LAURINI OFFICINE MECCANICHE S.R.L.

Organismo di Vigilanza

Organismo di Vigilanza

Adempimenti in relazione alle linee guida sui reati informatici, in relazione all'aggiornamento per adeguamento alle modifiche apportate dalla L.90/24 e dal perimetro di sicurezza nazionale.

1. I delitti informatici e trattamento illecito di dati

Art. 24-bis D.lgs. 231/01
Delitti informatici e trattamento illecito di dati
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).

2. Inquadramento generale

La presente parte speciale riguarda i reati presupposto previsti dall'art. 24-bis del D.lgs. n. 231/2001 avente ad oggetto i delitti informatici e il trattamento illecito dei dati. Le novità normative hanno comportato, da un lato, modifiche ai precedenti reati presupposto e, dall'altro, l'introduzione di nuove fattispecie che si sono rese necessarie per fare fronte alle innovazioni informatiche e telematiche. Lo sviluppo e l'utilizzo sempre maggiore delle tecnologie informatiche e telematiche all'interno dei sistemi aziendali e della Pubblica amministrazione hanno evidenziato la necessità di una maggiore e mirata repressione di quelle condotte illecite finalizzate all'accesso indebito in tali sistemi da parte di soggetti altrui la c.d. "criminalità informatica". La criminalità informatica è quel fenomeno criminale che si caratterizza per l'abuso e per l'uso disfunzionale della tecnologia informatica attraverso un elevato numero di tecniche in rapida espansione per attaccare i computer, smartphone, tablet e i dati in essi contenuti. Lo schema dell'illecito penale tradizionale viene in un certo qual modo scardinato in quanto i concetti di luogo e tempo sono vaghi poiché i crimini che si realizzano "in rete" possono essere sganciati dai concetti di spazio e di tempo potendo le attività essere pianificate e realizzate con operazioni programmate senza che vi sia necessità della presenza fisica dinnanzi al computer. La normativa di seguito descritta si è resa, dunque, necessaria a causa dell'espansione e dell'evoluzione delle reti informatiche che ha fatto emergere la necessità di consentire che l'utilizzo di un sistema informatico avvenga in condizioni di sicurezza, garantendo la libertà e l'autonomia di chi fa uso di siffatti sistemi e, al tempo stesso, di assicurare l'integrità e la riservatezza del sistema e dei dati ivi raccolti al fine di porre un valido argine all'espandersi della c.d. "criminalità informatica".

Occorre brevemente ripercorrere l'iter legislativo che ha condotto all'attuale assetto dell'articolo 24 bis del D.lgs. 231/01.

Con la Legge 23 dicembre 1993, n. 547, rubricata «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informativa», emanata su impulso della Raccomandazione n. 9 del 1989 del Consiglio d'Europa, il legislatore ha introdotto nuovi reati attinenti al mondo informatico.

Con il successivo intervento, ad opera della Legge 18 marzo 2008, n. 48, («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 legislatore ha inteso ricomprendere tra i reati presupposto all'interno della disciplina prevista in tema di responsabilità amministrativa dell'ente anche i delitti informatici. Difatti, con l'art. 12 della citata convenzione, il legislatore europeo ha imposto agli Stati di prevedere forme di responsabilità per le persone giuridiche che avessero commesso reati informatici a proprio vantaggio o nel proprio interesse. L'inserimento di tali reati presupposto nasce dall'esigenza di tutelare l'organizzazione e il patrimonio informatico.

La disciplina è stata oggetto di numerosi interventi legislativi. Nello specifico, con la Legge 238/21, il legislatore ha introdotto numerose modifiche al codice penale, tra cui gli artt. 615 quater, 615 quinquies, 617,617 bis, 617 quater e 617 quinquies c.p.

Recentemente, la normativa è stata oggetto di ulteriore modifica ad opera della Legge 28 giugno 2024, n. 90. Con tale intervento legislativo, si è cercato di rafforzare le misure nazionali in materia di cybersicurezza e di prevenire e inasprire le pene per i reati informatici. All'art. 20 della menzionata legge, difatti, il legislatore è intervenuto sul catalogo dei reati presupposto della responsabilità amministrativa degli enti di cui all'art. 24-bis del D.lgs. n. 231/2001. In particolare: (i) sono state innalzate le sanzioni previste (i.e. da 300 e 500 quote a 200 e 700 quote) (ii) è stata introdotta la sanzione pecuniaria da 300 a 800 quote in relazione alla commissione della nuova fattispecie di estorsione informatica di cui all'art. 629, co. 3 del c.p.; (iii) è stata modificata la sanzione pecuniaria originariamente prevista dal comma 2 dell'art. 24-bis e sono stati sostituiti alcuni dei reati ivi previsti.

Tanto premesso, prima di esaminare le singole fattispecie nel dettaglio, appare necessario chiarire alcune nozioni comuni a molti dei reati presupposto di cui all'art. 24-bis del D.lgs. n. 231/2001 e che consentono di individuare i confini della condotta illecita da prevenire. In particolare:

(i) per sistema informatico, si intende il complesso organico di elementi fisici (hardware) ed astratti (software) che compongono un apparato di elaborazione dati. L'art. 1 della convenzione di Budapest definisce sistema informatico qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati. In altri termini, per sistema informatico si intende una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione, anche in parte, di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di codificazione e decodificazione - dalla registrazione o memorizzazione, per mezzo di impulsi

elettronici, su un supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esaminare una particolare significato per l'utente.

(ii) per sistema telematico si intende, invece, ogni forma di telecomunicazione che si giovi dell'apporto informatico per la sua gestione oppure che sia al servizio di tecnologie informatiche, indipendentemente dal fatto che la comunicazione avvenga via cavo, via etere o con altri sistemi.

(iii) per misure di sicurezza, in assenza di una definizione sul punto, si intendono genericamente le protezioni apposte sia a livello di apparecchiature hardware sia di programmi (software) aventi lo scopo di impedire il libero accesso al sistema informatico o telematico. Rientrano in tale ambito anche le misure di carattere sia fisico (es. Chiavi metalliche per l'accensione dell'elaboratore) che organizzativo nonché i dispositivi tecnici di identificazione (es. le impronte digitali) o di natura logica (codici alfanumerici);

(iv) Per dato si intende un valore, tipicamente numerico in bit, che può essere elaborato e/o trasformato da un automa o meglio da un elaboratore elettronico. L'informazione, invece, è composta da una serie di dati tra loro connessi, mentre il programma informatico rappresenta il procedimento algoritmico applicato ad un problema dato da automatizzare, il quale viene poi tipicamente codificato in una serie di linee di codice scritte, utilizzando un linguaggio di programmazione da un programmatore in fase di programmazione del software, che può essere eseguito da un elaboratore, ricevendo specifici input di dati e restituendo in output gli eventuali risultati ottenuti a seguito dell'esecuzione/elaborazione delle sue istruzioni.

Di seguito verranno descritte le singole condotte dei reati presupposto per consentire ai destinatari del MOG di conoscere le condotte da prevenire e per orientarsi nella terminologia "tecnica" utilizzata dal legislatore, non sempre di facile comprensione.

3. FATTISPECIE E SANZIONI

Il presente paragrafo si riferisce ai delitti informatici e trattamento illecito dei dati, di cui all'art. 24-bis del D.lgs. 231/2001.

Di seguito, si riporta la descrizione, le sanzioni, gli esempi di condotte in concreto delle singole fattispecie delittuose previste dall'art. 24-bis del D.lgs. n. 231/2001.

3.1 Art. 615 ter Codice Penale: «Accesso abusivo ad un sistema informatico o telematico»

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 minaccia o 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 al 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.».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[1].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione

[1] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

dell'illecito; e) il divieto di pubblicizzare beni o servizi».

- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

Descrizione del reato di cui all'art. 615 ter c.p. (considerazioni specifiche)

L'art. 615-ter c.p. è stato introdotto dall'art. 4 della legge n. 547/1993 ed è stato collocato nel Codice penale al titolo «Delitti contro la persona», sezione «Delitti contro l'inviolabilità del domicilio». Tale collocazione assume particolare rilievo soprattutto se si tiene conto del fatto che la formulazione dell'art. 615-ter c.p. riprende in parte quanto previsto dall'art. 614 c.p., in materia di violazione del domicilio. In tal senso, il legislatore ha assimilato l'accesso abusivo ad un sistema informatico o telematico a quello del comune delitto di violazione di domicilio. Da ultimo, con la Legge 90 del 2024, il legislatore è intervenuto inasprendo le pene previste per il reato in commento e ampliando la fattispecie delittuosa. Nello specifico, è stata aumentata la pena prevista per le circostanze aggravanti ed è stato esteso il perimetro dell'aggravante di cui al comma 2, n. 3) anche per quelle condotte che, oltre al danneggiamento o distruzione dei sistemi, provocano la sottrazione, riproduzione, trasmissione o l'inaccessibilità ai dati e ai programmi in essi contenuti. Con riferimento, invece, all'aggravante di cui al comma 2, n. 2, il legislatore ha previsto che la condotta ivi descritta si realizza anche nell'ipotesi di minaccia sulle cose o alle persone.

Il bene giuridico tutelato dalla norma è il domicilio informatico inteso quale estensione del domicilio fisico. Il sistema informatico o telematico, difatti, costituisce - al pari del domicilio - un luogo inviolabile delimitato da uno spazio virtuale in cui l'individuo esplica liberamente la sua personalità in tutte le sue dimensioni e manifestazioni. Difatti, dalla lettera della norma si desume che l'intento del legislatore non è solo quello di tutelare i contenuti personalissimi dei dati raccolti nei sistemi informatici ma anche il luogo in cui essi sono contenuti, indipendentemente dal contenuto dei dati, purché riferibili alla sfera di pensiero o all'attività lavorativa dell'utente. In tal modo, la norma tutela anche gli aspetti economici e patrimoniali. La disposizione, difatti, non opera distinzioni tra sistemi a seconda dei contenuti ma si limita a richiedere che si tratti di sistemi protetti da misure di sicurezza.

Con tale fattispecie delittuosa si intende, altresì, tutelare il diritto alla riservatezza informatica delle comunicazioni e delle informazioni contenute e trasmesse mediante i sistemi informatici o telematici.

In altri termini, non si tratta di tutelare uno spazio materialmente inteso, quanto piuttosto uno spazio virtuale di cui il titolare deve poter godere in maniera esclusiva ed al riparo da ingerenze altrui. Si vuole, dunque, offrire tutela ad uno spazio in cui sia possibile estrinsecare la propria personalità

(art. 2 cost.), indipendentemente dalla presenza in esso di dati.

Si tratta, dunque, di un reato plurioffensivo, in quanto posto a tutela di interessi molteplici e variegati, rilevanti non solo a livello patrimoniale – quale il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo - ma anche a livello pubblicistico - qual è il diritto alla riservatezza, i diritti afferenti alla sfera militare, sanitaria, quelli inerenti all'ordine pubblico e alla sicurezza e, tra essi, anche quello al corretto funzionamento dell'amministrazione giudiziaria.

La norma prevede due ipotesi di condotta alternative:

(i) la condotta di colui che abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza;

(ii) la condotta di colui che, pur potendo legittimamente accedere al sistema, vi permane contro la volontà, espressa o tacita, dell'avente diritto.

L'elemento soggettivo richiesto per la realizzazione del reato è il dolo generico, ossia la consapevolezza dell'agente di introdursi o mantenersi volontariamente nell'altrui sistema informatico o telematico ovvero nella memoria interna di un elaboratore, senza il consenso del titolare e con la consapevolezza che quest'ultimo ha posto in essere misure di protezione del sistema.

La norma, dunque, sanziona l'accesso abusivo al sistema informatico telematico indipendentemente dalla finalità perseguita dall'agente, in quanto rilevante è il carattere abusivo dell'accesso stesso, compiuto violando le misure di sicurezza esistenti. Proprio con riferimento a quest'ultimo occorre segnalare che, per la realizzazione della fattispecie delittuosa è irrilevante il grado di idoneità ed efficacia delle misure di sicurezza, essendo sufficiente che queste esistano e vengano violate. A titolo di esempio potrebbe, dunque, integrare il reato di cui all'art. 615 ter c.p. la condotta di colui che accede abusivamente all'altrui casella di posta elettronica, trattandosi di uno spazio di memoria, protetto da una password personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio[2].

Il reato si consuma nel momento in cui il soggetto si introduce ovvero oltrepassa le barriere logiche e/o fisiche a cui è subordinato l'accesso ai dati ed ai programmi contenuti nella memoria del sistema. Viceversa, il reato non può dirsi consumato nell'ipotesi in cui il soggetto abbia iniziato ad interagire con il computer altrui (a.e. accendendolo) ma non sia riuscito a superare le barriere di

[2] Cfr. Cass., Sez. V, 28.10.2015-31.3.2016, n. 1305

protezione.

A tal fine, con il termine "accesso" si intende non tanto il semplice collegamento fisico o l'accensione dello schermo, ma quello logico, ossia il superamento della barriera di protezione del sistema che rende possibile il dialogo con il medesimo in modo che l'agente venga a trovarsi nella condizione di conoscere dati, informazioni e programmi. La norma, difatti, non prende in esame l'eventuale conoscenza di dati o programmi contenuti nel sistema informatico, ma si limita a considerare illegittimo il superamento delle barriere poste a tutela del sistema informatico.

Pertanto è sufficiente che l'agente si sia introdotto nel sistema altrui e abbia la possibilità, in astratto di visualizzare i documenti. In tal modo si realizza quella situazione di pericolo per la segretezza dei dati e dei programmi memorizzati nel l'elaboratore che giustifica l'intervento della sanzione penale.

Quanto, invece, alla seconda ipotesi, ossia la condotta del mantenersi nel sistema protetto contro la volontà espressa o tacita del titolare anche in questo caso, assume rilevanza penale, ai fini della punibilità, la mera permanenza nel sistema e non le attività poste in essere contestualmente, quali l'effettiva presa di conoscenza di dati o informazioni.

Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico è quello si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente[3].

Il delitto in commento costituisce un reato di mera condotta,(ad eccezione delle ipotesi di cui al secondo comma nn. 2 e 3) il quale si perfezionale con la violazione del domicilio informativo e, dunque, l'introduzione in un sistema informatico costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione della stessa.

Dal momento che oggetto di tutela è il domicilio virtuale e che i dati contenuti all'interno del sistema non sono in via diretta ed immediata protetti, consegue che l'eventuale uso illecito delle informazioni può integrare un diverso titolo di reato.

Per quanto riguarda le circostanze aggravanti, in presenza delle quali si registra un notevole inasprimento della pena edittale (da due a dieci anni), la norma ne prevede 4 (cfr. commi 2 e 3). Si tratta di circostanze ad effetto speciale che consentono che si proceda d'ufficio, ciò a differenza dell'ipotesi base del reato che, invece, è perseguibile a querela di parte.

Con riferimento alla prima circostanza aggravante, questa si caratterizza per lo specifico ruolo dell'autore del reato. In particolare, il comma 2 dell'art. 615 ter c.p. prevede l'aggravamento della penale nel caso in cui ad agire:

[3] Cfr. Cass. SS.UU, 24 aprile 2015, n. 17325

(i) sia il pubblico ufficiale ovvero l'incaricato di pubblico servizio, abusando dei propri poteri o violando i doveri inerenti alla propria funzione o al servizio; o

(ii) chi esercita abusivamente la professione di investigatore; nonché

(iii) per chi agisce abusando della qualità di operatore del sistema.

L'ipotesi si concretizza laddove l'accesso al sistema informatico viene commesso da un soggetto abilitato, abusando dei propri poteri ovvero violando i doveri inerenti la sua funzione o servizio. In conseguenza della particolare categoria di soggetti coinvolti, non risulta solo leso il diritto alla riservatezza ma anche il principio di imparzialità e buon andamento della P.A. (art. 97 Cost.) e, per tale ragione, il reato è procedibile d'ufficio.

La seconda circostanza aggravante, invece, riguarda le modalità della condotta (se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone ovvero se è palesemente armato).

Diversamente, la terza circostanza aggravante prevista al comma 2, n. 3 riguarda le conseguenze della condotta. In particolare, la norma fa riferimento all'eventualità che dal fatto (i.e. «accesso abusivo») derivi la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, l'inaccessibilità al titolare del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento di dati, informazioni o programmi «in esso contenuti».

In tale ipotesi, deve sussistere un nesso funzionale tra il danneggiamento e la realizzazione del reato di accesso abusivo. In altri termini, il danneggiamento deve costituire mezzo necessario o agevolatore.

Infine, ai sensi del 3° co., le condotte di cui al 1° ed al 2° comma le condotte delittuose sono sanzionate più gravemente laddove abbiano ad oggetto sistemi informatici o telematici di interesse pubblico, tra i quali rientrano, i sistemi «di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile». In tal senso, il legislatore ha inteso tutelare l'interesse collettivo al regolare funzionamento dei sistemi di interesse pubblico e la maggiore riservatezza dei dati contenuti all'interno degli stessi.

- Esempi di condotte idonee ad integrare il reato

A mero titolo esemplificativo, il reato si potrebbe configurare attraverso l'accesso abusivo al sistema di altro soggetto, protetto da misure di sicurezza, da parte di un dipendete di Laurini Officine Meccaniche S.r.L.. Il vantaggio può configurarsi, ad esempio, nell'acquisire dati ed informazioni utili per l'Ente e che lo stesso non potrebbe acquisire in altro modo.

3.2 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. 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 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 lire dieci milioni. 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). 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».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: sino a 400 quote (sino a 619.600)[4].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive « b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

[4] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

- Descrizione del reato di cui all'art. 615 quater c.p.

Il legislatore con la norma in commento ha inteso sanzionare l'abusiva acquisizione, diffusione e installazione con qualsiasi modalità, di apparecchiature, di mezzi o codici di accesso ovvero il fornire indicazioni utili o istruzioni per consentire a soggetti non legittimati l'accesso abusivo nel sistema informatico o telematico altrui, protetto da misure di sicurezza. Con tale disposizione si intende, dunque, prevenire le condotte prodromiche alla realizzazione del delitto di accesso abusivo al sistema informatico o telematico protetto da misure di sicurezza di cui al precedente articolo 615-ter c.p.

In altri termini, l'intento è quello di reprimere – indipendentemente dal verificarsi dell'evento – le condotte prodromiche alla realizzazione del delitto di accesso abusivo in un sistema informatico o telematico protetto da misure di sicurezza.

L'elemento soggettivo richiesto per la realizzazione del reato è il dolo specifico, vale a dire, la coscienza e volontà di procurarsi, riprodurre, diffondere, comunicare, consegnare, codici di accesso o mezzi similari al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno. In tal modo, non risponde del reato di cui all'art. 615-quater c.p. chiunque, per motivi leciti, comunichi una password di accesso ad un sistema informatico a terzi. Quest'ultima ipotesi ricorre nel caso in cui il proprietario di un computer, la cui scheda modem presenti difetti di funzionamento, comunichi la propria password al tecnico incaricato della riparazione.

Oggetto materiale della condotta sono, dunque, gli apparti, strumenti, parti di apparati o di strumenti, i codici, parole chiave e, infine, gli altri mezzi idonei all'accesso ad un sistema informatico o telematico che sia protetto da misure di sicurezza e, più in generale, tutti i mezzi – comprese le informazioni ed istruzioni – che permettono di accedere a tali sistemi protetti.

In merito alla nozione di «chiave di accesso» o «parola chiave», si intende la chiave che consente di collegarsi al sistema. Si può trattare di sequenze alfabetiche, numeriche o alfanumeriche o numerico logiche che, laddove digitate ovvero comunicate all'elaboratore, permettono di accedere ai dati ed ai programmi contenuti nella memoria interna.

Quanto alla nozione di «qualsiasi mezzo idoneo all'accesso», il legislatore ha inteso includere non solo tutti gli strumenti che consentono l'accesso al sistema, ma anche tutte le condotte che consentono al soggetto agente di accedervi. In altri termini, con tale clausola si si è inteso ricomprendere:

(i) i mezzi di accesso fisici che consentono direttamente l'accesso ad un sistema informatico protetto (es. tesserino magnetico di riconoscimento); e,

(ii) i mezzi logici, intesi come parole chiave nel senso di password, o come mezzi che

consentono di collegarsi logicamente al sistema; e, infine,

(iii) le indicazioni o istruzioni idonee a consentire l'accesso al sistema. Si tratta di tutte le informazioni tecniche riservate che, pur consistendo nella comunicazione o consegna del codice di accesso, svelano il metodo idoneo a raggiungere lo scopo o il modo idoneo ad eludere o neutralizzare le misure che proteggono il sistema dagli accessi abusivi ovvero che consentono o facilitano l'individuazione, la realizzazione, la riproduzione, la diffusione, la comunicazione o la consegna di mezzi idonei all'accesso a sistemi protetti.

In tal senso, costituisce mezzo idoneo allo scopo anche l'apprendere un'informazione riservata su come aggirare le misure di sicurezza "craccando" una password ovvero utilizzando i c.d. hacking tools.

La condotta tipica consiste, alternativamente, nel procurarsi, detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri o installare apparati, strumenti, parti di apparati o di strumenti.

Per quanto riguarda la nozione del termine "procurarsi", si fa riferimento all'appropriarsi in qualsiasi modo – anche mediante autonoma elaborazione – dei mezzi necessari per accedere al sistema informatico altrui. Questa può, dunque, concretizzarsi con l'acquisizione materiale della chiave metallica o della scheda magnetica ovvero con l'individuazione dei codici di accesso attraverso procedimenti logici tipici del computer.

Quanto alla riproduzione questa consiste nella realizzazione di una copia abusiva di un codice di accesso idoneo all'uso. Mentre per diffusione si intende la divulgazione ad un numero indeterminato di persone di un codice di accesso.

Quest'ultima ipotesi si differenzia da quella della comunicazione, la quale può avere ad oggetto solo mezzi di accesso logici (cioè, incorporei) ed è, per di più, rivolta ad una cerchia determinata di persone. Differente è, altresì, la consegna che ha ad oggetto solo cose materiali (es. schede magnetiche).

Il bene giuridico tutelato dalla norma è la riservatezza informatica e, in via mediata, la sicurezza informatica. Con la previsione normativa in commento, il legislatore ha inteso tutelare in via anticipata il domicilio informatico e, più in particolare, la segretezza dei dati e dei programmi contenuti all'interno dell'elaboratore.

Il reato si consuma nel momento e nel luogo in cui si realizza la condotta tipica, ossia nel momento in cui il soggetto agente acquista la disponibilità del codice di accesso entrando materialmente in possesso di esso, o lo individua, ovvero nel momento in cui viene compiuto il primo atto di diffusione o si realizza la comunicazione o la consegna a terzi di tali mezzi o di informazioni circa il

modo di eludere le barriere di protezione di un sistema informatico.

Per quanto riguarda le circostanze aggravanti, in presenza delle quali si registra un notevole inasprimento della pena edittale, la norma rinvia all'ipotesi descritte nel precedente articolo 615-ter, comma 2, n. 1) e comma 3, c.p., cui si rinvia.

- Esempi di condotte idonee ad integrare il reato

Si pensi al caso in cui, un tecnico informatico collaboratore sviluppa o detiene un software in grado di accedere a sistemi informatici protetti. Lo scopo è ottenere l'accesso ai database di un'altra società per acquisire informazioni su sistemi di lavorazione o informazioni commerciali. Il tecnico così fornisce uno strumento utile alla società per raccogliere dati strategici che consentono di migliorare le tecniche di lavorazione e/o rafforzare e migliorare i propri rapporti con aziende e istituzioni, utilizzando le informazioni acquisite illecitamente. In tal modo, l'ente potrebbe ottenere un vantaggio economico diretto sotto forma di incremento di clienti e miglioramento dei tempi di lavorazione etc.

3.3 Art. 635 bis c.p.: «Danneggiamento di informazioni, dati e programmi informatici »

Art. 635 bis c.p.
Danneggiamento di informazioni, dati e programmi informatici
«Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da 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».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. n. 231/2001
- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[5].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.
- Descrizione del reato di cui all'art. 635-bis c.p.

L'art. 635-bis costituisce una particolare ipotesi di danneggiamento caratterizzata dall'oggetto materiale della condotta. Si tratta di una disposizione introdotta nel codice penale dall'art. 5, comma 2, della Legge 18 marzo 2008, n. 48 per colmare le lacune previste dalla disciplina. La fattispecie delittuosa è stata, da ultimo, modificata dall'art. 16, comma 1, lett. n) della Legge 28 giugno 2024, n. 90. In particolare, tale intervento ha comportato un innalzamento del trattamento sanzionatorio previsto dal comma 1 ed ha ampliato il novero delle fattispecie aggravanti declinate nel successivo comma 2, aumentandone la pena.

L'elemento soggettivo richiesto per la realizzazione del reato è il dolo generico, consistente nella volontà di porre in essere quelle condotte, con la consapevolezza dell'altruità della cosa.

Oggetto materiale della condotta sono le informazioni, dati o programmi informatici.

Si tratta di un reato di evento, per cui le espressioni distruggere, deteriorare, cancella, alterare o sopprimere devono essere interpretate come eventi capaci di incidere su «informazioni, dati o programmi informatici altrui» (si veda paragrafo §2)

A tal fine, per distruzione si intende l'annientamento totale della cosa; mentre, il deterioramento, anche parziale, si configura nel momento in cui la cosa che ne costituisce oggetto è ridotta in uno stato tale da rendere necessario, per il suo ripristino, un'attività non agevole (Cass. 20930/2012). In altri termini, si ha deterioramento di una cosa o di un bene quando la capacità della cosa a soddisfare i bisogni umani o l'idoneità di essa di rispettare la sua naturale destinazione risulta ridotta, venendone compromessa la funzionalità (Cass. Pen. 15460/2016). Si tratta, dunque, di un concetto assimilabile all'inservibilità della cosa e, dunque, l'incapacità della stessa di soddisfare, sotto il profilo funzionale, l'uso cui era destinata.

[5] Ai sensi dell'art. 10 del D..gs. n. 231/2001: *«L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

Accanto alle condotte sopradescritte, si colloca quella dell'alterazione. In particolare, per alterazione si intende una modifica strutturale del dato, programma o informazione in grado di causare un'apprezzabile perdita di funzionalità. Il reato di danneggiamento di dati informatici previsto dall'art. 635 bis cod. pen. deve ritenersi integrato anche quando la manomissione ed alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento di recupero postumo, comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro.

Più difficile è definire, invece, i confini della condotta di cancellazione e soppressione, in quando lessicalmente condividono il significato di eliminazione. Sul punto, parte della dottrina definisce la cancellazione quale aggressione fisica dei supporti in cui sono contenuti i dati, i programmi o le informazioni tale da causarne la rimozione, anche mediante l'utilizzo di operazioni come la formattazione. A livello pratico, l'operazione della cancellazione consiste nella rimozione da un certo ambiente di determinati dati, in via provvisoria attraverso lo spostamento nell'apposito cestino o in via definitiva, mediante il successivo svuotamento dello stesso (Cass. 2728/2012). Pertanto, il delitto previsto dall'art. 635-bis c.p. si intende integrato nel caso di cancellazione di dati informatici, ancorché questi possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze (Cass. Pen., Sez. V, Sentenza, 18/11/2011, n. 8555).

Quanto alla soppressione, invece, questa consiste non solo nella eliminazione definitiva di dati, programmi o informazioni, ma anche nella impossibilità del titolare di accedervi e di disporne.

Alla luce di quanto sopra rappresentato, del tutto irrilevante, ai fini penali, è dunque la possibilità per il titolare di recuperare i file eliminati.

Elemento essenziale della fattispecie criminosa è che le informazioni, i dati o i programmi informatici interessanti dalle condotte manipolative siano altrui o appartengano, in esclusiva, ad un soggetto diverso da chi pone in essere la condotta illecita. Il bene giuridico tutelato dalla norma è l'integrità e la disponibilità delle informazioni, dati o programmi informatici.

Per quanto riguarda, le circostanze aggravanti, la norma prevede al comma 2 l'innalzamento della pena della reclusione da 3 a 8 anni laddove il fatto sia commesso:

(i) 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 (art. 635 bis, comma 2, n. 1) c.p.);

(ii) mediante uso di minaccia o violenza o da parte di persona palesemente armata

la norma ne prevede 4 (cfr. commi 2 e 3). Si tratta di circostanze ad effetto speciale che consentono

che si proceda d'ufficio, ciò a differenza dell'ipotesi base del reato che, invece, è perseguibile a querela di parte.

- Esempi di condotte idonee ad integrare il reato

Un dipendente con accesso al sistema informatico altrui (cliente), altera/cancella i dati o programma con l'obiettivo di acquisire un vantaggio o interesse da parte di Laurini Officine Meccaniche S.r.L..

3.4 Art. 635- ter c.p.: «Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico»

Art. 635-ter c.p.
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. 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. 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)»

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. n. 231/2001
- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[6].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la

[6] Ai sensi dell'art. 10 del D.lgs. n. 231/2001: *«L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».

- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

- Descrizione del reato di cui all'art. 635-ter c.p.

Il reato di cui all'art. 635-ter c.p. si pone accanto alle altre ipotesi di danneggiamento previste dagli artt. 635-bis, 635-quater e 635 quinquies c.p. Si tratta di una disposizione introdotta nel codice penale dall'art. 5, comma 2, della Legge 18 marzo 2008, n. 48 e riprende la formulazione dell'abrogato art. 420 c.p. La disposizione è stata successivamente modificata dal legislatore attraverso l'art. 16, comma 1, lett. o) della legge 28 giugno 2024, n. 90 che, oltre ad aver modificato la rubrica del reato , ha integralmente sostituito il comma 2 e 3, aggravando il trattamento sanzionatorio previsto.

La norma, secondo la dottrina prevalente, è configurata come un vero e proprio delitto di attentato, per cui il danneggiamento di dati o programmi pubblici prevede il compimento di "atti diretti a" realizzare gli eventi che sono previsti dalla norma.[7], di conseguenza la tutela risulta notevolmente anticipata.

Pertanto la consumazione è anticipata già al momento della commissione del fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici, senza che sia necessaria la loro effettiva realizzazione. In altri termini, è sufficiente che la condotta posta in essere dal soggetto agente sia diretta al loro compimento. Difatti, gli atti prodromici alla realizzazione degli eventi sopradescritti si considerano oggettivamente idonei a costituire un pericolo in concreto per il bene giuridico tutelato dalla norma.

Oggetto della condotta sono i dati, le informazioni, i programmi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

Elemento soggettivo necessario affinché si realizzi il reato è il dolo generico, vale a dire, la volontà di porre in essere atti idonei e finalizzati alla realizzazione di uno degli eventi di danno tipizzati dalle norme con la consapevolezza della peculiare appartenenza di tali dati, programmi, informazioni o sistemi informatici o telematici.

Il bene giuridico tutelato dalla norma è il patrimonio, in relazioni ad informazioni, dati o programmi

[7] Diritto penale giappichelli – terza edizione pag 370

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, . Particolare attenzione ai fini della configurazione del reato dovrà essere prestata ai dati ed informazioni relative ai contributi e fondi pubblici ed alla loro rendicontazione che potrebbero essere riconducibili alla nozione di "interesse pubblico".

Per quanto riguarda le circostanze aggravanti, è intervenuto recentemente il legislatore, il quale con l'art. 16, comma 1, lett. o) della Legge 28 giugno 2024, n. 90, ha previsto un inasprimento della pena edittale (da 3 a 8 anni) in caso di: (i) commissione del fatto 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; (ii) commissione del fatto con uso di minaccia o violenza ovvero da persona palesemente armata; (iii) derivazione dal fatto della distruzione, del deterioramento, della cancellazione, dell'alterazione o della soppressione delle informazioni ovvero della sottrazione, anche mediante riproduzione o trasmissione, o dell'inaccessibilità al legittimo titolare dei dati o dei programmi informatici

Al comma 2, dell'art. 635-ter c.p., così come modificato dal citato articolo 16, si è provveduto, dunque, ad uniformare l'elencazione delle circostanze aggravanti a quelle contenute all'art. 615-ter, comma 2, c.p.

Mentre, al successivo comma 3, il legislatore ha introdotto la disciplina del concorso di circostanze prevedendo che, qualora taluna delle circostanze di cui ai nn. 1), 2) del comma 2, concorre con taluna delle circostanze di cui al n. 3), la pena della reclusione è aumentata da 4 a 12 anni.

- Esempi di condotte idonee ad integrare il reato

Un dipendente accede al sistema informatico contenente informazioni di interesse militari o relativi alla sicurezza pubblica e altera alcuni dati o sopprime alcune informazioni per consentire di aumentare o contrattualizzare la manutenzione del relativo sistema informatico in favore di Laurini Officine Meccaniche S.r.L..

3.5 Art. 635-quater c.p.: «Danneggiamento di sistemi informatici o telematici».

Art. 635-quater c.p.

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

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. n. 231/2001
- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[8].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.
- Descrizione del reato di cui all'art. 635 quater c.p.

La fattispecie delittuosa descritta dall'art. 635 quater c.p. è stata introdotta dall'art. 5, comma 2, della Legge 48/2008. Insieme all'art. 635-bis c.p. la norma si colloca nel Titolo XIII, Capo I, dedicato ai «delitti contro il patrimonio mediante violenza alle cose o alle persone». Con la legge 28 giugno 2024, n. 90 il legislatore è intervenuto aumentando il trattamento sanzionatorio e sostituendo integralmente le circostanze aggravanti ad effetto speciale.

Da un lato, si richiedono le condotte di cui all'art. 635 bis (a cui si rimanda) alle quali si

[8] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

aggiungono quelle di introduzione o trasmissione di dati o programmi e, dall'altro ulteriori requisiti di cui alla norma in esame . L'art. 635-quater c.p. punisce chiunque mediante le condotte di cui all'art. 635-bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili i sistemi informatici o telematici altrui e ne ostacola gravemente il funzionamento.

Con tale norma, dunque, il legislatore ha inteso prestare particolare tutela a quelle condotte che si risolvono nella diffusione di ogni possibile tipologia di virus informatico. Si considera, dunque, penalmente rilevante l'ipotesi di danneggiamento logico, posto in essere a distanza, attraverso l'introduzione o la trasmissione di virus o malware.

Oggetto della condotta sono i sistemi informatici o telematici. A livello pratico, ai fini della configurabilità del reato di cui all'art. 635-quater c.p. oggetto materiale della condotta di danneggiamento deve intendersi un complesso di dispositivi interconnessi o collegati con unità periferiche o dispositivi esterni (componenti "hardware") mediante l'installazione di un "software" contenente le istruzioni e le procedure che consentono il funzionamento delle apparecchiature e l'esecuzione delle attività per le quali sono state programmate (Cass. pen., Sez. V, Sentenza, 08/01/2020, n. 4470). In buona sostanza la giurisprudenza ha ritenuto che, per evitare vuoti di tutela e per ampliare la sfera di protezione offerta ai sistemi informatici e telematici è opportuno accogliere la nozione più ampia possibile di computer o di unità di elaborazione di informazioni. Inoltre, la stessa giurisprudenza pone l'accento sulla necessità di tenere distinto "il contenitore" (sistematico informatico) rispetto "al contenuto", intendendosi come tale seconda accezione "il dato informatico" (Cass. pen., Sez. V, Sentenza, 08/01/2020, n. 4470). La differenza è ben presente negli artt. 635-bis, 635-ter, 635 quater e 635 quinquies che distinguono il danneggiamento dell'integrità dei dati (oggetto di tutela da parte dei primi due articoli) dal danneggiamento dell'integrità di un sistema (oggetto di tutela ad opera delle due successive disposizioni). Il concetto di sistema informatico è stato interpretato dalla giurisprudenza in maniera estensiva al punto di ricondurvi anche telecamere esterne adibita a videosorveglianza di aree di accesso. In buona sostanza si è ritenuto che il sistema di videosorveglianza presenta i requisiti di un "sistema informatico" inteso come complesso di apparecchiature elettroniche, interconnesse tra loro, che si avvalgono di tecnologie informatiche e che svolgono attività di registrazione o memorizzazione di dati su supporti adeguati.

Per quanto riguarda le circostanze aggravanti, la norma prevede – analogamente a quanto previsto dall'art. 635-bis c.p.- al comma 2 un aumento della pena (da 3 a 8 anni) laddove il fatto sia commesso:

(i) 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;
(ii) mediante uso di minaccia o violenza o da parte di persona palesemente armata

- Esempi di condotte idonee ad integrare il reato

Un dipendente con il consenso della società, danneggia un sistema informatico, attraverso l'introduzione di un virus, di una società concorrente al fine di impedirgli la realizzazione di attività similari a quelle di Laurini Officine Meccaniche S.r.L..

3.6 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».

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
«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».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: sino a 400 quote (sino a 619.600)[9].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive « b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

- Descrizione del reato di cui all'art. 635-quater.1 c.p.

La fattispecie penale in commento è stata introdotta con l'art. 16, comma 1 lett. q) della Legge 28 giugno 2024, n. 90. La norma riproduce al comma 1 la formulazione del previgente art. 615-quinquies c.p. (di cui contestualmente è stata disposta l'abrogazione con l'art.16 comma 1 lett. d). In particolare, viene punito chiunque 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, per danneggiare illecitamente ovvero favorire l'interruzione o alternazione di un sistema informatico o telematico ovvero le informazioni, i dati o i programmi ivi contenuti.

Oggetto della condotta sono, dunque, i sistemi informatici e telematici nonché i dati, le informazioni e i programmi in essi contenuti. In merito ai sistemi informatici è necessario che l'azione illecita riguardi un "sistema informatico", il quale presuppone l'attitudine della macchina (hardware) ad organizzare ed elaborare dati, in base ad un programma (software), per il perseguimento di finalità eterogenee. Ne consegue che, al fine di ritenere sussistente il reato, alla funzione di registrazione e di memorizzazione dei dati, anche elettronica, deve affiancarsi l'attività di elaborazione e di organizzazione dei dati medesimi (Cass. Pen. Sez. V, 16/04/2018, n. 40470).

Per quanto riguarda i termini "consegna" si intende la dazione materiale dei dispostivi su cui sono istallati i programmi nocivi; mentre con il termine "diffusione" ci si riferisce alla divulgazione di malware ad una platea indeterminata di persone attraverso l'utilizzo della rete telematica. Si potrebbe trattare del caso in cui il programma infetto sia offerto in vendita, attraverso la sua

[9] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

incorporazione in un adeguato supporto informatico(es. un nastro o un supporto magnetico) oppure sia reso accessibile agli utenti di un sistema o di una rete informatica, perché memorizzato in un archivio elettronico, dal quale sia consentito riprodurlo; mentre, con il termine "comunicazione", ci si riferisce alla divulgazione di virus attraverso la rete telematica ma destinata a persone determinate. Opportunamente il legislatore ha inserito, con riferimento alla messa a disposizione, l'espressione "in altro modo" poiché così si consente l'incriminazione di comportamenti non ancora descrivibili nel loro contenuto essenziale, ma resi possibili dalla rapida evoluzione tecnologica. La punibilità prescinde dal danneggiamento e quindi, si realizza un'anticipazione di tutela, tipica dei reati di pericolo astratto. In altri termini il soggetto, che abbia lo scopo o l'intenzione di danneggiare un sistema informatico altrui, incorre nel reato anche se non è in grado di arrecare alcun tipo di danno perché ad esempio il virus è inidoneo o perché l'agente decida di non utilizzarlo, Tale anticipazione di tutela è da ravvisarsi probabilmente in ragione del fatto che il danneggiamento del software o di dati conservati in un sistema informatico può avere effetti devastanti per il sistema sociale che si affida sempre di più al controllo dei sistemi informatizzati[10].

A delimitarne l'ambito di applicazione è l'elemento soggettivo che, comunque, richiede la sussistenza del dolo specifico ossia che la condotta sia univocamente indirizzata "allo scopo di danneggiare illecitamente ovvero favorire l'interruzione o alterare il funzionamento ai beni oggetto della condotta"(Tribunale Bologna, 22/12/2005, n. 1823). Infatti secondo la giurisprudenza (riferita al testo previgente dell'art. 615 quinquies c.p.) si tratta di reato di pericolo (Cass. Pen. Sez. V, 16/04/2018, n. 40470) e per sistema informatico si deve intendere, in senso ampio, ossia una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche (Cass. Sez. Unit. N.17325/2015), più in particolare, viene in rilievo, per definire la nozione di sistema informatico l'attitudine della macchina (hardware) ad organizzare ed elaborare dati, in base ad un programma (software), per il perseguimento di finalità eterogenee.

Ai fini della sussistenza del reato sono ricompresi sia i dispositivi hardware (ad es. chiavette USB) sia soprattutto i software, con particolare attenzione ai malware (comunemente definiti virus).Il bene giuridico tutelato è la riservatezza e sicurezza informatica. Con riferimento alle circostanze aggravanti, la pena edittale viene aumentata laddove ricorrano taluna delle circostanze di cui all'art. 615-ter, comma 2, n. 1) e comma 3 c.p..

[10] Corte suprema di Cassazione – ufficio Massimario e del ruolo – servizio penale Relazione su novità normativa n.20/2020

- Esempi di condotte idonee ad integrare il reato
- Un soggetto della società crea/detiene un programma (c.d. virus) destinato a danneggiare o interrompere il sistema informatico o telematico di una società concorrente (o per danneggiare un programma dell'ente allo scopo di cancellare i dati in esso contenuti per eliminarne le tracce di eventuale attività illecita) ottenendo un vantaggio/interesse dall'attività illecita.

3.7 Art. 635-quinquies c.p.: «Danneggiamento di sistemi informatici o telematici di pubblico interesse».

Art. 635-quinquies c.p.
Danneggiamento di sistemi informatici o telematici di pubblico interesse
« 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)».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. n. 231/2001

- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[11].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

- Descrizione del reato di cui all'art. 635-quinquies c.p.

Per orientarsi nell'esame dei reati presupposto occorre rilevare che il legislatore ha previsto ben quattro fattispecie di danneggiamento informatico/telematico: due relativi a dati e programmi, dovendosi poi distinguere ulteriormente tra fattispecie che riguarda dati e programmi "privati" (art.635 bis) e quella che invece ha ad oggetto dati e programmi a carattere pubblico (art. 635 ter); due fattispecie relative a sistemi informatici/telematici, dovendosi ulteriormente distinguere ancora una volta tra quella "privatistica" (art. 635 quater) e quella "pubblicistica (art. 635 quinquies).

L'articolo 635 quinquies c.p. è stato integralmente sostituito dall'art. 16, comma 1, lett. r) della Legge 28 giugno 2024, n. 90. Con il menzionato intervento legislativo, il legislatore ha, in primo luogo, aggravato il trattamento sanzionatorio e, in secondo luogo, è intervenuto modificando l'oggetto del reato sostituendo la nozione di servizi informatici o telematici di pubblica utilità con quella di servizi informatici o telematici di pubblico interesse.

In particolare, il vigente articolo punisce chiunque, mediante le condotte di cui all'art. 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.

Si tratta, secondo la dottrina prevalente, di un vero e proprio delitto di attentato, in quanto la consumazione dello stesso è anticipata al momento della commissione di un fatto «diretto a», senza che sia necessario che le ipotesi descritte dalla norma si realizzino compiutamente.

A tal fine, la norma si allinea, in merito all'enunciazione dei verbi «distruggere, danneggiare, rendere inservibile, ostacolarne gravemente il funzionamento» a quanto previsto dall'art. 635 quater c.p.

[11] Ai sensi dell'art. 10 del D.lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

Tuttavia, residuano alcuni dubbi sull'esatta definizione del termine «ostacolare gravemente il funzionamento di sistema informatico». Quest'ultima, difatti, costituisce una condotta non sempre facilmente apprezzabile, in quanto è richiesta una valutazione prognostica degli esiti di una condotta che non ha prodotto in toto gli effetti dannosi cui era indirizzata, almeno con riguardo alla fattispecie di pericolo della norma in esame, laddove viene punita quella sostanziatasi nella commissione di un fatto diretto a ostacolare gravemente il funzionamento del sistema informatico.
Oggetto della condotta sono i sistemi informatici e telematici di pubblico interesse. Per l'individuazione della nozione "di pubblico interesse" è utile rinviare alle argomentazioni indicate nella parte speciale relativa ai reati contro la pubblica amministrazione a cui si rimanda.

Il bene giuridico tutelato dalla norma è l'integrità e la disponibilità delle programmi informatici o telematici di pubblico interesse.
Per quanto riguarda le circostanze aggravanti previste dalla norma, il comma 2 dell'art. 635-quinquies c.p. richiama le ipotesi previste negli articoli precedentemente descritte a cui si rimanda.
In particolare, è previsto un innalzamento della pena edittale (da 3 a 8 anni) in caso di:
1) commissione del fatto 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) commissione del fatto con uso di minaccia o violenza ovvero da persona palesemente armata;
3) derivazione dal fatto della distruzione, del deterioramento, della cancellazione, dell'alterazione o della soppressione delle informazioni, dei dati o dei programmi informatici.

- Esempi di condotte idonee ad integrare il reato

Un soggetto introduce un programma (c.d. virus) diretto a danneggiare o distruggere o ostacolare gravemente o rendere inservibile il funzionamento di un sistema informatico o telematico di pubblico interesse allo scopo di acquisire una commessa per la manutenzione del sistema o approfittare del mancato funzionamento per acquisire altro vantaggio o interesse.

3.8 Art. 629, comma 3, c.p.: «Estorsione»

Art. 629, comma 3, c.p.

Estorsione
«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».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: da trecento a ottocento quote (da 464.700 euro a 1.239.200. euro)[12].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive, per una durata non inferiore a due anni: «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

- Descrizione del reato di cui all'art. 629, comma 3, c.p.

Il comma 3 dell'art. 629 c.p. è una nuova fattispecie inserita ad opera dell'art. 16, comma 1, lett. m), n. 2 l. n.90/2024. La nuova fattispecie punisce chi, mediante le condotte di cui artt. 615-ter (accesso abusivo ad un sistema informatico o telematico), 617-quater (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche), art. 617 sexies (falsificazione,

[12] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche), art. 635.bis (danneggiamento di informazioni, dati e programmi informatici), 635-quater (danneggiamento di sistemi informatici o telematici) e 635-quinquies (danneggiamento di sistemi informatici o telematici di pubblica utilità) con la minaccia di compierle, costringe taluno a fare o omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno. Da un lato, sembra trattarsi delle fattispecie indicate nei rispettivi articoli (tutti reati informatici) con l'aggiunta di un frammento costrittivo. Per la definizione e individuazione delle condotte si rimanda agli articolo indicati nella norma e alla loro descrizione nella presente parte speciale del Modello. Occorre rilevare che dalla condotta deve derivare a sé o ad altri un ingiusto profitto con altrui danno. Come si può notare dal dato normativo si tratta di un reato plurioffensivo il legislatore ha inteso proteggere sia il bene della sicurezza informatica sia il patrimonio della persona offesa, tramite l'irrogazione di pene molto elevate. La normativa ha inteso intervenire in maniera decisa sulla c.d. Cyber extortion che si propone di bloccare o limitare le funzioni di un dispositivo.

Occorre valutare con attenzione, nel caso concreto, se la semplice corresponsione della somma di un eventuale "ricatto" può dar luogo ad un illecito da reato presupposto, in quanto potrebbe costituire un interesse/vantaggio dell'ente ad avere il bene sottratto o bloccato il prima possibile, oppure che l'eventuale pagamento avvenga con indebito utilizzo di provvista sociale, o non contabilmente tracciata.

Esempi di condotte idonee ad integrare il reato

Preliminarmente si osserva che, pur ritenendo in astratto realizzabile la condotta, appare difficile individuare un caso concreto di un attività estorsiva che sia a vantaggio dell'ente. A mero titolo esemplificativo: Un dipendente attraverso un programma (virus) accede al sistema informatico di altra società concorrente costringendo la stessa ad omettere lo svolgimento di alcune attività, con la minaccia di bloccare l'intero sistema informatico e telematico, chiedendo un corrispettivo, e comunque con vantaggio o interesse dell'ente.

Oppure un'attività estorsiva posta in essere a vantaggio dell'ente

3.9 Art. 491 bis c.p.: «Documenti informatici»

Art. 491-bis c.p.

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.».

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: sino a 400 quote (sino a 619.600)[13].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive « c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

- Descrizione del reato di cui all'art. 491 bis c.p.

L'art. 491 bis è stato introdotto con la Legge 23 dicembre 1993, n. 547 (art.3) allo scopo di estendere la tutela ai falsi che hanno ad oggetto documenti informatici. Si tratta di documenti che presentano caratteristiche del tutto particolari e non facilmente riconducibili alle fattispecie previste in materia di falso, essendo quest'ultime concepite unicamente per i documenti cartacei. In tal modo, il legislatore ha inteso equiparare il documento informatico agli atti pubblici e alle scritture private, con il duplice obiettivo di «non mutare la struttura delle fattispecie in funzione della sola diversità dell'oggetto materiale» e di «sottoporre ad identico trattamento sanzionatorio fatti criminosi che non si differenziano sul piano dell'oggettività giuridica ovvero della natura dell'interesse violato» (cfr. Relazione al d.d.l. n. 2773).

La disposizione è stata successivamente modificata ad opera dell'art. 3, L. 18.3.2008, n. 48, di

[13] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

«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» (c.d. Convenzione Cybercrime). In tale sede il legislatore è intervenuto aggiungendo il termine "avente efficacia probatoria" ed eliminando la controversa definizione di documento informativo contenuta nel secondo periodo del primo comma dell'articolo.

Da ultimo, con il Decreto legislativo 15 gennaio 2016, n. 7, è stato eliminato il riferimento ai documenti informatici privati e alle disposizioni concernenti le scritture private, a seguito dell'abrogazione del reato di falso in scrittura privata di cui all' art. 485 c.p.

Con i citati interventi normativi si è inteso introdurre nel sistema penale la fattispecie del falso informatico, vale a dire la falsificazione di documenti informatici. La ragione di tale previsione normativa va individuata nella tutela della fede pubblica attraverso la salvaguardia dei documento informatico nella sua valenza probatoria. La lesione o la messa in pericolo del bene tutelato, infatti, si realizza solo quando la falsificazione introduce falsamente e fa venir meno la prova in ordine a un dato o informazione contenuto nel documento. La norma non contiene una definizione di documento informatico, ma essa può facilmente desumersi dall'art.1 lett. p) e successivi d.lgs. 7 marzo 2005 n.2 (codice amministrazione digitale) secondo cui deve intendersi per documento informatico "la rappresentazione informatica di atti, fatti o dati giuridici rilevanti". Pertanto, come è stato rilevato dalla giurisprudenza, l'art. 491 bis c.p. attribuisce la natura di documento informatico a qualsiasi specie di supporto, che contenga dati, informazioni e relativi specifici programmi di elaborazione. Il documento informatico, quindi, costituisce nient'altro che un documento codificato nel quale la rappresentazione dell'informazione, dato o programma, può essere letto, La rilevanza penale della falsificazione del documento informatico è subordinata alla funzione cui è destinato il documento stesso o, per meglio dire, i dati, le informazioni o i programmi in esso contenuti, essendo punita solo la falsificazione di quei documenti informatici che abbiano una funzione probatoria(Cass. N. 34479/2021 Sez. 5). Devono essere considerati atti pubblici dotati di efficacia probatoria anche gli atti cosiddetti interni, ovvero destinati ad inserirsi nel procedimento amministrativo, offrendo un contributo di conoscenza o di valutazione ,nonché quelli che si collocano nel contesto di una complessa sequela procedimentale – conforme o meno allo schema tipico – ponendosi come necessario presupposto dei momenti procedurali successivi. Occorre rilevare che possono sussistere delle ipotesi di reato di falso ideologico commesso dal privato su documento informatico pubblico nonché ipotesi di concorso nel reato commesso dal dipendente pubblico.

Elemento soggettivo necessario per integrare il reato è il dolo generico, non essendo necessaria né

la volontà di procurare a sé o ad altri un vantaggio, né di cagionare ad altri un danno, essendo sufficiente la volontà e la consapevolezza dell'agente di porre in essere la condotta indiscriminata.

- Esempi di condotte idonee ad integrare il reato

Un soggetto della società in concorso con un dipendente pubblico, falsifica un documento informatico pubblico in cui si attesta falsamente delle caratteristiche di Laurini Officine Meccaniche S.r.L..al fine della erogazione di finanziamenti pubblici o concessione di vantaggi fiscali.

3.10. Art 617 quater C.P. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

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; 3) ((NUMERO ABROGATO DALLA L. 28 GIUGNO 2024, N. 90))".

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[14].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.
- Descrizione del reato di cui all'art. 617 quater c.p.

L'articolo è stato introdotto dalla L.547/1993(art.6) e , da ultimo, è stato modificato dalla L. 90/2024 (dall'art. 16 lett. f), in particolare, il quarto comma, intervenendo sulle aggravanti: aumentando le pene e introducendo anche nuove aggravanti e abrogando il comma 4 n.3. La norma in oggetto è stata introdotta, secondo la dottrina maggioritaria, per garantire la segretezza, la libertà e riservatezza delle comunicazioni relative ai sistemi informatici o telematici o intercorrenti tra più sistemi. In particolare:

- la fraudolenta intercettazione del contenuto delle comunicazioni informatiche o telematiche violi la segretezza del contenuto delle comunicazioni, di cui è punita la mera apprensione;
- le condotte di interruzione e impedimento violano la libertà e la regolarità delle comunicazioni;
- le condotte di rivelazione, di cui al primo capoverso, offende, invece, il differente bene giuridico della riservatezza della comunicazione. Viene sanzionata, infatti, non già la fraudolenta intercettazione, bensì la indiscriminata divulgazione al pubblico del contenuto di una comunicazione.

Si tratta di un reato comune che, quindi, può essere commesso da chiunque. Particolari qualifiche soggettive dell'autore sono previste a titolo di aggravanti.

I soggetti passivi (o la persona offesa - ossia coloro che sono titolari del bene protetto dalla norma) sono coloro tra i quali intercorre la comunicazione attraverso lo strumento informatico o telematico, ossia i mittenti e destinatari sostanziali del contenuto della comunicazione in transito. Non subiscono di per sé alcuna offesa alla propria riservatezza, invece, né gli operatori informatici che abbiano materialmente introdotto i dati altrui nel sistema, né i titolari dei sistemi informatici

[14] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

utilizzati dai dialoganti per effettuare la comunicazione.

In merito all'oggetto materiale del reato, le condotte sanzionate incidono sulle comunicazioni relative ad un sistema informatico o telematico, o intercorrente tra più sistemi, nel momento dinamico della loro trasmissione. Per la definizione di sistema informatico o telematico si rinvia al paragrafo relativo all'inquadramento generale. In merito al sistema informatico si osserva che anche il personal computer, essendo dotato di periferiche e software complessi, è considerato un sistema informatico a sé stante. Si evidenzia che la Cassazione (Sezioni Unite 23.2.2000) ha incidentalmente ravvisato la qualità di sistema telematico nel sistema telefonico cellulare nonché nella telefonia fissa. Non è agevole, anche per i continui sviluppi del settore, percepire in concreto, la netta demarcazione tra comunicazioni relative a sistemi informatici, telematici o intercorrenti tra più sistemi, ma occorre anche rilevare che la questione è meramente classificatoria non comportando l'appartenenza di una comunicazione all'una o all'altra categoria differenze di disciplina o tutela. Può essere utile comprendere cosa debba intendersi per "comunicazioni tra più sistemi" ossia ciò che comporta il trasferimento di dati e informazioni da un sistema all'altro, attraverso un collegamento di natura telematica. Sono comunicazioni intercorrenti tra più sistemi la posta elettronica (e-mail), indipendentemente dal numero dei destinatari, i messaggi inviati ad un newsgroup per partecipare ad una determinata conferenza telematica, la videoconferenza (NetMeeting), tramite cui è possibile istaurare una comunicazione simultanea e condividere innumerevoli dati e documenti informatici tra più soggetti, ciascuno in contatto attraverso il proprio personal computer.

Il comma 1 prevede tre distinte condotte: la intercettazione, la interruzione e l'impedimento di comunicazioni:

1) la intercettazione è quella speciale ipotesi della presa di cognizione che si realizza attraverso la particolare modalità della intromissione nella comunicazione in corso tra terzi. La intercettazione deve avere ad oggetto il contenuto di una comunicazione informatica o telematica in atto, nel momento dinamico della sua trasmissione, in quanto la tutela della situazione statica (es. contenuto di un floppy disk o di un cd rom) è garantita da un'altra norma (es. l'art. 616 comma 1 e 4 c.p.). A titolo di esempio, nelle modalità di intercettazione può farsi rientrare la lettura dei messaggi di posta elettronica (email) diretti ad altri soggetti, una volta individuata (attraverso un software illecito la cui mera detenzione è sanzionata dall'art. 615 quater) la parola chiave ai accesso (password) alla altrui casella di posta elettronica. Integra, un'ipotesi di intercettazione di comunicazione relativa ad un sistema telematico l'abusiva ricezione di trasmissioni di emittenti televisive satellitari, attraverso la clonazione dei codici di decodificazione del messaggio televisivo.

La intercettazione deve essere caratterizzata, come previsto dal comma 1, da una modalità fraudolenta di realizzazione. Essa deve avvenire con strumenti idonei a celare ai comunicanti – o al sistema informatico stesso, che sia programmato per consentire o negare autonomamente l'accesso – l'abusiva intromissione del soggetto agente. E', altresì, considerata fraudolenta l'intrusione idonea a trarre in inganno i comunicanti, e ugualmente il sistema informatico stesso, sulla sua fonte e sulle sue modalità di realizzazione. Può essere considerata fraudolenta – come specificato in giurisprudenza- anche l'intromissione effettuata dall'amministratore di sistema eludendo, attraverso le password e gli altri strumenti d'accesso nella propria disponibilità in ragione delle funzioni, gli sbarramenti posti all'accesso di estranei alle comunicazioni.

2) le condotte di interruzione e impedimento consistono nel compimento di atti tecnicamente idonei, rispettivamente, a far cessare una comunicazione in corso e a impedire che una nuova abbia inizio. In questo caso si ritiene , secondo il tenore della norma, non sia richiesta una modalità fraudolenta di realizzazione. Può ricondursi alla norma in esame la condotta di chi utilizzi particolari software in grado di accedere all'altrui computer durante la navigazione in internet, provocando l'immediato spegnimento del modem e dunque la disconnessione dell'utente dalla rete, con la conseguente interruzione di tutte le comunicazioni che fossero in corso.

Per la realizzazione delle condotte è richiesto il dolo generico.

La norma in oggetto prevede al comma 4 delle circostanze aggravanti per la cui individuazione si rinvia all'art. 615 ter e per la nozione di pubblico ufficiale o incaricato di pubblico servizio si rinvia alla parte speciale del Modello dei reati contro la P.A.

Occorre solo rilevare che l'operatore di sistema è, indipendente dalla struttura pubblica o privata, il soggetto che controlla il processo di ricezione, elaborazione e diffusione dei dati, potendo influire sulla loro destinazione o integrità. La qualifica di operatore di sistema non deve essere confusa con quella assai più specifica di "tecnico di sistema" o "tecnico programmatore", che presuppone particolari livelli di abilità tecnica, non richiesti dalla norma penale per l'operatività della circostanza aggravante.

- Esempi di condotte idonee ad integrare il reato

Un soggetto di Laurini Officine Meccaniche S.r.L., attraverso un software illecito, individua la password di accesso alla casella di posta elettronica di un soggetto dipendente di una società concorrente. In questo modo, attraverso la lettura dei messaggi di posta elettronica (email) diretto ad altro soggetto, riesce a acquisire informazioni commerciali che gli consentono alla società di aggiudicarsi una gara d'appalto, avendo presentato un offerta inferiore rispetto alla società

concorrente.

3.11 Art. 617 quinquies C.P. 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.
Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche
"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. ((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)). ((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)) .."

Sanzione per l'ente ai sensi dell'art. 24-bis del D.lgs. n. 231/2001

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: da duecento a settecento quote (da 309.800 euro a 1.084.300 euro)[15].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione

[15] Ai sensi dell'art. 10 del D.lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

dell'illecito; e) il divieto di pubblicizzare beni o servizi».

- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.
- Descrizione del reato di cui all'art. 617 quinquies c.p.

La norma è stata introdotto dalla L. 547/93 (art.6) e modificata, da ultimo, dalla L. 90/2024 e, in particolare, in relazione alle circostanze aggravanti.

La norma offre una tutela anticipata al bene giuridico della segretezza e libertà delle comunicazioni informatiche o telematiche. Infatti la norma incrimina le più gravi tra le condotte prodromiche (si deve intendere un fatto che precede e annuncia il manifestarsi di un altro fenomeno) alla realizzazione dei fatti di intercettazione, impedimento o interruzione di cui all'art. 617 quater c.p. Si tratta di un reato di pericolo concreto, che richiede l'accertamento giudiziale dell'effettiva potenzialità lesiva del materiale istallato. La condotta consiste nel procurarsi, detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri o installare 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. Per le relative nozioni si rinvia all'art 617 quater. L'integrazione del reato è stata ravvisata nell'istallazione, all'interno di un bancomat, di uno scanner per bande magnetiche con batteria autonoma di alimentazione e microchip, idoneo a leggere, raccogliere e memorizzare le relative comunicazioni di scambio di dati (Cass. N.3236/2020 Sez. V).

La L. 238/21 ha modificato il dolo richiesto dalla norma incriminatrice che, con la nuova formulazione, è il dolo specifico consistente nel fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedirle o interromperle.

Per le circostanze aggravanti si rinvia all'art. 617 quater c.p.

- Esempi di condotte idonee ad integrare il reato

Si rinvia agli esempi di cui all'art. 617 quater tenendo conto che sono punite le condotte prodromiche alla realizzazione di cui all'art.617 quater. Es. un soggetto di Laurini Officine Meccaniche S.r.L. detiene, diffonde un sistema informatico, allo scopo di intercettare comunicazioni intercorrenti tra più sistemi, a vantaggio e nell'interesse dell'ente.

3.12 Art. 640 quinquies C.P. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

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)"

- Sanzione per l'ente ai sensi degli artt. 9, 18, 19 e 24-bis del D.lgs. 231/2001
- Sanzione pecuniaria: sino a 400 quote (sino a 619.600)[16].
- sanzione interdittiva: nei confronti dell'ente, in caso di condanna, ai sensi dell'art.24 bis e 9 si applicano le seguenti sanzioni interdittive « c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi».
- Confisca: nei confronti dell'ente è sempre disposta, in caso di condanna, la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 D.lgs. 231/01.

- Descrizione del reato di cui all'art. 640 quinquies c.p.

Occorre premettere che la norma di cui all'art.24 bis d.lgs. 231/01 comma 3) con l'inciso "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…" intende escludere dalla fattispecie di cui all'art. 640 quinquies quelle condotte di frode informatica in danno dello stato o di altro ente pubblico indicate nell'art. 24 del D.lgs. 231/01. Infatti l'art. 24 del Decreto ricomprende tra i reati presupposto anche la Frode informatica in danno dello stato o di altro ente pubblico o dell'Unione Europea; di conseguenza per tali condotte si applica la sanzione di cui all'art. 24 D.lgs. 231/01.

[16] Ai sensi dell'art. 10 del D.Lgs. n. 231/2001: «*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*». Pertanto, l'importo della singola quota va da un minimo di euro 258 a un massimo di euro 1549. A tal proposito, si segnala che la sanzione pecuniaria è calcolata tenendo conto della quota massima.

3.13 Art.1 comma 11 decreto legge 105/2019 perimetro di sicurezza nazionale cibernetica
Inquadramento generale

In considerazione dei servizi e delle attività svolte dall'azienda e per comprendere le condotte da prevenire è necessaria una premessa che inquadri il contesto normativo relativo al perimetro di sicurezza nazionale cibernetica e il Decreto cybersecurity e i suoi collegamenti con il D.lgs. 231/01.
La legge 105/2019 c.d. " decreto cybersecurity" dal titolo "disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica" nasce principalmente da una duplice dall'esigenza. In primo luogo, come indicato in premessa dalla stessa norma, dalla necessità e urgenza, di disporre, per le finalità di sicurezza nazionale, di un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti, in linea con le più elevate ed aggiornate misure di sicurezza adottate a livello internazionale. Ma anche dalla necessità di prevedere, il raccordo con le disposizioni in materia di valutazione della presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G e dei dati che vi transitano ai sensi dell'art. 1 bis decreto legge 21/12. Si elencano i punti principali del Decreto.
Con il decreto viene istituito il "perimetro di sicurezza nazionale cibernetica". Sostanzialmente si tratta dell'insieme di quelle amministrazioni pubbliche, enti, operatori pubblici e privati aventi una sede sul territorio nazionale, il cui ruolo risulta strettamente correlato all'esercizio di una funzione essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello stato. In altri termini, si tratta di quei soggetti per cui il malfunzionamento, interruzione od utilizzo improprio di reti e sistemi informativi può causare un pregiudizio per la sicurezza nazionale.
I soggetti rientranti nel perimetro saranno tenuti al rispetto di misure ed obblighi specifici, quali la predisposizione di un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, l'obbligo di notifica degli incidenti al CSIRT (gruppo d'intervento per la sicurezza informatica),ecc.
In merito all'individuazione concreta del perimetro di sicurezza nazionale e per quanto attiene la definizione dei profili concreti degli obblighi citati il decreto demandava ad un momento successivo di cui si dirà di seguito.
In merito al sistema sanzionatorio la struttura della norma segue una duplice corsia: sanzioni

amministrative e sanzioni penali. In merito alle sanzioni amministrative si rinvia al testo della norma. Per quanto attiene alle sanzioni penali il decreto propone nuove ipotesi di reato.

La L. 105/2019, infatti, ha introdotto un ulteriore tassello di collegamento tra la normativa sulla cybersecurity e il D.lgs. 231/01. In particolare Il decreto Legge 105/2019 all'art.1 comma 11 bis ha previsto che "all'art.24 bis comma 3 del D.lgs. 231/01, sono inserite le seguenti "e dei delitti di cui all'art.1 comma 11 del decreto-legge 21 settembre 2019n.105."

Pertanto, il comma 3 dell'art. 24 bis del D.lgs. 231/01, a seguito dell'intervento legislativo, prevede l'adozione di sanzioni amministrative sino a 400 quote per i delitti di cui agli artt. 491 bis e 640 quinquies c.p., "e dei delitti di cui all'art.1 comma 11 del decreto legge 21 settembre 2019 n.105".

Il delitto di cui all'art.1 comma 11 D.L 105/2029 è un reato di nuovo conio avente ad oggetto l'ostacolo o condizionamento dei procedimenti di predisposizione ed aggiornamento degli elenchi di rete, sistemi informativi e servizi informatici inclusi nel perimetro di sicurezza nazionale, della comunicazione al CVCN (centro di valutazione e certificazione nazionale – istituito presso il ministero dello sviluppo economico) dell'affidamento di forniture di beni, sistemi e servizi ICT (information and Communication Tecnologies) nonché delle relative attività ispettive e di vigilanza.

ART.1 DECRETO LEGGE 105/2019
Perimetro di sicurezza nazionale cibernetica

*** * * * ***

Adempimenti alle linee guida sui reati informatici in relazione all'aggiornamento per adeguamento alle modifiche apportate dalla L.90/24 e dal perimetro di sicurezza nazionale.

Tale attività è necessaria e importante tenuto conto che la Cassazione ha ritenuto che se nel modello ci sono tutti gli adempimenti previsti dalle linee guida, il Giudice per negare l'idoneità del modello dovrà adottare una motivazione rafforzata. Certamente non è una certezza di idoneità (dovendo essere il modello costruito su misura) ma un supporto.

Indicazioni:

- adozione di procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche;
- procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro (art. 615 ter);
- aggiornamento regolare dei sistemi informativi in uso (art. 615 ter);
- modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto (art. 615 ter);
- procedura per il controllo degli accessi (art. 615 ter);
- tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali (art. art. 615 ter);
- definizione e attuazione di un processo di autorizzazione della direzione per le strutture di elaborazione delle informazioni (art. 615 ter).

<u>Art. 617 quater e art. 617 quinques</u>

- definizione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- elaborazione di procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione;
- utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse;
- allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione;
- definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato;
- previsione di controlli su: - rete aziendale e informazioni che vi transitano - instradamento (routing) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza; - installazione di software sui sistemi operativi; - predisposizione di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.

<u>Art. 615 quinques c.p. - art. 635 bis c.p. - art. 635 quater c.p.</u>

- Formalizzazione di regole al fine di garantire un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- procedure per l'etichettatura e il trattamento delle informazioni in base allo schema di classificazione adottato dall'ente;
- controlli di individuazione, prevenzione e ripristino al fine di proteggere da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema Presenza di misure per un'adeguata protezione delle apparecchiature incustodite;
- previsione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business;
- procedure di controllo della installazione di software sui sistemi operativi;
- procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.

Art. 635 ter c.p. - Art. 635 quinques c.p.

- Formalizzazione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione;
- controlli di individuazione, prevenzione e ripristino al fine di proteggere da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema. Procedure di controllo della installazione di software sui sistemi operativi.

Roma, 26.06.2025

SCIULLO FEDERICO
2025.06.26 19:22:35
Avv. Federico Sciullo
CN=SCIULLO FEDERICO
C=IT
O=ORDINE AVVOCATI ROMA
2.5.4.97=VATIT-80230130587
RSA/2048 bits