PARTE SPECIALE K

REATI IN TEMA DI CRIMINALITÀ INFORMATICA E DI TRATTAMENTO ILLECITO DI DATI

Parte speciale K

REATI IN TEMA DI CRIMINALITÀ INFORMATICA E DI TRATTAMENTO ILLECITO DI DATI

La “Parte speciale K” è dedicata alla trattazione dei reati in materia di criminalità informatica e di trattamento illecito di dati così come individuati nell’art. 24 *bis* D.Lgs. n. 231 del 2001.

Di seguito viene riportato l’elenco delle fattispecie criminose prese in considerazione dalle suddette disposizioni, le modalità attraverso le quali queste fattispecie criminose possono essere compiute nonché le “macro aree” sensibili, i ruoli aziendali coinvolti e i “protocolli di prevenzione” attuati all’interno della Società. Infine, vengono riportati anche i c.d. “processi strumentali”, i “principi generali di comportamento” e i “compiti dell’Organismo di Vigilanza”.

Ai fini del presente documento si considera Protocollo di prevenzione “una specifica connotazione di una variabile organizzativa, secondo cui è progettata l’attività sensibile o che agisce sugli output della stessa, con l’effetto di azzerare o ridurre la probabilità o la frequenza con cui può essere compiuto un reato del catalogo di cui al D.Lgs. n. 231 del 2001”.

a) Art. 491-bis c.p.: Falsità in un documento informatico pubblico o avente efficacia probatoria

Testo della norma del Codice Penale ([1])

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.

Descrizione

La norma attribuisce la natura di documento informatico a qualsiasi specie di supporto (disco fisso, floppy disk, nastro, CD, disco ottico, …) che contenga dati, informazioni e relativi specifici programmi di elaborazione. Esso non è nient’altro che un documento codificato nel quale la rappresentazione

([1]) Così come modificato dal D.lgs. 15 gennaio 2016, n. 7.

dell’informazione, dato o programma può essere letto solo con un particolare apparato di visualizzazione o di decodificazione.

Anche il possibile abuso della firma elettronica è ascrivibile nell’ambito del falso.

La lesione o messa in pericolo del bene tutelato si realizzano solo quando la falsificazione introduce falsamente e fa venir meno la prova in ordine ad un dato o informazione contenuto nel documento.

L'articolo in questione è ad inserirsi nell'ambito del Capo III "Della falsità in atti" contenuto nel Titolo VII "Dei delitti contro la fede pubblica" del codice penale e richiama i seguenti articoli del Codice penale:

- Art. 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici;
- Art. 477. Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative;
- Art. 478. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti;
- Art. 479. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici;
- Art. 480. Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative;
- Art. 481. Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità;
- Art. 482. Falsità materiale commessa dal privato;
- Art. 483. Falsità ideologica commessa dal privato in atto pubblico;
- Art. 484. Falsità in registri e notificazioni;
- Art. 487. Falsità in foglio firmato in bianco. Atto pubblico;
- Art. 488. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali;
- Art. 489. Uso di atto falso;
- Art. 490. Soppressione, distruzione e occultamento di atti veri;
- Art. 492. Copie autentiche che tengono luogo degli originali mancanti;
- Art. 493. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico.

b)

c) Art. 476 c.p.: Falsità materiale commessa dal pubblico ufficiale in atti pubblici (richiamato dall’art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale, con il quale può concorrere l'estraneo qualora, con la propria attività, abbia cooperato ad offendere il bene giuridico protetto. Non occorre che il pubblico ufficiale sia l'autore materiale del delitto, ma è sufficiente che la sua partecipazione sia determinata dalla sua qualità particolare.

Descrizione

Il reato si identifica nel falso materiale, il quale può manifestarsi nella forma della contraffazione, quando proviene da un autore diverso da quello reale, o della alterazione, quando subisce, dopo la sua formazione, modificazioni di qualsiasi specie, anche da parte dello stesso autore reale, senza autorizzazione degli aventi diritto.

La formazione di un atto falso può essere anche parziale, ma, in tal caso, essa equivale a quella totale.

La falsificazione di più parti di un documento può incidere sulla gravità del fatto, ma non configura una pluralità di reati, neanche uniti dal vincolo della continuazione.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale pubblico ufficiale, forma, in tutto o in parte, un atto falso o altera un atto vero.
- La Società, agendo quale pubblico ufficiale, falsifica il modulo con cui dà atto del pagamento della somma dovuta per imposte da parte del contribuente suo cliente, il quale, in cambio, investe il proprio denaro in prodotti della società medesima (secondo Cass., 31 maggio 1990, n. 7853, detto modulo è atto pubblico, poiché produce effetti giuridici di rilevanza pubblicistica in relazione all'assolvimento dell'obbligo tributario).

a)

b) Art. 477 c.p.: Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

Per ciò che concerne la condotta di contraffazione ed alterazione, si rimanda all'art. 476 c.p., mentre per ciò che riguarda la seconda condotta, la falsa attestazione, mediante contraffazione od alterazione, ci si riferisce agli elementi complementari dell'atto, come ad esempio, le legalizzazioni di firme, le vidimazioni, il pagamento di tasse.

È un delitto istantaneo, poiché si consuma nel momento in cui è realizzata la contraffazione o l'alterazione, senza che occorra l'uso dell'atto falso.

Integra, inoltre, il reato in questione la fotocopia di un documento autorizzativo legittimamente detenuto, realizzata con caratteristiche e dimensioni tali da avere l'apparenza dell'originale, idonea a trarre in inganno i terzi in buona fede (ad es. di un tesserino di appartenenza all'Arma dei Carabinieri o di autorizzazione all'accesso in una zona a traffico limitato).

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale pubblico ufficiale, contraffà o altera certificati o autorizzazioni amministrative, ovvero mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità.

a)

b) Art. 478 c.p.: Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre ad otto anni.

Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

Per copia si intende la riproduzione fedele ed integrale, avvenuta con ogni mezzo, anche meccanico, di un documento ed è autenticata se rilasciata da un pubblico ufficiale che ne garantisca la conformità all'originale.

Gli attestati sono, invece, le certificazioni sintetiche o parziali di altri documenti. L'unico elemento distintivo dell'attestato rispetto al certificato (di cui all'art. 477 c.p.) è nel riferimento del primo al contenuto di altri atti e quindi ai fatti giuridici relativi, con funzione innegabilmente probatoria, assolta ugualmente nel certificato, ma in relazione a fatti o a situazioni risultanti aliunde al pubblico ufficiale. Gli attestati, dunque, diversamente dai certificati, sono documenti a carattere derivativo, perché sinteticamente riproduttivi di altri atti o registri originali, ai quali il loro autore fa organico riferimento per approntarne il contenuto.

Le condotte sanzionate dalla norma sono di tre tipi: il rilascio, in forma legale, di una copia simulata di un atto pubblico supposto ed inesistente; il rilascio di una copia di un atto pubblico o privato diversa dall'originale; la falsificazione, totale o parziale, attinente ad un attestato sul contenuto di un atto pubblico o privato.

Il reato si perfeziona, in tutte e tre le ipotesi, con il rilascio della copia o dell'atto infedeli, rilascio che fa emergere l'atto all'esterno e che può avvenire mediante consegna all'interessato o mediante affissione all'albo di un ufficio o mediante trasmissione ad altra autorità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale pubblico ufficiale, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale.

a)

b) Art. 479 c.p.: Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

Questo è un caso di falsità ideologica, la quale si ha in ogni caso in cui il documento, non contraffatto né alterato, contiene dichiarazioni menzognere, ("attesta falsamente").

La condotta del pubblico ufficiale integra il reato se attesta falsamente che un atto è stato da lui compiuto o è avvenuto in sua presenza.

Le altre ipotesi sono rappresentate dalla falsa attestazione di dichiarazioni non ricevute, dall'omissione o alterazione di dichiarazioni ricevute e, infine, dalla falsa attestazione di fatti dei quali l'atto è destinato a provare la verità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale pubblico ufficiale e ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da essa compiuto o è avvenuto in sua presenza, o attesta come da essa ricevute dichiarazioni non rese, ovvero omette o altera dichiarazioni da essa ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità.

a)

b) Art. 480 c.p.: Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

L'oggetto di tale reato ha la stessa natura di quello di cui all'art. 479 c.p.

La condotta tipica consiste nella falsa attestazione, ad opera del pubblico ufficiale nell'esercizio delle sue funzioni, in certificati o autorizzazioni amministrative, di fatti dei quali l'atto è destinato a comprovarne la verità.

L'espressione "fatti" va intesa in senso ampio, ricomprendendo tutti gli avvenimenti e le situazioni personali (come il pagamento di una tassa, la qualità di cittadino, ecc.), alla cui prova è destinato l'atto in forza del potere certificante del pubblico ufficiale. Ne discende che la falsità può riferirsi a fatti il cui inserimento nell'atto sia del tutto facoltativo, purché siano rilevanti e dotati di potenziale efficacia giuridica. Sono, invece, del tutto irrilevanti il valore probatorio - processuale dell'atto e la circostanza che il soggetto destinatario dello stesso ne abbia fatto o meno uso.

In particolari condizioni, si ritiene che la falsa attestazione possa essere realizzata anche in forma omissiva: la falsità ideologica documentale sussiste non solo quando si affermi in termini contrari al vero l'esistenza di una determinata situazione, ma anche quando, nel descrivere quest'ultima, si omettano elementi rilevanti di connotazione della medesima.

Si può configurare il reato in questione, nel caso di falsa attestazione, da parte del pubblico ufficiale competente, dell'avvenuta riunione di un organo collegiale in apposita seduta, quando, in realtà, i singoli componenti di detto organo erano stati interpellati ed avevano dato i loro pareri separatamente.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale pubblico ufficiale, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità.

a) Art. 481 c.p.: Falsità ideologica commessa da persone esercenti un servizio di pubblica necessità (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino ad un anno o con la multa da € 51,00 a € 516,00.

Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

Autore del reato

L'illecito in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

La condotta tipica consiste nella falsa attestazione in un certificato, da parte di colui che esercita una professione sanitaria o forense od altro servizio di pubblica necessità dei fatti dei quali l'atto è destinato a provare la verità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, nell'esercizio di un servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità (ai sensi dell'art. 359 c.p., agli effetti della legge penale, sono persone che esercitano un servizio di pubblica necessità: a) i privati che esercitano […] professioni il cui esercizio sia per legge vietato senza una speciale abilitazione dello Stato, quando dell'opera di essi il pubblico sia per legge obbligato a valersi; b) i privati che, non esercitando una pubblica funzione, né prestando un pubblico servizio, adempiono un servizio dichiarato di pubblica necessità mediante un atto della pubblica amministrazione).

a)

b) Art. 482 c.p.: Falsità materiale commessa dal privato (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.

Autore del reato

Soggetto attivo del reato è il privato ovvero pubblico ufficiale fuori dell'esercizio delle sue funzioni.

Descrizione

La norma punisce il privato che commette alcuno dei fatti preveduti dagli artt. 476, 477 e 478 c.p.; le condotte sono le stesse previste dai tre articoli richiamati, essendo diverso solo il soggetto attivo del reato.

L'invalidità o l'inesistenza giuridica dell'atto, derivanti dalla stessa falsità, non escludono la rilevanza penale del falso, essendo sufficiente, per la configurabilità del reato, che l'atto appaia valido al momento in cui è posto in essere e determini così la possibilità, valutata ex ante, della lesione della pubblica fede.

Comportamenti che possono integrare il reato in questione sono, ad esempio: la falsificazione delle ricevute bancarie di delega ai versamenti tributari, la falsificazione del modulo con il quale gli istituti di credito danno atto del pagamento della somma dovuta per imposta da parte del contribuente, ecc.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale soggetto privato, forma, in tutto o in parte, un atto falso o altera un atto vero.

a)

b) Art. 483 c.p.: Falsità ideologica commessa dal privato in atto pubblico

Testo della norma del Codice Penale

Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.

Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.

Autore del reato

Il reato in esame è un illecito comune, ossia può essere commesso da "chiunque".

Descrizione

Il reato ricorre qualora il privato attesti falsamente al pubblico ufficiale, in atto pubblico, fatti che l'attestante ha il dovere giuridico di esporre veridicamente e dei quali l'atto, in cui tali attestazioni sono inserite, è destinato a provare la verità. Il reato è configurabile anche per quello che viene taciuto allorquando determini una rappresentazione non veridica.

In tale nozione di atto pubblico, qui intesa, non rientrano soltanto i documenti redatti da un notaio o da un altro pubblico ufficiale autorizzato, ma anche quelli formati dal pubblico ufficiale o dal pubblico impiegato, nell'esercizio delle loro funzioni, per uno scopo diverso da quello di conferire ad essi pubblica fede, purché aventi l'attitudine ad assumere rilevanza giuridica e/o valore probatorio interno alla pubblica amministrazione.

La falsa attestazione deve essere resa ad un pubblico ufficiale e non ad un pubblico impiegato incaricato di un pubblico servizio, poiché l'art. 493 c.p. estende a questi soggetti l'applicabilità esclusivamente delle norme riguardanti le falsità commesse dai pubblici ufficiali, mentre in questo caso l'autore delle falsità è il privato.

L'attestazione del privato deve riguardare fatti: sono escluse le dichiarazioni aventi a contenuto giudizi o dichiarazioni di volontà. Da ciò discende la non punibilità della simulazione dei negozi giuridici.

Il reato in questione si ravvisa, ad esempio, nella falsa dichiarazione del presidente di un'assemblea straordinaria di un consorzio di imprese nel processo verbale redatto da un notaio, in cui sono presenti o rappresentati per delega tutti i consorziati e quando l'assemblea sia validamente costituita.

Esemplificazioni

Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale soggetto privato, attesta falsamente al pubblico ufficiale, in un atto

pubblico, fatti dei quali l'atto è destinato a provare la verità.

a)

b) Art. 484 c.p.: Falsità in registri e notificazioni

Testo della norma del Codice Penale

Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

In linea di principio, può affermarsi che l'obbligo sancito dalla norma di cui all'art. 484 c.p. sia riferito esclusivamente a registrazioni <soggette all'ispezione dell'Autorità di pubblica sicurezza> e non di altre Autorità.

A conferma di tale assunto si pongono vuoi la letteratura in materia (così, per tutti, CRISTIANI, Fede pubblica, in NssDI, VII, 17), vuoi la più risalente e costante giurisprudenza di legittimità (in questo senso, tra le tante, Cass. pen., sez. V, 23 novembre 1978, Frabetti, secondo la quale <si ha riguardo principalmente alle registrazioni e alle notificazioni previste dal testo unico di pubblica sicurezza (r.d. 18 giugno 1931, n. 773 e relativo regolamento>).

Quanto alla portata della locuzione <Autorità di pubblica sicurezza>, è a dire come la medesima paia richiamare implicitamente la l. 1° aprile 1981, n. 121, recante norme in materia di <[n]uovo ordinamento dell'Amministrazione della pubblica sicurezza>.

Orbene, ai sensi della prefata legge, Autorità di pubblica sicurezza sono il prefetto (art. 13), il questore (art. 14), i funzionari preposti ai locali commissariati di polizia e, in loro vece, il sindaco – funzionario di Governo (art. 15).

Statuisce poi l'art. 16 che tra le forze di polizia rientrino pure l'Arma dei carabinieri – quale forza armata in servizio permanente di pubblica sicurezza – e il Corpo della guardia di finanza – ma solo in vista del <concorso al mantenimento dell'ordine e della sicurezza pubblica> –. Ad essi, infine, debbono aggiungersi il Corpo degli agenti di custodia e il Corpo forestale dello Stato, che <possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica>.

Repertori di giurisprudenza alla mano, preme evidenziare come delle cennate definizioni categoriali la Corte di cassazione paia tenere debito conto.

In questo senso, si è, ad esempio, escluso che l'art. 484 c.p. incrimini anche la falsità nelle registrazioni IVA previste dall'art. 24 D.P.R. n. 633 del 1972, essendo esse assoggettate esclusivamente al controllo degli uffici provinciali IVA e della guardia di finanza. In parte motiva, la Suprema Corte ha precisato appunto che, per quanto il Corpo della guardia di finanza sia compreso tra le forze di polizia dalla l. 1 aprile 1981 n. 121, esso <non fa parte dell'organizzazione amministrativa della pubblica sicurezza>, essendo chiamato unicamente a <concorrere> al mantenimento dell'ordine e della sicurezza pubblica (Cass. pen., sez. V, 15 maggio 1987, D.).

Su questa stessa scia, peraltro, parrebbero porsi tutte le non numerose pronunce giurisprudenziali sul tema.

Secondo la Corte regolatrice, infatti, integra falsità in registri la condotta di colui che, in qualità di titolare di un'agenzia di pratiche auto, lasci, nel registro sottoposto ad ispezione da parte dell'Autorità di pubblica sicurezza, spazi in bianco, ancorché numerati, trattandosi di attività diretta in modo non equivoco alla abusiva annotazione di pratiche svolte in un momento successivo rispetto a quello che sarebbe risultato in ragione dell'alterata collocazione cronologica (Cass. pen., sez. V, 7 novembre 2007, B.); la condotta di colui che inserisce false indicazioni nei registri di carico e scarico rifiuti (Cass. pen., sez. II, 13 febbraio 2004, I. e altri); la condotta di colui che, titolare dell'autorizzazione alla vendita di armi, ne violi i limiti imposti per qualità o quantità, falsamente registrando i dati inerenti i destinatari della vendita (Cass. pen., sez. V, 7 novembre 2000, Duodero); la condotta di colui che proceda a false indicazioni nei registri tenuti dai commercianti di zucchero a norma dell'art. 74 D.P.R. 12 febbraio 1965, n. 162, posto che le indicazioni anzidette, al pari di quelle che siano contenute nelle bollette di accompagnamento dello zucchero, rientrano nel novero delle registrazioni da notificare all'Autorità (Cass. pen., sez. VI, 18 giugno 1992, Casella).

D'altro canto, ad inopinate estensioni analogiche in materia penale parrebbe ostare il principio di tassatività, che in siffatto contesto rinviene copertura anche costituzionale.

Un dato, tuttavia, va tenuto in debito conto: come la Corte di cassazione ha avuto modo di precisare, a ché si abbia il reato di cui all'art. 484 c.p. è sufficiente <l'esistenza di un qualsiasi potere di controllo dell'Autorità di pubblica sicurezza, anche se le registrazioni e le notificazioni sono destinate ad altra pubblica amministrazione> (Cass. pen., sez. V, 23 novembre 1978, Frabetti).

Ciò significa che il reato sussiste ogni qual volta la registrazione o la notificazione possa essere oggetto di controllo anche da parte dell'Autorità di pubblica sicurezza, pur non essendo esse direttamente indirizzate a quest'ultima, bensì ad altra pubblica amministrazione.

Riannodando i fili del discorso, pare a chi scrive che, alla luce di quanto sopra affermato, sia invero arduo sostenere che Banca d'Italia, CONSOB, UIF, etc. siano Autorità di pubblica sicurezza ai fini che qui ci occupano. Peraltro, lo si ribadisce, una corretta esegesi della norma, rispettosa dell'irrinunciabile principio di tassatività costituzionalmente tutelato, parrebbe destituire di fondamento ogni contraria interpretazione sul punto.

Ciò non di meno, è bene tenere a mente che registrazioni e notificazioni indirizzate ad autorità diverse da quelle di pubblica sicurezza possono rilevare ai predetti fini ogni qual volta possano essere oggetto di ispezione anche da parte delle autorità da ultimo menzionate.

La qual cosa, se non amplia la portata operativa della norma in esame, impone, tuttavia, attenta riflessione operativa caso per caso.

La falsità ivi contemplata è di natura ideologica poiché attiene all'atto (di registrazione o di notificazione) e non alla sua documentazione.

Il reato può essere compiuto solo da colui che per legge è obbligato a fare registrazioni in relazione ad una sua qualsiasi attività e da colui che, pur per legge, sia obbligato a comunicare all'Autorità di PS fatti inerenti ad una attività industriale, commerciale o professionale. L'obbligo di fare le registrazioni o le notificazioni deve derivare da una norma giuridica.

Il reato consiste nello scrivere o nel lasciare scrivere (cioè nel caso in cui il soggetto obbligato, potendo impedire la perpetrazione del falso, non la impedisce) false indicazioni nelle registrazioni soggette all'ispezione dell'Autorità, ovvero false indicazioni nelle notificazioni all'Autorità circa le proprie operazioni industriali, commerciali o professionali. Rispetto alle notificazioni, il reato si consuma con la ricezione dell'atto dall'Autorità destinataria, mentre rispetto alle registrazioni, la consumazione è anticipata al momento della *editio falsi*, dato che esse sono sempre immediatamente ispezionabili dall'Autorità.

Esemplificazioni

Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società – obbligata per legge a fare registrazioni soggette all'ispezione dell'autorità di pubblica sicurezza, o a fare notificazioni all'autorità stessa circa le proprie operazioni industriali, commerciali o professionali – scrive o lascia scrivere false indicazioni.

a)

Art. 485 c.p.: Falsità in scrittura privata

Questo articolo è stato abrogato dall'art. 1 comma 1 lett. a) d.lgs. n. 7/2016.

Art. 486 c.p.: Falsità in foglio firmato in bianco. Atto privato

Questo articolo è stato abrogato dall'art. 1 comma 1 lett. a) d.lgs. n. 7/2016

Art. 487 c.p.: Falsità in foglio firmato in bianco. Atto pubblico (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

Essendo l'autore del reato il pubblico ufficiale, il possesso del foglio firmato in bianco deve essere dovuto ad una ragione d'ufficio. È necessario che l'agente abbia scritto o fatto scrivere un atto pubblico; non occorre che venga fatto uso del documento.

Il delitto si consuma nel tempo e nel luogo dell'avvenuto riempimento non autorizzato.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale e abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio o per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligata o autorizzata.

Art. 488 c.p.: Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale ([2])

Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dall'art. 487 si applicano le disposizioni sulle falsità materiali in atti pubblici.

Descrizione

Il reato si verifica quando viene riempito un documento firmato in bianco ad opera di chi non aveva il potere di realizzarlo. Si tratta di una falsità materiale.
Presupposto del reato è che il documento non sia stato acquisito legittimamente ovvero che il riempimento sia stato effettuato senza un valido mandato *ad scribendum*, perché mai esistito o perché non valido in quel momento o dopo che questo sia cessato.

Esemplificazioni

Non si forniscono esemplificazioni del reato in esame poiché l'art. 488 c.p. è una norma di rinvio e le esemplificazioni a riguardo sono già contenute nell'esemplificazioni di carattere generale concernenti le falsità materiali in atti pubblici.

Art. 489 c.p.: Uso di atto falso ([3])

Testo della norma del Codice Penale

Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Il reato è integrato dall'uso dell'atto falsificato da parte di persona diversa dall'autore o concorrente nella falsificazione. Risponde del reato in questione, per l'uso del documento contraffatto, l'autore della contraffazione che non risulti punibile a seguito di estinzione del reato, nonché l'autore della falsificazione tutte le volte in cui il reato di falso è venuto meno (per prescrizione o amnistia) o non è punibile (reato commesso all'estero) e l'autore o concorrente nella falsificazione persiste nel far uso dell'atto falso.

Esemplificazioni

Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

([2]) Così come modificato dal D.lgs. 15 gennaio 2016, n. 7.
([3]) Articolo modificato dall'art. 2, comma 1, lett. a) d.lgs. n. 7/2016.

- La Società, senza essere concorsa nella falsità, fa uso di un atto falso.

Art. 490 c.p.: Soppressione, distruzione e occultamento di atti veri ([4])

Testo della norma del Codice Penale

Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero, o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Il reato è configurabile anche quando il contenuto del documento possa essere ricostruito attraverso altri originali (duplicati) o sia stato riprodotto in atti derivati o sia desumibile aliunde.

Si presuppone l'esistenza di un obbligo giuridico di conservazione del documento, necessario per la qualificazione antigiuridica della condotta.

Le condotte previste come punibili sono tre: distruzione, soppressione e occultamento. Distruggere significa non far più sussistere il documento nella sua materialità, in tutto, o in parte, giuridicamente rilevante; sopprimere significa far scomparire o rendere illeggibile lo scritto in tutto o in parte; occultare significa tenere anche temporaneamente celato l'atto impedendone l'utilizzo giuridicamente rilevante.

Esemplificazioni

Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero.

b)

c) Art. 492 c.p.: Copie autentiche che tengono luogo degli originali mancanti (richiamato dall'art. 491-bis c.p.)

d) Testo della norma del Codice Penale

Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.

Descrizione

Per copia autentica si intende la riproduzione esatta, completa e letterale, tratta dall'originale di un atto pubblico o di una scrittura privata, formata sotto la responsabilità di un pubblico ufficiale o di un incaricato di

([4]) Articolo modificato dall'art. 2, comma 1, lett. d) d.lgs. n. 7/2016.

pubblico servizio competente ad attribuire ad essa la pubblica fede attestandone l'autenticità e da lui effettivamente autenticata.

La tutela penale riguarda solo la copia autentica che tenga luogo dell'originale mancante e non le altre copie autentiche o gli originali duplicati o gli attestati.

Il reato sussiste anche se la copia autentica sia stata formata apponendo, accanto alla falsa firma del notaio rogante, l'impronta del sigillo di un diverso notaio.

1.16.1 Esemplificazioni

Non si forniscono esemplificazioni del reato in esame poiché norma di carattere esplicativo. Pertanto è sufficiente riportarne il testo.

e)

f) Art. 493 c.p.: Falsità commesse da pubblici impiegati incaricati di un servizio pubblico (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

Autore del reato

Soggetto attivo del reato è il pubblico impiegato incaricato di esercitare un pubblico servizio.

Descrizione

Questa disposizione equipara gli atti redatti da pubblici impiegati incaricati di pubblico servizio agli atti pubblici, estendendo ai primi la tutela penale predisposta per i secondi.

È pubblico impiegato ogni dipendente dell'ente pubblico che svolga prestazioni permanenti, purché non esclusivamente manuali.

Esemplificazioni

Non si forniscono esemplificazioni del reato in esame poiché lo stesso non è rilevante per la Società.

La Società, infatti, agisce unicamente da soggetto privato. Di conseguenza, l'art. 493 c.p., richiamato dall'art. 491-bis c.p., non è applicabile alla Zaccaria Costruzioni S.r.l.

g)

h) Art. 615-ter c.p.: Accesso abusivo ad un sistema informatico o telematico

Testo della norma del Codice Penale

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

La pena è della reclusione da uno a cinque anni:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

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

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da “chiunque”.

Descrizione

La qualità soggettiva di cui al comma 2 n. 1) integra una circostanza aggravante.

È punito sia colui che si introduce abusivamente, cioè senza il consenso del titolare dello *ius excludendi* in un sistema informatico o telematico munito di sistemi di sicurezza, sia colui che permane in collegamento con il sistema stesso continuando a fruire dei servizi resi o ad accedere alle informazioni in esso custodite, nonostante il titolare abbia esercitato, sia pur tacitamente, lo *ius escludendi*.

Il reato si consuma con il semplice accesso ad un sistema telematico o informatico, a prescindere dal fine, purché il sistema sia protetto da misure di sicurezza (è sufficiente anche una protezione semplice, cioè una password).

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- Il dipendente della Società si introduce nel sistema informatico di una Società concorrente onde apprendere notizie su piani di investimento al fine di rendere più competitiva la propria azienda
- La Società 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 diritto di escluderla.

a)

b) Art. 615-quater c.p.: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Testo della norma del Codice Penale

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164,00.

La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da “chiunque”.

Descrizione

Questa norma completa la tutela prevista dalla precedente e punisce l’abusiva acquisizione in qualunque modo (comprensivo dell’autonoma elaborazione) dei mezzi o codici di accesso, che consegue a soggetti non legittimati di inserirsi nel sistema informatico o telematico altrui, vanificando l’ostacolo costituito dalle misure di protezione.

“Procurarsi” significa appropriarsi fisicamente della chiave meccanica o della scheda magnetica, oppure individuare i codici di accesso attraverso procedimenti logici tipici del computer. La mera detenzione di un mezzo per l’accesso ad un sistema informatico altrui è penalmente irrilevante se non è seguita dall’uso.

“Riprodurre” significa realizzare una copia abusiva di un codice di accesso, idonea all’uso.

La divulgazione a terzi del codice o della parola-chiave si ottiene mediante la diffusione, la comunicazione, la consegna, condotte che possono concorrere con il mero procacciamento.

Esemplificazioni

Si riporta di seguito l’esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

a)

b) Art. 615-quinquies c.p.: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Testo della norma del Codice Penale

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a € 10.329,00.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Rispetto alla norma precedente da questa sostituita, vi è stata un'estensione delle condotte punibili, con l'aggiunta delle locuzioni "si procura, produce, riproduce, importa" oltre a quelle già originariamente presenti di chi "diffonde, comunica, consegna", completando con quella di "mettere a disposizione di altri".

Le predette condotte, per essere punibili, devono essere dirette a danneggiare o interrompere illecitamente un sistema informatico o telematico. Se così non fosse, sarebbero perfettamente lecite, in quanto usuali nell'attività di ogni operatore privato o commerciale.

È il solo fine dell'agente che rende penalmente illecito il fatto.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società finanzia direttamente o indirettamente – ovvero concorre nel reato agevolandone l'operato – soggetti o strutture che diffondono, comunicano o consegnano programmi informatici da loro stessi o da altri redatti, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.
- La Società diffonde, comunica o consegna programmi informatici da lei stessa o da altri redatti, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

a)

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

Testo della norma del Codice Penale

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2. da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3. da chi esercita anche abusivamente la professione di investigatore privato.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

La norma intende tutelare sia la libertà di comunicare che il diritto alla riservatezza delle comunicazioni. E' così estesa la tutela apprestata alle comunicazioni telegrafiche e telefoniche dall'art. 617 c.p. anche alle comunicazioni informatiche e telematiche.

La pena è aumentata se l'autore è un pubblico ufficiale o un incaricato di pubblico servizio con abuso di poteri o con violazione di doveri funzionali ovvero con abuso della qualità di operatore del sistema, intendendosi per tale il soggetto addetto con funzioni tecniche al coordinamento o alla diretta gestione delle operazioni di comunicazione dei dati.

Per intercettazione si intende l'attività di captazione del contenuto delle comunicazioni informatiche o telematiche in corso di svolgimento tra operatori abilitati del sistema. Con l'interruzione e l'impedimento, assumono rilevanza tutte quelle attività tecniche finalizzate, attraverso qualsiasi modalità concreta, a sospendere da un certo momento in poi ovvero a precludere lo stesso inizio di una comunicazione informatica o telematica.

Per essere punibile, tale condotta deve essere realizzata attraverso strumenti di comunicazione di massa o comunque in grado di raggiungere un numero indeterminato di destinatari, non assumendo rilevanza la mera rivelazione eseguita ad uno o più soggetti determinati.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.
- La Società rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi fraudolentemente intercettate.

a)

b) Art. 617-quinquies c.p.: Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Testo della norma del Codice Penale

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

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

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

La norma in questione offre una forma di tutela anticipata rispetto ai beni protetti dal precedente articolo, attraverso la previsione di punibilità per comportamenti prodromici rispetto a quelli di vera e propria interferenza nelle comunicazioni informatiche o telematiche.

La condotta consiste nell'installazione di strumenti idonei ad intercettare, impedire o interrompere le comunicazioni; non è necessario il loro effettivo funzionamento, a meno che non si tratti di mezzi tecnici assolutamente incapaci a realizzare una qualsiasi interferenza.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, fuori dei casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

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

Testo della norma del Codice Penale ([5])

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

([5]) Così come modificato dal D.lgs. 15 gennaio 2016, n. 7.

Descrizione

Oltre alle ipotesi tradizionali di “distruzione” e di “deterioramento”, sono state aggiunte a questa norma anche quelle di “cancellazione, alterazione e soppressione” delle informazioni, dei dati o dei programmi informatici altrui.

Per individuare, nell’ipotesi in esame, la persona offesa dal reato ed interpretare il concetto di altruità, non si può fare riferimento al concetto giuridico di possesso dei dati, delle informazioni o dei programmi, poiché caratterizzati dalla immaterialità. La cerchia degli aventi diritto all’integrità dei dati, delle informazioni e dei programmi dovrà essere determinata alla stregua della pluralità degli interessi giuridicamente rilevanti, di natura obbligatoria, anziché “reale”, che su di essi possono convergere.

Nel caso di danneggiamento di programmi, possono essere considerate persone offese il concessionario, il legittimo utilizzatore, il concedente, il proprietario, l’operatore del sistema, nonché i partners commerciali o di lavoro di un’impresa o di un professionista, rispetto ad informazioni i dati da essi forniti per determinate finalità operative.

Esemplificazioni

Si riporta di seguito l’esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui.

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

Testo della norma del Codice Penale ([6])

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l’alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da “chiunque”.

Descrizione

La norma in questione si allinea con il contenuto di cui all’art. 635-bis, con la differenza che, in questo caso, si parla di danneggiamento di dati di pubblica utilità. Fin dalla rubrica, infatti, si parla di sistemi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, la quale viene riferita ad informazioni, dati o programmi informatici.

([6]) Così come modificato dal D.lgs. 15 gennaio 2016, n. 7.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

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

Testo della norma del Codice Penale ([7])

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Rispetto a quanto previsto e punito nell'art. 635-bis c.p., la norma in questione contempla come condotte punibili anche l'introduzione o la trasmissione di dati, informazioni o programmi.
Si è, inoltre, aggiunta un'ulteriore e nuova ipotesi alternativa, realizzabile quando si ostacola gravemente il funzionamento del sistema, risultato che può essere l'effetto di una qualsiasi delle descritte condotte, comprese quelle più neutrali della mera immissione e trasmissione dei dati.

Esemplificazioni

Si riporta di seguito l'esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, mediante le condotte di cui all'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

([7]) Così come modificato dal D.lgs. 15 gennaio 2016, n. 7.

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

Testo della norma del Codice Penale (8)

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Tale articolo si allinea alla formulazione dell'art. 635-quater c.p. per quanto attiene all'enunciazione dei verbi "distruggere, danneggiare, rendere, in tutto o in parte, inservibili od ostacolarne gravemente il funzionamento". Facendosi qui riferimento, in rubrica, solo alla pubblica utilità, si ritiene che questa formula generica sia idonea ad abbracciare tutte le situazioni menzionate nella norma, non chiedendo come condizione necessaria l'utilizzazione effettiva da parte di un soggetto pubblico.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, mediante le condotte di cui all'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ne ostacola gravemente il funzionamento.

(8) Così come modificato dal D.lgs. 15 gennaio 2016, n. 7.

a)

b)

c) Art. 640-quinquies c.p.: Frode informatica del certificatore di firma elettronica

Testo della norma del Codice Penale

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 € 51,00 a € 1.032,00.

Autore del reato

Il reato in esame è un reato proprio, ossia può essere commesso dal soggetto che presta servizi di certificazione di firma elettronica.

Descrizione

In questa fattispecie il fine di procurare a sé o ad altri un ingiusto profitto è previsto in termini alternativi rispetto a quello di arrecare ad altri un danno, che non è connotato in termini patrimoniali (a differenza dell'art. 640 c.p.).

La mera strumentatiti della violazione di uno degli obblighi extrapenali destinata al perseguimento di un generico interesse di parte (profitto proprio o di terzi ovvero danno di altri) è sufficiente alla consumazione del fatto tipico, con forte anticipazione della soglia di punibilità.

La realizzazione del descritto fatto è molto simile a quella del delitto proprio del pubblico ufficiale, rispetto al quale anticipa la soglia di punibilità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società – laddove dovesse agire quale soggetto deputato a prestare servizi di certificazione di firma elettronica – 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.

1 Le “macro aree” di attività sensibili in relazione ai reati in tema di criminalità informatica e di trattamento illecito di dati e i ruoli aziendali coinvolti

Con riferimento agli illeciti sopra elencati, nell’affrontare l’attività di *risk mapping*, occorre fare alcune considerazioni:

- l’utilizzo della strumentazione informatica è ormai talmente generalizzato da estendersi a ogni area e ad ogni processo operativo esistente in qualunque tipo di società. In queste condizioni, difficilmente la mappatura dei rischi di commissibilità di reati informatici potrà escludere qualche area o qualche processo operativo della società, anche perché, a differenza di altri reati presupposto, quelli informatici sono commissibili non tanto nello svolgimento di specifiche attività ma in funzione dell’utilizzazione degli strumenti informatici e alla condizione del possesso, da parte di chi vuole commetterli, dell’indispensabile livello di competenza informatica. Ciò significa che non è possibile escludere a priori nessun settore di attività della società dalla mappa di commissibilità di reati informatici presupposto;
- non è detto che la commissine di reati informatici presupposto avvenga mediante l’utilizzo dei mezzi informatici messi a disposizione dalla società ai suoi dipendenti o apicali ovvero nel normale svolgimento delle attività lavorative proprie della società: chi li commette può ben utilizzare strumenti informatici di sua proprietà o comunque a sua disposizione e può agire operando al di fuori della società: In questi casi, qualsiasi misura preventiva risulterà inutile;
- per quanto riguarda i ruoli aziendali coinvolti nelle suddette fattispecie delittuose, è evidente che i reati richiamati dall’art. 491 *bis* c.p. che, a loro volta, fanno riferimento a comportamenti propri dei pubblici ufficiali, potranno essere compiuti da dipendenti o apicali della società soltanto a titolo di concorso ai sensi dell’art. 110 c.p.;
- in generale, i ruoli aziendali coinvolti nei reati qui considerati saranno tutti coloro che, all’interno della società, hanno accesso al sistema informatico.

2 I protocolli preventivi adottati dalla Società

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole stabilite nel Modello di organizzazione, gestione e controllo (di seguito "Modello"), i soggetti aziendali coinvolti nella gestione delle "macro aree" di attività sensibili individuate in relazione ai reati di cui all'art. 24 *bis* del Decreto sono tenuti, al fine di prevenire e impedire il verificarsi dei reati, al rispetto di una serie di "Protocolli preventivi" ("di sistema" o, talvolta, "specifici").

Di seguito è riepilogato il quadro in precedenza esposto.

PROTOCOLLI PREVENTIVI DI SISTEMA

Previsione dei divieti nel Codice Etico

Diffusione del Codice Etico verso tutti i dipendenti e i terzi destinatari

Sistema di deleghe

Informazione e formazione specifica del personale

Segregazione dei compiti tra i differenti soggetti coinvolti nei processi

Sistema disciplinare

Documento programmatico di sicurezza

Clausola 231/01 nei contratti con i terzi

Gestione delle risorse finanziarie

Tracciabilità/archiviazione

Direttiva aziendale antiriciclaggio

Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori

Procedura di nomina del responsabile interno autorizzato a trattare con la PA

Iscrizione nella *white list* istituita presso la Prefettura

Clausola l. 122/2012 nei contratti di appalto e di fornitura

PROTOCOLLI PREVENTIVI SPECIFICI

a) Art. 491-bis c.p.: Falsità in un documento informatico pubblico o avente efficacia probatoria

Oltre ai controlli generali, dovrebbero essere applicati i seguenti controlli specifici:

- misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema accessibile al pubblico, al fine di prevenire modifiche non autorizzate; gestione del sito online da parte di una Società di consulenza esterna;
- misure di protezione dei documenti elettronici (es. firma digitale);
- procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali; non vengono installati software senza licenza e ogni installazione può essere eseguita solo se autorizzata; all'installazione procede direttamente la società di consulenza esterna incaricata.

b) Art. 615-ter c.p.: Accesso abusivo ad un sistema informatico o telematico

L'accesso abusivo, oltre ad essere di per sé un illecito, può essere strumentale alla realizzazione di altre fattispecie criminose. I controlli predisposti per prevenire tale fattispecie di reato devono pertanto risultare efficaci anche per la prevenzione di altri reati. Tra tali controlli si segnalano:

- rimozione dei diritti di accesso al sistema informatico aziendale al termine del rapporto di lavoro nonché rimozione della casella di posta elettronica;
- rapporti con la Pubblica Amministrazione: le autorizzazioni per gestire online i rapporti con la PA (es. Agenzia delle Entrate, INPS, INAIL, etc.) e le credenziali per accedere ai rispettivi siti internet sono concesse dai relativi enti, previa richiesta della Zaccaria Costruzioni S.r.l., a personale dipendente determinato e individuato;
- gestione dei sistemi informativi;
- previsione di specifiche misure di sicurezza descritte all'interno del DPS della Società: in particolare, la rete privata è costituita da un server e da un dispositivo di backup localizzati nell'area CED ad acceso controllato; i locali sono protetti da dispositivi antincendio, gruppo di continuità dell'alimentazione elettrica e impianto di condizionamento; al fine di impedire accessi non autorizzati, sono inoltre adottate le seguenti misure: suoneria di ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;
- aggiornamento delle misure di sicurezza e controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup.

c) Art. 615-quater c.p.: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Oltre ai controlli generali, devono essere applicati i seguenti controlli specifici:

- individuazione autonoma da parte dei dipendenti delle credenziali personali per l'accesso al sistema informativo aziendale e consegna delle stesse, in modalità riservata, a personale all'uopo incaricato che provvede alla conservazione in cassaforte;
- previsione di specifiche istruzioni per i dipendenti in merito alle modalità di elaborazione e custodia delle password necessarie per accedere agli elaboratori elettronici, alle modalità di utilizzo e custodia degli strumenti elettronici e dei supporti rimuovibili, alle procedure e alle modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- rimozione dei diritti di accesso al sistema informatico aziendale al termine del rapporto di lavoro nonché rimozione della casella di posta elettronica;
- rispetto di tutti i requisiti minimi indicati dall'allegato b) della l. 196 del 2003 (es. cambio automatico della password ogni sei mesi).

d) Art. 615-quinquies c.p.: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Oltre ai controlli generali, devono essere applicati i seguenti controlli specifici:

- formalizzazione di regole e specifiche istruzioni impartite ai dipendenti 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 dalla società;
- previsione di sistemi antivirus su tutti i computer al fine di proteggere il sistema informatico da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema; tutta la rete privata della Zaccaria Costruzioni S.r.l. è gestita a livello globale e protetta da firewell ed ogni singolo pc ha installato un firewell, che si attiva automaticamente quando il pc non è collegato in rete, e un programma antivirus; aggiornamento trimestrale automatico del sistema di protezione;
- procedure di controllo della installazione di software sui sistemi operativi e hardware; i software vengono installati dalle Società di consulenza esterne;
- procedure per rilevare e indirizzare le vulnerabilità tecniche dei sistemi; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup.

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

Art. 617-quinquies c.p.: Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Oltre ai controlli generale, devono essere applicati i seguenti controlli:

- utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse; i locali (area CED) sono protetti da dispositivi antincendio, gruppo di continuità dell'alimentazione elettrica e impianto di condizionamento; al fine di impedire accessi non

autorizzati, sono inoltre adottate le seguenti misure: suoneria di ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;

- definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato (Società di consulenza esterna);
- previsione di controlli sulla rete aziendale e sulle informazioni che vi transitano; previsione di black list dei siti cui non è possibile accedere;
- esistenza di controlli per l'instradamento (routing) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza;
- esistenza di procedure di controllo della installazione di software sui sistemi operativi e di hardware; i software vengono installati dalle Società di consulenza esterne;
- esistenza di procedure per rilevare e indirizzare le vulnerabilità tecniche dei sistemi; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup.

f) Art. 635-bis c.p.: Danneggiamento di informazioni, dati e programmi informatici

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

Oltre ai controlli generali, dovrebbero essere applicati i seguenti controlli specifici:

- utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse; i locali (area CED) sono protetti da dispositivi antincendio, gruppo di continuità dell'alimentazione elettrica e impianto di condizionamento; al fine di impedire accessi non autorizzati, sono inoltre adottate le seguenti misure: suoneria di ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;
- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti informatici (UserID e password personalizzate);
- formalizzazione di regole per un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni; previsione di specifiche istruzioni per i dipendenti in merito alle modalità di elaborazione e custodia delle password necessarie per accedere agli elaboratori elettronici, alle modalità di utilizzo e custodia degli strumenti elettronici e dei supporti rimuovibili, alle procedure e alle modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione;
- previsione di sistemi antivirus su tutti i computer al fine di proteggere il sistema informatico da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema; tutta la rete privata della Zaccaria Costruzioni S.r.l. è gestita a livello globale e protetta da firewell ed ogni singolo pc ha installato un firewell, che si attiva automaticamente quando il pc non è collegato in rete, e un programma antivirus; aggiornamento trimestrale automatico del sistema di protezione;
- procedure di controllo della installazione di software sui sistemi operativi e hardware; i software vengono installati dalle Società di consulenza esterne;

- procedure per rilevare e indirizzare le vulnerabilità tecniche dei sistemi; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup.

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

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

Oltre ai controlli generali, devono essere applicati i seguenti controlli specifici:

- definizione di regole per un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni; previsione di specifiche istruzioni per i dipendenti in merito alle modalità di elaborazione e custodia delle password necessarie per accedere agli elaboratori elettronici, alle modalità di utilizzo e custodia degli strumenti elettronici e dei supporti rimuovibili, alle procedure e alle modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione;
- misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse; i locali (area CED) sono protetti da dispositivi antincendio, gruppo di continuità dell'alimentazione elettrica e impianto di condizionamento; al fine di impedire accessi non autorizzati, sono inoltre adottate le seguenti misure: suoneria di ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;
- definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato (Società di consulenza esterna);
- presenza di misure per un'adeguata protezione delle apparecchiature incustodite; prescrizione ai dipendenti di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro; predisposizione di istruzioni specifiche in merito alle modalità di utilizzo e custodia degli strumenti elettronici e dei supporti informatici rimuovibili;
- previsione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business; i locali ove si svolge il trattamento dei dati sono protetti da dispositivi antincendio, gruppo di continuità dell'alimentazione elettrica, impianto di condizionamento e sono adottate le seguenti misure al fine di impedire accessi non autorizzati: suoneria di ingresso e attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate.

h) Art. 640-quinquies c.p.: Frode informatica del certificatore di firma elettronica

Oltre ai controlli generali, devono essere applicati i seguenti controlli specifici:

- misure volte alla protezione dei documenti elettronici (es. firma digitale);
- procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali.

3 I “processi strumentali” relativi ai reati tema di criminalità informatica e di trattamento illecito di dati societari (art. 24 bis del decreto)

Seguendo la stessa metodologia utilizzata per l’individuazione delle attività “a rischio reato”, sono state individuate, nell’ambito della struttura organizzativa ed aziendale della Zaccaria Costruzioni S.r.l., i processi considerati strettamente “strumentali”, ovvero quei processi c.d. “di supporto” alle attività che insistono sulle aree “ a rischio reato”.

Nell’ambito di ciascuna attività “strumentale”, sono stati, inoltre, individuati i Ruoli Aziendali coinvolti e le relative attività c.d. “sensibili”. Sono stati, infine, individuati i principali protocolli preventivi che insistono su ciascuna area “strumentale”.

Di seguito è riepilogato il quadro in precedenza esposto.

Con riferimento agli illeciti sopra elencati, i “processi strumentali” collegati alle “macro aree” sensibili ritenute più specificamente a rischio risultano essere le seguenti:

- Gestione dei sistemi informativi aziendali

1) GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI

ruoli aziendali coinvolti
Amministratore di sistema
Responsabile del sito web
Società di consulenza esterne

attività sensibili

- **a)** Gestione dell'attività di sviluppo di nuovi sistemi informativi
- **b)** Gestione dell'attività di manutenzione dei sistemi esistenti
- **c)** Gestione dell'attività di elaborazione dei dati
- **d)** Gestione della sicurezza informatica sia a livello fisico che a livello logico:
  1. Configurazione delle security policy dei firewall ai fini della tutela delle intrusioni esterne;
  2. Gestione e protezione dei back up dei dati
  3. Elaborazione di un Disaster Recovery Plan a tutela del patrimonio informativo

protocolli preventivi
Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. esiste una procedura per il tracciamento e la documentazione della manutenzione dei sistemi, basati su due ambienti segregati (Società di consulenza esterne);
2. i sistemi sono monitorati e gestiti dai vari team di maintanance, sia a livello applicativo che infrastrutturale, secondo schedulazioni predefinite (Società di consulenza esterna);
3. esistono software per il controllo e le verifiche dello stato dei sistemi informatici (Società di consulenza esterne);
4. la rete privata, realizzata mediante collegamenti via cavo, è costituita da un server localizzato nell'area CED; dieci postazioni lavoro; un dispositivo di backup localizzato nell'area CED ad accesso controllato; un pc portatile collegabile in rete;
5. oltre alle istruzioni generali, vengono fornite esplicite istruzioni ai dipendenti in merito alle modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici; la prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro; procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi; procedure per il salvataggio dei dati; modalità di custodia ed utilizzo dei supporti rimuovibili; il dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal Responsabile Sistemi informativi, sulle misure di sicurezza;
6. il DataCenter è protetto ed allarmato e l'accesso è consentito alle sole persone autorizzate; in particolare, al fine di scongiurare il rischio di perdita o danneggiamento dei dati a seguito di eventuali eventi distruttivi, i locali sono protetti da: dispositivi antincendio previsti dalla normativa vigente; gruppo di continuità dell'alimentazione elettrica; impianto di condizionamento. Sono inoltre adottate le seguenti misure, al fine di impedire accessi non autorizzati: suonerie d'ingresso; attivazione automatica – ad orari prestabiliti – del sistema di allarme collegato telefonicamente a persone individuate;

7. realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'l'identità delle persone che hanno accesso agli strumenti informatici; le postazioni di lavoro munite di videoterminale sono state dotate di password o parola chiave, che consentono l'accesso ai soli soggetti autorizzati a conoscenza di dette parole chiavi; l'accesso alla rete e ai sistemi aziendali è pertanto soggetto ad autenticazione mediante l'uso di UserID e Password personali; le password sono soggette a scadenza (ogni 6 mesi) e criteri di robustezza (Amministratore di sistema);
8. conferimento della qualifica di custode delle password e vice custode delle password a personale dell'azienda individuato, con l'obbligo di stilare un elenco di parole chiave e di mantenerlo aggiornato; obbligo di comunicazione, per i dipendenti, al custode delle password delle parole chiave e di eventuali variazioni, ulteriori rispetto alle modifiche obbligatorie periodiche (ogni 6 mesi);
9. protezione di strumenti e dati da malfunzionamenti e attacchi informatici. Tutta la rete della Zaccaria Costruzioni S.r.l. è gestita a livello globale e protetta da firewall; ogni singolo pc ha installato un firewall (le policy sono gestite a livello corporate per le varie tipologie di firewall e non è possibile cambiarle localmente), che si attiva automaticamente quando il pc non è collegato alla rete aziendale, e un programma antivirus; il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione; aggiornamento trimestrale del sistema di protezione;
10. esiste una procedura di Disaster Recovery a tutela del patrimonio informativo della Zaccaria Costruzioni S.r.l.;
11. esiste un dispositivo di backup localizzato nell'area CED ed esiste una procedura standardizzata e documentata per la gestione dei backup dei dati del server; previsione di procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema; il salvataggio dei dati avviene con frequenza giornaliera e le copie vengono custodite in luogo protetto;
12. aggiornamento delle misure di sicurezza; controllo – con frequenza almeno mensile – dell'efficacia delle misure adottate relativamente all'accesso fisico ai locali, all'efficacia e all'utilizzo delle misure di sicurezza degli strumenti elettronici e all'integrità dei dati e delle loro copie di backup;
13. Zaccaria Costruzioni S.r.l. ha chiaramente informato gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dalle Società di consulenza esterne;
14. tutta la posta aziendale in uscita e in ingresso viene mantenuta e salvata ed è soggetta alle stesse regole di autenticazione degli altri sistemi aziendali;
15. il sistema di posta elettronica è protetto da un sistema ANTISPAM che blocca immediatamente l'ingresso della posta indesiderata;
16. il sistema è dotato di un web filtering perimetrale per evitare l'accesso di virus in azienda tramite web e per limitare l'accesso ad alcuni siti internet da parte degli utenti (black list);
17. gestione del sito online da parte di una Società di consulenza esterna e aggiornamento dei contenuti da parte del Responsabile Servizi informativi;
18. tutte le attività devono prevedere un sistema di autorizzazioni, deleghe e/o separazioni dei compiti, per ciascuna delle attività dei singoli processi;
19. la Società deve porre particolare attenzione affinché, nelle procedure riguardanti il processo di gestione dei sistemi informativi e in tutte le attività ad esso collegate, siano ben definite e controllate le responsabilità delle funzioni preposte allo sviluppo delle singole attività e che tali responsabilità siano coerenti con il quadro dei controlli specifici ai fini del D.Lgs. 231/01;
20. la funzione preposta deve informare l'OdV periodicamente – e comunque con frequenza almeno trimestrale – attraverso uno specifico report, sugli aspetti significativi afferenti le diverse attività di propria competenza, in particolare per quando attiene: le attività di salvaguardia delle attrezzature hardware e dei programmi software; i controlli e le verifiche periodiche sull'efficienza del sistema. La funzione preposta ha l'obbligo di comunicare immediatamente all'OdV ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata (Amministratore di sistema).

protocolli preventivi di sistema
Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi destinatari
Sistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processi
Sistema disciplinare
Documento programmatico di sicurezza
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale in materia di antiriciclaggio
Clausola l. 136/2010 nei contratti con i subappaltatori e i fornitori
Procedura di nomina del responsabile interno autorizzato a trattare con la PA
Clausola l. 122/2012 nei contratti di appalto e di fornitura
Iscrizione nella *white list* istituita presso la Prefettura

protocolli preventivi specifici
DPS

4 I compiti dell'Organismo di Vigilanza

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'OdV nel documento approvato dall'Amministratore unico e denominato "Parte speciale C – Regolamento dell'Organismo di Vigilanza", in relazione alla prevenzione dei reati di cui alla presente Parte speciale, l'OdV, tra l'altro, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati in tema di criminalità informatica e di trattamento dei dati;
- verificare, in particolare, il rispetto delle regole procedurali e del Modello in ordine ai flussi finanziari aziendali, con riferimento sia ai pagamenti da/verso i terzi sia a quello da/verso le società del Gruppo;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi di flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi *sub* responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività;
- verificare la correttezza della valutazione della congruità economica degli investimenti effettuati dai soggetti aziendali competenti o dai consulenti all'uopo nominati;
- verificare l'applicazione dei punti di controllo previsti nelle procedure riferibili alla prevenzione dei reati contro la P.A. (Parte speciale "E") e ai reati societari (Parte speciale "F"), qualora inerenti le medesime attività "sensibili" o "strumentali" rilevanti ai fini della prevenzione dei reati informatici e di trattamento illecito di dati.