimme, laddove tali strumenti siano preordinati ad un utilizzo illegale finalizzato al danneggiamento o alterazioni di sistemi informatici ovvero di dati/programmi in essi racchiusi;

Elemento soggettivo: è richiesto il dolo specifico, cioè la coscienza e volontà della condotta finalizzata al danneggiamento informatico.

La legge n.238 del 23 dicembre 2021 ha modificato/integrato le condotte punite dalla norma.

- **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 cinque 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 tre a otto 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…".

Le condotte, per essere penalmente rilevanti, devono essere compiute "fraudolentemente"; non risponde perciò del reato chi, per esempio, a causa di un guasto di linea, prenda cognizione di comunicazioni telematiche altrui.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

Venire a conoscenza, direttamente o indirettamente, in tempo reale o in un momento successivo, mediante l'ausilio di strumentazioni idonee allo scopo, di qualsiasi dato o informazione trasmesso con modalità informatica, da considerarsi riservato. Divulgazione con qualsiasi mezzo di dati o informazioni trasmesse mediante strumento informatico, senza autorizzazione dell'autore o del destinatario dei medesimi.

La legge n.238 del 23 dicembre 2021 ha modificato la pena in aumento sia nel primo che nel quarto comma

- **DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE E DI ALTRI MEZZI ATTI AD INTERCETTARE, IMPEDIRE OD INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617 *QUINQUES* C.P.):**

"…***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 a 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 c.p. …".***

La condotta vietata dall'Art. 617-quinquies è, pertanto, costituita non solo dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, ma anche se le si detiene solamente o vengono diffuse. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata abbia, obiettivamente, una potenzialità lesiva

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Posa in opera di strumenti tecnici o installazione di software informatici atti a captare, memorizzare e riprodurre dati e informazioni trasmesse da un sistema informatico.
- Qualunque atto preparatorio all'intercettazione o interruzione di comunicazioni informatiche/telematiche.

  Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche

La legge n.238 del 23 dicembre 2021 ha modificato la rubrica dell'articolo e notevolmente ampliato la portata della norma sia inserendo nuove condotte punibili sia introducendo in maniera chiara la finalità cui le condotte devono essere destinate e cioè intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle

- **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 il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Distruzione, deterioramento o riduzione apprezzabile della funzionalità o qualità di sistemi informatici o telematici di terzi ovvero cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore

- **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 il fatto è commesso con violenza alla persona o con minacciaovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata …".

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Lesione, cancellazione volontaria, danneggiamento o procurata inservibilità di programmi software, applicativi, banche dati o comunque informazioni di proprietà o in uso allo Stato o ad Ente pubblico o di pubblica utilità;

- Deterioramento, soppressione, alterazioni di dati, informazioni e contenuti di proprietà o in uso allo Stato o ad ente pubblico o di pubblica utilità.

Questo delitto si distingue da quello di cui all'art. 635 bis c.p. poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato

- **DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635 *QUATER* C.P.):**

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

***Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata…*".** Articolo introdotto dall'art 5 L. 18 marzo 2008, n. 48.

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Chiunque, mediante l'introduzione o la trasmissione di dati, danneggi - in parte o in maniera irreversibile - il sistema informatico/telematico altrui;

- Chiunque, mediante l'introduzione o la trasmissione di dati, ostacola gravemente il funzionamento del sistema informatico/telematico altrui.

- Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus)

- **DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635 *QUINQUIES* C.P.):**

**"*… Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*

***Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata …*".**

Articolo introdotto dall'art 5 L. 18 marzo 2008, n. 48.

Per sistema informatico di pubblica utilità, si allude, ad esempio, alla banca dati online (archivio informatizzati) della Polizia, gestito dall'apposito sistema informativo "Interforze" del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, che permette di consultare in tempo reale l'archivio contenente dati sui veicoli rubati, documenti di identità falsi o smarriti, etc.:

ESEMPI DI POSSIBILI COMPORTAMENTI ILLECITI

- Chiunque danneggi un sistema informatico o telematico di pubblica utilità;
- Intromissione all'interno di un sistema informativo alterandone il funzionamento per renderlo inservibile per gli scopi per cui è stato costruito.
- Il reato si può configurare nel caso in cui un dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

- **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, il 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…*".

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata

I.2. PRINCIPALI AREE A RISCHIO DI COMMISSIONE DEI DELITTI INFORMATICI

Il rischio di potenziale commissione dei reati in oggetto è, per la natura stessa di tali fattispecie delittuose, presente in tutte le attività svolte dai dipendenti o collaboratori aziendali che prevedano l'utilizzo di strumenti informatici, sistemi e applicativi informatici della società.

In generale, le attività sensibili, attinenti con i reati in materia di trattamento illecito di dati previsti dall'art 24 bis del Decreto, sono tutte le attività/aree dove si fa uso di sistemi/strumenti informatici e telematici.

I.3. DESCRIZIONE DEI PROCESSI A RISCHIO ("PROCESSI SENSIBILI")

Di seguito si riporta il processo che, a seguito dell'analisi dei rischi, è risultato sensibile in relazione al rischio di commissione dei reati informatici, di cui all'art 24 *bis* del D.lgs. n. 231/01:

PRO.7: SISTEMI E CONNESSIONI

I.4. PRINCIPI GENERALI DI COMPORTAMENTO

Per prevenire la commissione di tali reati-presupposto di cui all'art 24 bis si rinvia ai principi contenuti nel Codice Etico approvato dalla società nonché alle regole di condotta contenute nelle procedure aziendali e nei protocolli di controllo costituenti il MOG.

- Tutti i responsabili del processo (ivi inclusi i terzi collaboratori) **devono:**

- Operare nel rispetto della normativa vigente, delle regole stabilite nel Modello 231 e nella presente Parte Speciale, del Codice Etico, delle procedure interne aziendali, mantenendosi aggiornati sull'evoluzione normativa;
- Rispettare la normativa sulla privacy (D.lgs. n. 196/2003; Reg. UE 2016/679; D.lgs.101/2018);
- Garantire, in particolare, che tutti i dipendenti e collaboratori osservino rispettino le seguenti misure:

- Per quanto attiene i "Trattamenti con strumenti elettronici" dovrà essere garantito un sistema di autenticazione informatica: il trattamento di dati personali con strumenti elettronici è consentito solo a soggetti specificatamente incaricati dalla Società, dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

- Adottare idonee misure di sicurezza per garantire la sicurezza fisica e tecnologica dei pc, dei sistemi informatici/telematici e dei software (es: sistemi di rilevazione di incendi/gas; installazione periodica di antivirus, firewall, etc.);
- Far sottoscrivere ai consulenti e alle società esterne che prestano servizi informatici per la Società specifiche "*Clausole 231*", che li vincolino al rispetto del MOG e del Codice Etico adottato dalla Società (si evidenzia, infatti, che il server aziendale, di proprietà della società, è gestito in outsourcing).

- Nell'ambito dei reati informatici, a titolo esemplificativo non esaustivo, è **fatto divieto di:**

- Accedere a sistemi informativi utilizzati dalla Pubblica Amministrazione o di alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questi pertinenti per ottenere e/o modificare indebitamente informazioni a vantaggio dell'azienda o di terzi, o comunque al fine di trarne vantaggio per l'azienda o per terzi; • Falsificare documenti informatici;
- Accedere abusivamente ad un sistema informatico o telematico;
- Detenere o diffondere abusivamente i codici di accesso a sistemi informatici e telematici;
- Diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere il funzionamento di un sistema informatico o telematico;
- Intercettare, impedire o interrompere illecitamente le comunicazioni informatiche o telematiche;
- Danneggiare informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- Danneggiare sistemi informatici o telematici (anche di pubblica utilità).

I.5. PRESIDI SPECIFICI PER MITIGARE IL RISCHIO DI COMMISSIONE DEI DELITTI INFORMATICI

Dovranno essere rispettati i protocolli e le procedure aziendali finalizzate a regolamentare e controllare lo svolgimento delle attività sensibili in oggetto.

In particolare, di seguito sono state definite specifiche modalità operative al fine di prevenire eventuali comportamenti in grado di condurre a ipotesi di reato rilevanti ai sensi dell'art 24 bis del D.lgs. n. 231/01

L'iter procedurale da rispettare è scandito da diverse attività, come di seguito descritte.

A. Creazione, modifica e cancellazione di account e profili (credenziali di autenticazione)

- Connessione degli utenti alla rete tramite codice di autenticazione univoco e personale;
- Assegnazione della password al momento del conferimento del potere di accesso con obbligo di sostituirla al primo accesso;

- Obbligo per i dipendenti, qualora prendano coscienza che taluno possa aver visionato la digitazione o essere comunque a conoscenza della password, di cambiarla immediatamente;
- Divieto di annotazione della password in chiaro e/o su supporto cartaceo o informatico;
- Obbligo di rifiuto di comunicazione orale della password;
- Indicazione dei requisiti minimi di complessità della password: a titolo esemplificativo, non esaustivo, richiedere la redazione della password con caratteri maiuscoli/minuscoli; divieto di inserimento di simboli, numeri, punteggiatura o lettere, etc.
- Previsione della lunghezza della password in almeno 8 caratteri;
- Prevedere un obbligo di modifica della password almeno ogni due mesi;
- Divieto di utilizzare password che facciano riferimento alla persona che le utilizza, evitando riferimenti a persone e date connesse alla propria vita privata e lavorativa.
- Non utilizzare nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o "remember password" presenti nei browser o in altre applicazioni.

B. Gestione rete internet

- Tutti gli utenti della rete devono avere l'account sul dominio di lavoro della società. L'account deve essere un identificativo composto da cognome.inizialenome@CNGTRADE dell'addetto destinatario.

- E' vietato ai dipendenti l'accesso e la navigazione in siti non inerenti l'attività aziendale, poiché il collegamento ad internet è esclusivamente finalizzato all'esercizio dell'attività stessa, con ogni più ampio divieto di utilizzo per fini personali. In particolare, è fatto assoluto divieto di navigare in siti riferibili, o che utilizzano argomenti illegali quali, ad esempio: armi, gioco d'azzardo, criminalità, droga, malware, pornografia/pedopornografia, etc.

- Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili, salvo nei casi espressamente autorizzati dalla società.

- Sono interdette le partecipazioni, per motivi non professionali, a mailing list, forum, community così come l'utilizzo di chat line, di bacheche elettroniche, anche utilizzando psuedonimi (nickname) mediante il pc aziendale.

Si ricorda che l'azienda esercita attività di controllo generale per evitare navigazioni in siti pericolosi per l'integrità dei suoi sistemi e può in qualunque momento, anche senza preavviso, attivare meccanismi di monitoraggio per fini organizzativi, funzionali e di controllo della sicurezza informatica dell'impianto aziendale.

C. Gestione della posta elettronica

A tutti gli utenti viene assegnata una casella di posta elettronica al momento dell'ingresso in azienda. Il nome della casella deve essere formato utilizzando la seguente regola: cognome.nome@xxx.it, ad eccezione delle caselle email dedicate ai servizi che devono assumere la seguente forma: nomeservizio@xxx.it.

- Deve essere consigliato che tutti gli allegati che superano i 500K siano preventivamente compressi mediante strumento apposito. E' vietato utilizzare le caselle di posta elettronica per uso personale e/o non inerente l'attività aziendale. Conseguentemente, al fine di non ledere il diritto il diritto alla riservatezza e segretezza della posta utilizzata per scopi personali, i dipendenti non dovranno utilizzare la caselle di posta elettronica per fini che esulano dal contesto aziendale. In caso di assenza per qualsiasi motivo dell'utilizzatore (malattia,ferie, allontanamento temporaneo dal posto di lavoro), qualora si renda necessario, il Responsabile del trattamento dei dati od un suo delegato deve poter accedere alla posta elettronica dell'utente per noninterrompere né rallentare il processo produttivo aziendale o, semplicemente, per prendere visione dello storico delle comunicazioni di interesse aziendale.

- E' fatto divieto di divulgare le notizie e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti tutti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza previsti a carico di tutti i dipendenti.

D. Gestione di reti interne, implementazione e manutenzione.

La rete interna può essere istituita per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa e non può essere utilizzata per scopi diversi da quelli ai quali è destinata, senza espressa autorizzazione scritta del responsabile informatico.

- E' fatto divieto di far circolare nelle rete interna file non espressamente autorizzati, né software non forniti dalla società né alcuna notizia, informazione o dato non inerente l'attività aziendale.

- E' vietato utilizzare la rete per operazioni non attinenti l'azienda o l'attività e le mansioni cui l'utente è preposto.

- E' vietato prelevare dalla rete documenti, file o dati non attinenti lo svolgimento delle attività aziendali, le mansioni od i progetti in cui l'utente opera.

- Devono essere previsti ed attuati meccanismi di monitoraggio delle attività di rete per fini organizzativi o di controllo della sicurezza dell'impianto.

E. Sicurezza dei server

- Deve essere previsto un sistema costante di controllo sui sistemi di prevenzione del sistema tale da garantire la sicurezza dei server. Devono essere mantenuti aggiornati tutti i programmi che possono essere oggetto di attacco dagli hacker. Deve essere impostata la modalità di aggiornamento automatico su tutti i sistemi.

- E' fatto assoluto divieto di utilizzare i server interni senza specifiche necessità ed al di fuori delle necessità aziendali. F. Installazione programmi Gli strumenti di lavoro, sia laptop che desktop vengono assegnati al personale già configurati per l'utilizzo che se ne prevede.

Le configurazioni software non possono essere modificate se non dietro espressa autorizzazione della società. Si ricorda che:

- Sul personal computer in uso non devono essere installati dall'utilizzatore applicativi che non siano ufficialmente forniti/autorizzati dall'azienda, alla quale compete la definizione del sistema operativo ritenuto idoneo e gli strumenti di produzione individuale;
- E' vietato acquisire ed installare, per scopi personali o aziendali, programmi reperiti in rete o da qualunque altra sorgente esterna fatto salvo espressa autorizzazione della società;
- Qualora a seguito di controllo sui pc in uso, risulti presente un software non espressamente autorizzato dalla società, potranno essere posti in essere richiami disciplinari (i programmi in questione saranno rimossi).

G. Sicurezza locale – antivirus

Ogni computer deve essere dotato di un proprio antivirus che si aggiorna automaticamente via internet. Se non è attivato il firewall personale deve essere attivato quello fornito con il sistema operativo. Il server di posta

aziendale deve essere provvisto di un antivirus che analizza le e-mail in ingresso e cancella quelle infette e di un antispam che elimina le e-mail che non provengono da un server di posta canonico.

I.6. FLUSSI INFORMATIVI VERSO L'ODV

Sussiste a carico di tutti i Destinatari del MOG (Apicali, sottoposti, consulenti informatici, etc.) un obbligo di segnalazione immediata all'OdV in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nella presente parte speciale del Modello, nelle procedure aziendali, nel Modello Organizzativo e nel Codice Etico.

Le segnalazioni dovranno avvenire attraverso comunicazione via e-mail alla casella di posta elettronica dell'ODV.

Con riferimento ai controlli periodici sui processi aziendali ed alle tempistiche con cui trasmettere le informazioni all'OdV, il D.Lgs. n. 231/01 prevede specifici flussi informativi verso l'OdV, a carico di tutti i Destinatari del Modello, come meglio specificato nella Procedura "Flussi Informativi".