PARTE SPECIALE – Delitti informatici e trattamento illecito dei dati ai sensi dell'art. 24 bis del D.Lgs. 231/2001

L'art. 7 della legge 18 marzo 2008, n. 48, che ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica, ha inserito nel D.Lgs. 231/01 l'art. 24 bis afferente tutti i delitti informatici compresi quelli innovati ed introdotti *ex novo* dalla medesima legge.

L'articolo 24-bis del D.Lgs. 231/2001[1], rubricato "Delitti informatici e trattamento illecito dei dati" stabilisce:

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[2], n. 105, si applica 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, lettera 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).

I reati indicati in questa disposizione di legge sono riconducibili a queste tipologie di reato:

1. Le falsità

- (art. 491 bis. c.p.) Documenti informatici

2. Delitti contro la riservatezza informatica (e la indisturbata fruizione del sistema informatico)

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

---

[1] Da ultimo aggiornato dalla Legge 28 giugno 2024, n. 90.

[2] Inserito dall'Articolo 1, comma 11-bis del decreto-legge 21 settembre 2019, n. 105 recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", che ha introdotto una nuova fattispecie di reato prevedendo sanzioni a carico delle società nei casi di ostacoli all'attuazione degli adempimenti previsti da tale normativa.

- (art. 615 quater c.p.) Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici
- (art. 635 quater.1 c.p.) Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

3. Delitti contro l'inviolabilità dei segreti

- (art. 617 quater) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- (art. 617 quinquies) Detenzione, diffusione e installazione di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

4. Delitti contro il patrimonio mediante violenza alle cose o alle persone

- (art. 629, co. 3) Estorsione informatica
- (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. 639 ter c.p.) Circostanze attenuanti

5. Delitti contro il patrimonio mediante frode

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

6. Perimetro di sicurezza nazionale cibernetica

- (art. 1, comma 11, D.L. n. 105/2019) Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica

Segue la lettera degli articoli del Codice Penale che vengono in rilievo, accompagnata da una sintetica spiegazione della singola fattispecie.

1. Le falsità

Art. 491 bis c.p. Documenti informatici

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

Questa disposizione, inserita dall'art. 3 della legge 23 dicembre 1993, n. 547, è stata modificata dalla legge 18 marzo 2008, n. 48 che ha soppresso il secondo periodo dell'articolo ed ha aggiunto la locuzione "avente

efficacia probatoria" specificando la nozione di documento informatico rilevante ai fini dell'applicabilità del titolo del codice penale sulle falsità in atti.

Da ultimo, questa disposizione è stata modificata dall'art. 2 lettera e) del decreto legislativo 15 gennaio 2016, n. 7, che ha eliminato il riferimento alle falsità riguardanti i documenti informatici privati e, di conseguenza, il rimando all'applicazione per gli stessi delle disposizioni concernenti le scritture private.

2. Delitti contro la riservatezza informatica (e la indisturbata fruizione del sistema informatico)

Art. 615 ter c.p. Accesso abusivo ad un sistema informatico o telematico

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

La pena è della reclusione da due a dieci 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 ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità del titolare 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 tre a dieci anni e da quattro a dodici anni.

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

Il presente articolo è stato aggiornato dall'art. 16 della Legge 28 giugno 2024, n. 90.

Il bene giuridico protetto dal precetto in esame è la riservatezza delle comunicazioni e/o delle informazioni il cui scambio avviene tramite sistemi informatici.

Per "sistema informatico" deve intendersi un insieme di apparecchiature destinate ad assolvere funzioni utili all'uomo attraverso l'utilizzo (anche parziale) di tecnologie informatiche.

Si precisa che:

- la condotta penalmente rilevante è duplice e si concretizza nell'accesso abusivo ad un sistema informatico protetto o nella permanenza in detto sistema nonostante l'espressione di volontà contraria da parte di chi ha il diritto di escluderlo;
- l'elemento soggettivo è il dolo generico, inteso quale coscienza e volontà di entrare in un sistema e di permanervi contro la volontà dell'avente diritto;
- il reato è di mera condotta e si consuma quando l'agente porta a compimento una delle condotte sopra descritte ovvero accede al sistema informatico, senza che sia necessario che si configuri una lesione del sistema o che l'accesso sia stato effettuato con il fine di violare la riservatezza degli utenti autorizzati.

Art. 615 quater c.p. 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 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.

2. 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).

3. 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.

Il presente articolo è stato aggiornato dall'art. 16 della Legge 28 giugno 2024, n. 90 e, prima, ampiamente modificato dalla L. n. 238/2021 che, per quanto di interesse in questa sede, ha aggiunto le condotte di detenzione, produzione, importazione e installazione come rilevanti per la commissione del reato aggiungendo, altresì, una previsione ampia di chiusura "*mette in altro modo a disposizione di altri*".

Il reato previsto dal precetto è un reato di pericolo finalizzato a prevenire la commissione di delitti più gravi contro la riservatezza o contro il patrimonio.

Si precisa che:

- la condotta penalmente rilevante consiste nel detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, o mettere comunque a disposizione di altri password per l'accesso ad un sistema informatico o telematico ovvero installare apparati o strumenti (o parti di essi) idonei ad accedere a un sistema informatico o telematico;
- l'elemento soggettivo è il dolo specifico in quanto la condotta deve essere perpetrata al fine di procurare a sé o ad altri un profitto ovvero per cagionare un danno;
- il reato si consuma con il porre in essere le condotte descritte.

Le aggravanti previste dal secondo comma della norma in esame afferiscono alla natura del sistema informatico o al soggetto che compie la violazione[3].

Art. 635 quater.1 c.p. 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.

2. 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).

3. 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, primo periodo.

Il reato *de quo* è stato oggetto di aggiunta all'interno del catalogo delle fattispecie rilevanti ad opera dell'art. 16 della Legge 28 giugno 2024, n. 90, sostituendo l' art. 615 quinquies c.p., oggetto di abrogazione. L'articolo precedentemente in vigore era stato, invero, adeguato a quanto previsto nella Convenzione del Consiglio d'Europa nel senso di un maggiore severità nella configurazione del reato. Inoltre, la L. n. 238/2021 ha aggiunto quali condotte rilevanti, oltre alla diffusione, la detenzione e l'installazione di apparecchiature, dispositivi o programmi informatici e ha introdotto l'avverbio "abusivamente".

Si precisa che:

- si configura come reato di pericolo astratto;
- le condotte penalmente rilevanti consistono nel produrre, riprodurre, detenere, procurarsi, importare, diffondere, comunicare, consegnare e mettere a disposizione di altri virus informatici;
- l'elemento soggettivo richiesto è il dolo specifico, ovvero la coscienza e volontà nel porre in essere una delle condotte descritte al fine di danneggiare il sistema;
- il reato si consuma nel momento in cui una delle condotte viene realizzata senza che rilevi il conseguimento dello scopo lesivo.

A seguito della riforma della norma apportata dalla Legge 28 giugno 2024, n. 90, sono state inserite due circostanze aggravanti nel secondo e terzo comma, che si concretizzano qualora il fatto sia perpetrato da un pubblico ufficiale abusando dei propri poteri, da un incaricato di pubblico servizio ovvero da un investigatore privato, o ancora se commesso a danno di un pubblico ufficiale nell'esercizio delle sue funzioni o in ragione delle stesse.

[3] Le aggravanti saranno oggetto di un'analisi più dettagliata nel prosieguo della trattazione, avuto riguardo alla disamina dell'art. 617 quater c.p., cui l'art. 615 quater fa espresso richiamo.

3. Delitti contro l'inviolabilità dei segreti.

Art. 617 quater c.p. Intercettazione, impedimento, o interruzione illecita di comunicazioni informatiche o telematiche.

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e 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 quattro a dieci anni se il fatto è commesso:

1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma;

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.

Il presente articolo è stato modificato dall'art. 16 della Legge 28 giugno 2024, n. 90. Il bene giuridico protetto dalla norma è la segretezza delle comunicazioni che, oltre ad essere telefoniche (art. 617 c.p.) e telegrafiche (617 bis c.p.), sono, soprattutto al giorno d'oggi, informatiche.

Si precisa che:

- le condotte penalmente rilevanti consistono nell'intercettazione, interruzione o impedimento delle comunicazioni di un sistema informatico o telematico o di più sistemi in comunicazione tra loro, ovvero nel rivelare con qualsiasi mezzo di informazione, il contenuto di predette comunicazioni;
- l'intercettazione delle comunicazioni deve avvenire con mezzi fraudolenti;
- l'elemento soggettivo è il dolo generico, inteso come coscienza e volontà di porre in essere una delle condotte sopra descritte.

Aggravanti speciali sono, da ultimo, previste nel comma terzo della norma in esame.

Esse sono:

- la natura statale, pubblica o l'appartenenza ad un'impresa esercente attività di pubblico servizio o di pubblica utilità del sistema in danno del quale vengono poste in essere le condotte penalmente rilevanti;
- la qualifica di pubblico ufficiale o di incaricato di pubblico servizio dell'agente qualora perpetri una delle condotte descritte con abuso dei poteri, violazione dei doveri inerenti al servizio od alla funzione o con abuso della qualità di operatore del sistema;
- l'esercizio abusivo della professione di investigatore privato.

Il verificarsi delle aggravanti sopra esposte implica la procedibilità d'ufficio del reato nonché l'applicabilità della pena della reclusione da tre a otto anni.

Art. 617 quinquies Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

1. 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.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

2. 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.

3. 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.

Il presente articolo è stato modificato dall'art. 16 della Legge 28 giugno 2024, n. 90 e modificato dalla L. n. 238/2021 che ha esteso le condotte penalmente rilevanti.

La fattispecie di reato in esame ha la funzione di punire le attività prodromiche all'intercettazione, impedimento od interruzione delle comunicazioni.

Si precisa che:

- le condotte penalmente rilevanti consistono nell'installazione (o nel metterle comunque a disposizione) di apparecchiature, programmi, codici, parole chiave o altri mezzi idonei a violare la segretezza delle comunicazioni;
- l'elemento soggettivo richiesto è il dolo specifico inteso come finalità di procedere all'installazione di apparecchiature atte all'intercettazione, impedimento od interruzione della comunicazione;
- il reato si consuma con l'installazione delle apparecchiature.

Sono applicabili le aggravanti speciali del quarto comma dell'art. 617 quater c.p.

4. Delitti contro il patrimonio mediante violenza alle cose o alle persone

Art. 629 c.p. Estorsione informatica

Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.

La pena è della reclusione da sette a venti anni e della multa da da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate nel terzo comma dell'art. 628 c.p.

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.

Art. 635 bis c.p. Danneggiamento di informazioni, dati e programmi informatici.

1. 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.

2. 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.

Il reato è stato aggiornato dall'art. 16 della Legge 28 giugno 2024, n. 90 ed è stato ridelineato dalla legge 48/08 che ha ovviato ad alcune critiche mosse dalla dottrina in quanto la fattispecie riproduceva, pedissequamente, quella costruita per il reato di "danneggiamento", non tenendo conto delle specificità afferenti i beni informatici.

Si precisa che:

- le condotte penalmente rilevanti consistono nel distruggere, deteriorare, danneggiare informazioni, dati o programmi informatici (software);
- l'elemento soggettivo è il dolo generico inteso come coscienza e volontà del porre in essere la condotta descritta con la consapevolezza dell'altruità dell'oggetto materiale del reato;
- il delitto si consuma con il verificarsi dell'evento di danneggiamento.

Costituisce circostanza aggravante del reato il fatto che sia stato commesso con violenza o minaccia alla persona o con l'abuso della qualità di operatore di sistema.

Art. 635-ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

1. 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.

2. 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.

3. 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).

La norma è stata introdotta *ex novo* dalla legge 48/08 ed è stata da ultimo aggiornata dalla Legge 28 giugno 2024, n. 90.

La struttura del reato è analoga a quella descritta nell'art. 635 bis c.p., sia dal punto di vista delle condotte rilevanti, dell'oggetto materiale del reato nonché dell'elemento soggettivo.

La peculiarità della fattispecie risiede nel fatto che le informazioni, i dati e i programmi informatici sono utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque, di pubblica utilità.

Quando la lesione delle informazioni, dei dati o dei programmi si realizza è previsto un aggravio sanzionatorio.

Da ultimo, il terzo comma della disposizione è stato modificato dall'art. 2 lettera n) del decreto legislativo 15 gennaio 2016, n. 7, che, intervenendo sulla prima parte dello stesso, ha sostituito la locuzione "Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635" con la locuzione "Se il fatto è commesso con violenza alla persona o con minaccia".

Art. 635-quater c.p. Danneggiamento di sistemi informatici o telematici.

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, 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.

2. 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.

La fattispecie di reato è stata introdotta dalla legge n. 48/08. In ossequio a quanto previsto nella Convenzione ratificata con la medesima legge, la fattispecie dell'art. 635 bis c.p. è stata sdoppiata, ovvero le condotte penalmente rilevanti sono state ripartite in due distinte fattispecie. E' stata altresì introdotta una ulteriore specificazione dei possibili e peculiari comportamenti lesivi dei sistemi informatici o telematici.

Da ultimo, il secondo comma della disposizione è stato modificato dall'art. 2 lettera o) del decreto legislativo 15 gennaio 2016, n. 7, che, intervenendo sulla prima parte dello stesso, ha sostituito la locuzione "Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635" con la locuzione "Se il fatto è commesso con violenza alla persona o con minaccia".

Da ultimo il reato è stato aggiornato dalla Legge 28 giugno 2024, n. 90.

Art. 635-quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità.

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.

2. 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.

*3. 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).*La fattispecie è analoga, in quanto a struttura, a quella dell'art. 635 ter c.p.

Il presente articolo è stato ridelineato dall'art. 16 della Legge 28 giugno 2024, n. 90.

Art. 639 ter c.p. - Circostanze attenuanti

Le pene comminate per i delitti di cui agli articoli 629, terzo comma, 635 ter, 635 quater 1 e 635 quinquies sono diminuite quando, per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.

Le pene comminate per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.

Non si applica il divieto di cui all'articolo 69, quarto comma.

5. Delitti contro il patrimonio mediante frode

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

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.

La fattispecie è stata introdotta dalla L. n. 48/08.

Si precisa che:

- la condotta penalmente rilevante va individuata nella violazione della normativa afferente i certificatori accreditati e qualificati (cfr. D.Lgs. 7 marzo 2005, n. 82);
- l'elemento soggettivo è il dolo specifico che va ricercato nel fine ulteriore del certificatore di procurare a sé un ingiusto profitto ovvero di cagionare ad altri un danno.

6. Perimetro di sicurezza cibernetica

Art. 1, comma 11, D.L. n. 105/2019

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, e' punito con la reclusione da uno a tre anni [e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote].

Il presente articolo è stato inserito nel catalogo dei reati presupposto ad opera del D.L. n. 105/2019, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133.

La nuova fattispecie di reato prevede sanzioni a carico delle società nei casi di ostacoli all'attuazione degli adempimenti previsti dalla normativa (censimento reti, sistemi informativi e servizi informatici comprensivo di architettura e componentistica; affidamento forniture di beni e di servizi ICT e relativi test; attività ispettive e di vigilanza) e, pertanto, è un reato c.d. proprio.