TESSELLIS

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/01 DI TESSELLIS S.P.A.

PARTE SPECIALE 5

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (24-BIS)

aggiornamento marzo 2023

1. DESTINATARI E FINALITÀ DELLA PARTE SPECIALE – DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Sono destinatari (di seguito i "Destinatari") della presente Parte Speciale del Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001 di Tessellis S.p.A. (di seguito la "Società") e si impegnano al rispetto del contenuto dello stesso:

- gli amministratori e i dirigenti della Società (cosidetti soggetti *apicali*);
- i dipendenti della Società (cosiddetti soggetti interni *sottoposti ad altrui direzione*);
- gli amministratori, i dirigenti e i dipendenti delle altre società del Gruppo Tessellis che svolgono continuativamente un servizio per conto o nell'interesse della Società nell'ambito delle attività sensibili identificate nella presente Parte Speciale.

Limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari di specifici obblighi, strumentali ad un'adeguata esecuzione delle attività di controllo interno previste nella presente Parte Speciale, i seguenti soggetti esterni (di seguito i "Soggetti Esterni"):

- i collaboratori, gli agenti e i rappresentanti, i consulenti e in generale i soggetti che svolgono attività di lavoro autonomo nella misura in cui essi operino nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società;
- i fornitori e i partner (anche sottoforma di associazione temporanea di imprese, nonché di *joint-venture*) che operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività cosiddette sensibili per conto o nell'interesse della Società.

Tra i Soggetti Esterni così definiti debbono ricondursi anche coloro che, sebbene abbiano il rapporto contrattuale con altra società del Gruppo, nella sostanza operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società.

La presente Parte Speciale del Modello ha l'obiettivo di indirizzare, mediante regole di condotta, le attività sensibili poste in essere dai Destinatari al fine di

prevenire il verificarsi dei delitti informatici e di trattamento illecito dei dati di cui all'art. 24 bis del D.Lgs. 231/2001.

Nello specifico, essa ha lo scopo di:

- illustrare le fattispecie di reato riconducibili alle tipologie dei reati sopraindicati;
- identificare le attività sensibili ossia quelle attività che la Società pone in essere in corrispondenza delle quali, secondo un approccio di *risk assessment*, la Società stessa ritiene inerenti e rilevanti i rischi-reato, riprendendo il contenuto della "matrice dei rischi", nella quale, per ciascuna funzione, sono state individuate dai relativi responsabili le attività a rischio. Detto documento forma parte integrante di tutte le Parti Speciali del Modello;
- riprendere e specificare i principi generali di comportamento del Modello (i.e. riepilogo, integrazione e/o specificazione delle norme comportamentali del Codice Etico di rilievo; obblighi e divieti; sistema delle procure e deleghe interne rilevanti; etc.);
- illustrare i Protocolli comportamentali, implementati dalla Società al fine di prevenire i rischi-reato in esame, che i Destinatari sono tenuti ad osservare per una corretta applicazione della presente Parte Speciale del Modello;
- riepilogare i riferimenti alle specifiche policies e procedure aziendali finalizzate alla prevenzione dei rischi-reato in esame;
- fornire all'Organismo di Vigilanza gli strumenti operativi per esercitare le necessarie attività di controllo, monitoraggio e di verifica.

2. I DELITTI INFORMATICI E IL TRATTAMENTO ILLECITO DEI DATI DI CUI ALL'ART. 24 BIS DEL D. LGS. 231/01

L'articolo 24 bis del D.Lgs. 231/2001, rubricato "Delitti informatici e trattamento illecito dei dati" così recita:

"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 cento a cinquecento quote.

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

Si tratta dei seguenti reati previsti dal Codice Penale, nel caso in cui la falsità riguardi un documento informatico:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici;
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative;
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti;
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici;
- Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative;
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità;
- Falsità ideologica commessa dal privato in atto pubblico;
- Falsità in registri e notificazioni;
- Falsità in scrittura privata;
- Falsità in foglio firmato in bianco. Atto privato;
- Falsità in foglio firmato in bianco. Atto pubblico;

- Altre falsità in foglio firmato in bianco;
- Uso di atto falso;
- Soppressione, distruzione e occultamento di atti veri;
- Copie autentiche che tengono luogo degli originali mancanti;
- Falsità commesse da pubblici impiegati incaricati di un servizio pubblico;

Ed ancora:

Accesso abusivo ad un sistema informatico o telematico;

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
- Danneggiamento di informazioni, dati e programmi informatici;
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- Danneggiamento dì sistemi informatici o telematici;
- Danneggiamento di sistemi informatici o telematici di pubblica utilità;
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

Ed inoltre del delitto previsto dall'art. 1, comma 11, del D.L. 21 settembre 2019, n. 105, convertito dalla L. 18 novembre 2019, n. 272 in materia di ostacolo ai procedimenti in materia di creazione del perimetro di sicurezza nazionale cibernetica.

Qui di seguito è riportata la lettera degli articoli del Codice Penale che vengono in rilievo per la comprensione di ciascuna fattispecie, accompagnata da una sintetica illustrazione del reato e da una descrizione astratta a titolo esemplificativo delle attività potenzialmente a rischio-reato

(come detto i menzionati reati di falso rilevano ai fini d questa norma nell'ipotesi in cui concernano documenti informatici):

"Art. 476 codice penale. Falsità materiale commessa dal pubblico ufficiale

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."

"Art. 477 codice penale. Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative

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."

"Articolo 478 codice penale. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti

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 a 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.

"Articolo 479 codice penale. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici

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."

"Articolo 480 codice penale. Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative [sotto forma di documento informatico avente efficacia probatoria
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.

"Articolo 481 codice penale. Falsità ideologica in certificati [sotto forma di documento informatico avente efficacia probatoria] commessa da persone esercenti un servizio di pubblica necessità
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 a 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.

"Articolo 482 codice penale. Falsità materiale commessa dal privato [in documento informatico pubblico avente efficacia probatoria
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.

"Articolo 483 codice penale. Falsità ideologica commessa dal privato in atto pubblico
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."

"Articolo 484 codice penale. Falsità in registri e notificazioni
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."

"Articolo 485 codice penale. Falsità in scrittura privata
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.
Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

"Articolo 486 codice penale. Falsità in foglio firmato in bianco. Atto privato
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.
Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito."

"Articolo 487 codice penale. Falsità in foglio firmato in bianco. Atto pubblico
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.

"Articolo 488 codice penale. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali.
Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private."

"Articolo 489 codice penale. Uso di atto falso
Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.
Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno."

"Articolo 490 codice penale. Soppressione, distruzione e occultamento di atti veri
Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute.
Si applica la disposizione del capoverso dell'articolo precedente."

"Articolo 492 codice penale. Copie autentiche che tengono luogo degli originali mancanti
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."

"Articolo 493 codice penale. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico

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."

"Articolo 615-ter codice penale. 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 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.
4) 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."

Articolo 615-quater codice penale. 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 profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a 5.164 euro.

La pena è della reclusione da uno a tre anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui al quarto comma dell'articolo 617-quate

Articolo 615-quinquies codice penale. 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, 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, (3) produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa (4) apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329

Articolo 617-quater codice penale. 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 tre a otto anni se il fatto è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato

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

Articolo 635-bis codice penale. 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 sei mesi a tre anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 [con violenza alla persona o con minaccia] ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Articolo 635-ter codice penale. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 [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.

Articolo 635-quater codice penale. 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 uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 [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.

Articolo 635-quinquies codice penale. Danneggiamento di sistemi informatici o telematici di pubblica utilità
Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 [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.

Articolo 640-quinquies codice penale. 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 € 51,00 a € 1.032,00.

Al fine di comprendere i rischi-reato in esame e meglio valutare gli ambiti dell'organizzazione aziendale nei quali queste fattispecie possono essere compiute, occorre precisare quanto segue.
Le prime fattispecie (dall'art. 476 c.p all'art. 493 c.p.) richiamate in modo esplicito dall'art. 491 bis c.p. riguardano i reati di falso nei documenti informatici. Infatti, l'art. 491-bis c.p. stabilisce che se alcuna delle falsità documentali previste riguarda un documento informatico pubblico o privato

avente efficacia probatoria, di applicano le disposizioni concernenti rispettivamente gli atti pubblici e le scritture private.

In particolare, il bene giuridico tutelato, dalle fattispecie di reato di cui al capo III del titolo VII del codice penale, è la fede pubblica documentale, si tratta di quella particolare fiducia che la collettività ripone sulla veridicità o autenticità di un documento.

Per documento informatico si intende qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; i documenti informatici rilevanti ai fini delle norme in questione sono quelli pubblici o privati, dotati di efficacia probatoria, cioè con firma elettronica qualificata o emessi nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità.

Può trattarsi di qualunque atto scritto, file o altro contenuto di un programma informatico, del quale sia riconoscibile l'autore che in esso si palesa, contenente una dichiarazioni di scienza (esposizione di dati o fatti) o manifestazioni di volontà.

I reati di falso possono avere ad oggetto un atto pubblico oppure di una scrittura privata.

La nozione di atto pubblico, ai fini della tutela penale, è certamente più ampia di quella del codice civile, poiché sono ricompresi non solo i documenti redatti con le debite formalità prescritte dalla legge da un notaio o da un pubblico ufficiale autorizzato ad attribuire pubblica fede al documento, ma vi sono ricompresi tutti i documenti formati da un pubblico ufficiale o da un pubblico impiegato o incaricato di un pubblico servizio e compilato, con le formalità previste dalla legge, al fine di comprovare un fatto giuridico o al fine di attestare fatti da lui compiuti o avvenuti in sua presenza e destinato ad assumere rilevanza giuridica.

La nozione di pubblico ufficiale, incaricato di pubblico servizio ed esercente di un servizio di pubblica necessità sono contenute rispettivamente negli artt. 357, 358 e 359 c.p.

E' pubblico ufficiale colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa. Le prime due attività sono riconducibili

rispettivamente alla produzione di norme e all'esercizio della funzione giurisdizionale (non solo i magistrati, ma anche altri soggetti chiamati a svolgere determinate funzioni, come ausiliari, periti, testimoni etc.). L'attività amministrativa è, invece, quella caratterizzata da una regolamentazione pubblicistica, dalla formazione e manifestazione della volontà della pubblica amministrazione e ha ad oggetto l'esercizio di poteri autoritativi, di certificazione e attestazione e documentazione di attività giuridicamente rilevante.

E' incaricato di pubblico servizio, invece, colui che presta, a qualunque titolo, un servizio pubblico, cioè un'attività diretta a soddisfare finalità pubbliche di utilità sociale, caratterizzata da una disciplina di tipo pubblicistico e dall'assenza dei poteri autoritativi tipici di quest'ultima, da un lato, e dall'esclusione di attività non discrezionali, di mera esecuzione di compiti impartiti dall'autorità e di prestazione di opera meramente materiale, dall'altro.

L'esercente di un servizio di pubblica necessità è il privato che, qualora non rientri nelle prime due categorie, eserciti una professione, sanitaria, forense o altra professione per cui è necessaria una particolare abilitazione pubblica, ovvero il privato chiamato a svolgere un servizio dichiarato di pubblica necessità mediante un atto della pubblica amministrazione.

Occorre sottolineare che i reati di cui al capo III del titolo VII del codice penale si possono distinguere a seconda che vengano commessi da soggetti che rivestano una particolare qualifica (c.d. reati propri) ovvero da chiunque (c. d. reati comuni) nel modo seguente:

1) Falsità commesse da pubblico ufficiale o da impiegato incaricato di pubblico servizio (reati propri):

1a) materiale in atti pubblici (art. 476c.p., con pena aggravata se è atto fidefacente), in certificati o autorizzazioni (art. 477 c.p.), in copie autentiche o attestati (art. 478 c.p.);

1b) ideologica in atti pubblici (art. 479 c.p.), in certificati o autorizzazioni (art. 480 c.p.)

2) Falsità commesse dal privato (reati comuni) :

2a) materiale in atti pubblici, in certificati, o autorizzazioni, in copie autentiche o attestati (art. 482 c.p., con riduzione di un terzo delle pene rispetto al fatto commesso da un pubblico ufficiale);

2b) ideologica in atti pubblici (art. 483 c.p.).

È doveroso sottolineare che anche un soggetto che non riveste le qualifiche richieste per la commissione dei reati propri può commettere il reato in concorso con il pubblico ufficiale o l'incaricato di un pubblico servizio.

Infine occorre evidenziare che l'art. 602 ter c.p. ha introdotto una circostanza aggravante, che determina un aumento di pena da 1/3 ad 1/2 nell'ipotesi in cui i reati di falso vengano commessi per realizzare o agevolare i reati di cui agli articoli 600, 601, 602 c.p. (riduzione in schiavitù, tratta di persone, acquisto e alienazione di schiavi).

Per quanto attiene ai reati informatici in senso stretto (dall'art. 615 ter all'art. 615 quinquies e dall'art. 617 quater e 617 quinquies dal 635 bis al 635 sexies e dall'art. 640 quinquies c.p.) occorre precisare che per le fattispecie indicate che vanno dall'art. 615 ter all'art. 617 sexies c.p. il bene giuridico tutelato consiste nella riservatezza delle notizie e delle comunicazioni trasmesse tramite mezzi informatici e vengono presi in considerazione non solo i sistemi informatici complessi ma anche i singoli *personal computers*. l'ipotesi di reato di cui all'art. 617 sexies c.p. tutela l'interesse giuridico al mantenimento della genuinità e veridicità delle comunicazioni informatiche e telematiche.

Le fattispecie di reato contenute negli artt. 635 bis, ter, quater c.p. tutela l'interesse giuridico dell'integrità del patrimonio e dei sistemi informatici.

La distinzione operata tra reati informatici in senso stretto e reati di falso richiamati dall'art. 491 bis si riverbera in qualche modo anche sul regime sanzionatorio. Infatti, nei casi di condanna per uno dei delitti di falso indicati dall'art. 491 bis oltreché nell'ipotesi di cui all'art. 640 quinquies si applica all'ente una sanzione pecuniaria fino a 400 quote e le seguenti sanzioni interdittive: divieto di contrarre con la P.A.; l'esclusione da agevolazioni

finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi oltreché il divieto di pubblicizzare beni o servizi.

Nei casi di condanna per uno dei reati informatici in senso stretto le sanzioni pecuniarie sono comprese tra 100 e 500 quote e si applicano le seguenti sanzioni interdittive: sospensione o revoca delle autorizzazioni licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi e nei casi più gravi (artt. 615 ter, 617 quater e quinquies, 635 bis, ter, quater, quinquies c.p.) si giunge fino alla interdizione dall'esercizio dell'attività.

Come ricordato, l'art. 1, comma 11, del D.L. 105/2019, convertito dalla L. 272/2919, ha introdotto tra i reati rilevanti ai sensi dell'art. 24 bis del D. Lgs. 231/2001anche quello di ostacolo ai procedimenti in materia di creazione del perimetro di sicurezza nazionale cibernetica. Si riporta di seguito il testo normativo:

Art. 1 Perimetro di sicurezza nazionale cibernetica

1. Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attivita' civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale,e' istituito il perimetro di sicurezza nazionale cibernetica.

2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):

a) sono individuati le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati di cui al comma 1, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; alla predetta individuazione, fermo restando

che per gli Organismi diinformazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri:

1) il soggetto esercita una funzione essenziale dello Stato,ovvero assicura un servizio essenziale per il mantenimento di attivita' civili, sociali o economiche fondamentali per gli interessi dello Stato;

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale;

b) sono definiti i criteri in base ai quali i soggetti di cui alla precedente lettera a) predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al presente comma, i soggetti pubblici e quelli di cui all'articolo 29 del codicedell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonche' quelli privati, individuati ai sensi della lettera a) trasmettono tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico;la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico inoltrano gli elenchi di rispettiva pertinenza alDipartimento delle informazioni per la sicurezza, anche per le attivita' di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonche'all'organo del Ministero dell'interno per la sicurezza e la regolarita' dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

3. Entro dieci mesi dalla data di entrata in vigore della legge diconversione del presente decreto, con decreto del Presidente delConsiglio dei ministri, che

ne disciplina altresi' i relativi termini e modalita' attuative, adottato su proposta del CISR:

a) sono definite le procedure secondo cui i soggetti individuati ai sensi del comma 2, lettera a), notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera b), al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, che inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attivita' demandate al Nucleo per la sicurezza cibernetica; il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche cosi' ricevute all'organodel Ministero dell'interno per la sicurezza e la regolarita' dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonche' alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato;

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b), relative:

1) alle politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrita' delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuita' del servizio;

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.

4. All'elaborazione delle misure di cui al comma 3, lettera b), provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

5. Per l'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si procede secondo le medesime modalita' di cui ai commi 2, 3 e 4 con cadenza almeno biennale.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, sono disciplinati le procedure, le modalita' e i termini con cui:

a) fatti salvi i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni e di servizi ICT cui sia indispensabile procedere in sede estera, i soggetti di cui al comma 2, lettera a), che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei serviziinformatici di cui al comma 2, lettera b), diversi da quelli necessari per lo svolgimento delle attivita' di prevenzione,accertamento e repressione dei reati, ne danno comunicazione alCentro di valutazione e certificazione nazionale (CVCN), istituitopresso il Ministero dello sviluppo economico, che, sulla base di unavalutazione del rischio, anche in relazione all'ambito di impiego ein un'ottica di gradualita', puo', entro trenta giorni, imporrecondizioni e test di hardware e software; in tale ipotesi, i relativibandi di gara e contratti sono integrati con clausole checondizionano, sospensivamente ovvero risolutivamente, l'affidamentoovvero il contratto al rispetto delle condizioni e all'esitofavorevole dei test disposti dal CVCN; per le forniture di beni,sistemi e servizi ICT da impiegare su reti, sistemi informativi eservizi informatici del Ministero della difesa, individuati ai sensidel comma 2, lettera

b), il predetto Ministero procede, nell'ambitodelle risorse umane e finanziarie disponibili a legislazione vigentee senza nuovi o maggiori oneri a carico della

finanza pubblica, incoerenza con quanto previsto dal presente decreto, attraverso unproprio Centro di valutazione in raccordo con la Presidenza delConsiglio dei ministri e il Ministero dello sviluppo economico per iprofili di rispettiva competenza; resta fermo che per lo svolgimentodelle attivita' di prevenzione, accertamento e di repressione deireati e nei casi in cui si deroga all'obbligo di cui alla presentelettera, sono utilizzati reti, sistemi informativi e serviziinformatici conformi ai livelli di sicurezza di cui al comma 3,lettera b), qualora non incompatibili con gli specifici impieghi cuiessi sono destinati;

b) i soggetti individuati quali fornitori di beni, sistemi eservizi destinati alle reti, ai sistemi informativi e ai serviziinformatici di cui al comma 2, lettera b), assicurano al CVCN e,limitatamente agli ambiti di specifica competenza, al Centro divalutazione operante presso il Ministero della difesa, la propriacollaborazione per l'effettuazione delle attivita' di test di cuialla lettera a) del presente comma, sostenendone gli oneri; il CVCNsegnala la mancata collaborazione al Ministero dello sviluppoeconomico, in caso di fornitura destinata a soggetti privati, o allaPresidenza del Consiglio dei ministri, in caso di fornitura destinataa soggetti pubblici ovvero a quelli di cui all'articolo 29 del codicedi cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltratealtresi' alla Presidenza del Consiglio dei ministri le analoghesegnalazioni del Centro di valutazione del Ministero della difesa;

c) la Presidenza del Consiglio dei ministri, per i profili dipertinenza dei soggetti pubblici e di quelli di cui all'articolo 29del codice dell'Amministrazione digitale di cui al decretolegislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2,lettera a), e il Ministero dello sviluppo economico, per i soggettiprivati di cui alla medesima lettera, svolgono attivita' di ispezionee verifica in relazione a quanto previsto dal comma 2, lettera b),dal comma 3 e dalla lettera a) del presente comma e senza che cio'comporti accesso a dati o metadati personali e amministrativi,impartendo, se necessario, specifiche prescrizioni; per le reti, isistemi informativi e i servizi informatici di cui al comma 2,lettera b), connessi alla funzione di prevenzione e repressione deireati, alla tutela dell'ordine e della sicurezza pubblica e alladifesa e sicurezza militare dello

Stato, le attivita' di ispezione everifica sono svolte, nell'ambito delle risorse umane e finanziariedisponibili a legislazione vigente e senza nuovi o maggiori oneri acarico della finanza pubblica, dalle strutture specializzate in temadi protezione di reti e sistemi, nonche' in tema di prevenzione e dicontrasto del crimine informatico, delle amministrazioni da cuidipendono le Forze di polizia e le Forze armate, che ne comunicanogli esiti alla Presidenza del Consiglio dei ministri per i profili dicompetenza.

7. Nell'ambito dell'approvvigionamento di prodotti, processi,servizi ICT e associate infrastrutture destinati alle reti, aisistemi informativi e per l'espletamento dei servizi informatici dicui al comma 2, lettera b), il CVCN assume i seguenti compiti:

a) contribuisce all'elaborazione delle misure di sicurezza di cuial comma 3, lettera b), per cio' che concerne l'affidamento diforniture di beni, sistemi e servizi ICT;

b) ai fini della verifica delle condizioni di sicurezza edell'assenza di vulnerabilita' note, anche in relazione all'ambito diimpiego, svolge le attivita' di cui al comma 6, lettera a), dettando,se del caso, anche prescrizioni di utilizzo al committente; a talifini il CVCN si avvale anche di laboratori dallo stesso accreditatisecondo criteri stabiliti da un decreto del Presidente del Consigliodei ministri, adottato entro dieci mesi dalla data di entrata invigore della legge di conversione del presente decreto, su propostadel CISR, impiegando, per le esigenze delle amministrazioni centralidello Stato, quelli eventualmente istituiti, senza nuovi o maggiorioneri a carico della finanza pubblica, presso le medesimeamministrazioni;

c) elabora e adotta, previo conforme avviso dell'organismotecnico di supporto al CISR, schemi di certificazione cibernetica,laddove, per ragioni di sicurezza nazionale, gli schemi dicertificazione esistenti non siano ritenuti adeguati alle esigenze ditutela del perimetro di sicurezza nazionale cibernetica.

8. I soggetti di cui agli articoli 12 e 14 del decreto legislativo18 maggio 2018, n. 65, e quelli di cui all'articolo 16-ter, comma 2,del codice delle

comunicazioni elettroniche di cui al decretolegislativo 1° agosto 2003, n. 259, inclusi nel perimetro disicurezza nazionale cibernetica:

a) osservano le misure di sicurezza previste, rispettivamente,dai predetti decreti legislativi, ove di livello almeno equivalente aquelle adottate ai sensi del comma 3, lettera b), del presentearticolo; le eventuali misure aggiuntive necessarie al fine diassicurare i livelli di sicurezza previsti dal presente decreto sonodefinite dalla Presidenza del Consiglio dei ministri, per i soggettipubblici e per quelli di cui all'articolo 29 del codice di cui aldecreto legislativo 7 marzo 2005, n. 82, individuati ai sensi delcomma 2, lettera a), del presente articolo, e dal Ministero dellosviluppo economico per i soggetti privati di cui alla medesimalettera, avvalendosi anche del CVCN; il Ministero dello sviluppoeconomico e la Presidenza del Consiglio dei ministri si raccordano,ove necessario, con le autorita' competenti di cui all'articolo 7 deldecreto legislativo 18 maggio 2018, n. 65;

b) assolvono l'obbligo di notifica di cui al comma 3, lettera a),che costituisce anche adempimento, rispettivamente, dell'obbligo dinotifica di cui agli articoli 12 e 14 del decreto legislativo 18maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensidell'articolo 16-ter del codice di cui al decreto legislativo 1°agosto 2003, n. 259, e delle correlate disposizioni attuative; a talfine, oltre a quanto previsto dal comma 3, lettera a), anche inrelazione alle disposizioni di cui all'articolo 16-ter del codice dicui al decreto legislativo 1° agosto 2003, n. 259, il CSIRT italianoinoltra le notifiche ricevute ai sensi del predetto comma 3, letteraa), all'autorita' competente di cui all'articolo 7 del decretolegislativo 18 maggio 2018, n. 65.

9. Salvo che il fatto costituisca reato:

a) il mancato adempimento degli obblighi di predisposizione e diaggiornamento dell'elenco delle reti, dei sistemi informativi e deiservizi informatici di cui al comma 2, lettera b), e' punito con lasanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

b) il mancato adempimento dell'obbligo di notifica di cui alcomma 3, lettera a), nei termini prescritti, e' punito con lasanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

c) l'inosservanza delle misure di sicurezza di cui al comma 3,lettera b), e' punita con la sanzione amministrativa pecuniaria daeuro 250.000 a euro 1.500.000;

d) la mancata comunicazione di cui al comma 6, lettera a), neitermini prescritti, e' punita con la sanzione amministrativapecuniaria da euro 300.000 a euro 1.800.000; e) l'impiego di prodotti e servizi sulle reti, sui sistemiinformativi e l'espletamento dei servizi informatici di cui al comma2, lettera b), in violazione delle condizioni imposte dal CVCN o inassenza del superamento dei test di cui al comma 6, lettera a), e'punito con la sanzione amministrativa pecuniaria da euro 300.000 aeuro 1.800.000;

f) la mancata collaborazione per l'effettuazione delle attivita'di test di cui al comma 6, lettera a), da parte dei soggetti di cuial medesimo comma 6, lettera b), e' punita con la sanzioneamministrativa pecuniaria da euro 250.000 a euro 1.500.000;

g) il mancato adempimento delle prescrizioni indicate dalMinistero dello sviluppo economico o dalla Presidenza del Consigliodei ministri in esito alle attivita' di ispezione e verifica svolteai sensi del comma 6, lettera c), e' punito con la sanzioneamministrativa pecuniaria da euro 250.000 a euro 1.500.000;

h) il mancato rispetto delle prescrizioni di cui al comma 7,lettera b), e' punito con la sanzione amministrativa pecuniaria daeuro 250.000 a euro 1.500.000.

10. In caso di inottemperanza alle condizioni o in assenzadell'esito favorevole dei test di cui al comma 6, lettera a), il contratto non produce ovvero cessa di produrre effetti, secondo quanto previsto dalle condizioni ad esso apposte. L'esecuzionecomunque effettuata in violazione di quanto previsto al primo periodocomporta, oltre alla sanzione di cui al comma 9, lettera e), lasanzione amministrativa accessoria della incapacita' ad assumereincarichi di direzione, amministrazione e controllo nelle personegiuridiche e nelle imprese, per un periodo di tre anni a decorreredalla data di accertamento della violazione.

11. Chiunque, allo scopo di ostacolare o condizionarel'espletamento dei procedimenti di cui al comma 2, lettera b), o alcomma 6, lettera a), o delle

attivita' ispettive e di vigilanzapreviste dal comma 6, lettera c), fornisce informazioni, dati oelementi di fatto non rispondenti al vero, rilevanti per lapredisposizione o l'aggiornamento degli elenchi di cui al comma 2,lettera b), o ai fini delle comunicazioni di cui al comma 6, letteraa), o per lo svolgimento delle attivita' ispettive e di vigilanza dicui al comma 6), lettera c) od omette di comunicare entro i terminiprescritti i predetti dati, informazioni o elementi di fatto, e'punito con la reclusione da uno a cinque anni e all'ente,responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231,si applica la sanzione pecuniaria fino a quattrocento quote.

12. Le autorita' competenti per l'accertamento delle violazioni eper l'irrogazione delle sanzioni sono la Presidenza del Consiglio deiministri, per i soggetti pubblici e per i soggetti di cuiall'articolo 29 del codice di cui al decreto legislativo 7 marzo2005, n. 82, individuati ai sensi del comma 2, lettera a), delpresente articolo, e il Ministero dello sviluppo economico, per isoggetti privati di cui alla medesima lettera.

13. Ai fini dell'accertamento e dell'irrogazione delle sanzioniamministrative di cui al comma 9, si osservano le disposizionicontenute nel capo I, sezioni I e II, della legge 24 novembre 1981,n. 689.

14. Per i dipendenti dei soggetti pubblici individuati ai sensi delcomma 2, lettera a), la violazione delle disposizioni di cui alpresente articolo puo' costituire causa di responsabilita'disciplinare e amministrativo-contabile.

15. Le autorita' titolari delle attribuzioni di cui al presentedecreto assicurano gli opportuni raccordi con il Dipartimento delleinformazioni per la sicurezza e con l'organo del Ministerodell'interno per la sicurezza e la regolarita' dei servizi ditelecomunicazione, quale autorita' di contrasto nell'esercizio delleattivita' di cui all'articolo 7-bis del decreto-legge 27 luglio 2005,n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155.

16. La Presidenza del Consiglio dei ministri, per lo svolgimentodelle funzioni di cui al presente decreto puo' avvalersi dell'Agenziaper l'Italia Digitale (AgID) sulla base di apposite convenzioni,nell'ambito delle risorse finanziarie e umane disponibili alegislazione vigente, senza nuovi o maggiori oneri per la finanzapubblica.

17. Al decreto legislativo 18 maggio 2018, n. 65, sono apportate leseguenti modificazioni: a) all'articolo 4, comma 5, dopo il primo periodo e' aggiunto ilseguente: «Il Ministero dello sviluppo economico inoltra tale elenco alpunto di contatto unico e all'organo del Ministero dell'interno perla sicurezza e la regolarita' dei servizi di telecomunicazione, dicui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144,convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.»; b) all'articolo 9, comma 3, le parole «e il punto di contattounico» sono sostituite dalle seguenti: «, il punto di contatto unico e l'organo del Ministerodell'interno per la sicurezza e la regolarita' dei servizi ditelecomunicazione, di cui all'articolo 7-bis del decreto-legge 27luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31luglio 2005, n. 155,».

18. Gli eventuali adeguamenti alle prescrizioni di sicurezzadefinite ai sensi del presente articolo, delle reti, dei sistemiinformativi e dei servizi informatici delle amministrazionipubbliche, degli enti e degli operatori pubblici di cui al comma 2,lettera a), sono effettuati con le risorse finanziarie disponibili alegislazione vigente. 19. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui ai commi 6 e 7 e' autorizzata la spesa di euro 3.200.000per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020al 2023 e di euro 750.000 annui a decorrere dall'anno 2024.

Come ricordato la fattispecie è stata inclusa nel catalogo dei reati presupposto nell'ambito dei reati informatici previsti dall'articolo 24-bis, comma 3, del D. Lgs. 231/01.

La norma punisce chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti o delle attività ispettive e di vigilanza previste in materia di istituzione del perimetro di sicurezza nazionale cibernetica, fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi o ai fini delle comunicazioni relative, o per lo svolgimento delle attività ispettive e di vigilanza od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

Il perimetro di sicurezza nazionale cibernetica è istituito al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

La disposizione è finalizzata ad assicurare la completezza e la veridicità delle informazioni relative al perimetro di sicurezza cibernetica.

3. LE MACROATTIVITÀ SENSIBILI EX ART. 24 BIS DEL D.LGS. 231/2001

Con riferimento al rischio di commissione dei reati illustrati nel paragrafo precedente (di cui all'articolo 24 bis del D.Lgs. 231/2001) e ritenuti rilevanti a seguito del *risk assessment* eseguito internamente, la Società valuta come "sensibili" le seguenti macroattività che essa pone in essere per mezzo dei Destinatari della presente Parte Speciale anche eventualmente in collaborazione con i Soggetti Esterni:

- Gestione delle attività di accesso ai sistemi informatici/telematici e applicazioni (autenticazione, account e profili);
- Attività di manutenzione dei sistemi informatici/telematici e di accesso alle applicazioni;
- Gestione e manutenzione hardware;
- Gestione e manutenzione software;
- Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT;
- Attività di creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;

- Attività di trasmissione di dati e informazioni all'Autorità Giudiziaria (e.g. tabulati telefonici);
- Operazioni dirette a consentire all'Autorità Giudiziaria, anche a mezzo degli Organi di P.G., le intercettazioni di comunicazione telefoniche o telematiche;
- Attività di trasmissione di dati e informazioni alle Autorità Governative in materia di perimetro nazionale di sicurezza cibernetica;

Le macroattività sensibili come sopra identificate, meglio specificate, funzione per funzione, nella "*matrice delle attività a rischio*" e fatta salva l'integrazione delle stesse in fase di implementazione, nonché, in divenire, ad opera dell'OdV o delle singole funzioni in collaborazione con l'OdV medesimo, rilevano anche quando esse sono svolte continuativamente dagli amministratori, i dirigenti e i dipendenti della Società per conto o nell'interesse di un'altra società del Gruppo Tessellis. Risultano, pertanto, applicabili anche in tali ipotesi le regole di condotta ad esse associate sotto forma di principi generali di comportamento, protocolli nonché flussi informativi; questi ultimi opportunamente indirizzati all'Organismo di Vigilanza della società del Gruppo Tessellis beneficiaria del servizio.

4. I REATI EX ART. 24 BIS DEL D.LGS. 231/2001 – PROTOCOLLI COMPORTAMENTALI

Ai fini dell'attuazione delle regole comportamentali e dei divieti elencati nel precedente capitolo, i Destinatari della presente Parte Speciale del Modello, oltre a rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale del presente Modello, devono rispettare i seguenti protocolli comportamentali qui di seguito descritti, posti a presidio dei rischi-reato sopra identificati (art. 24 bis del D.Lgs. 231/2001) e riferibili alle attività sensibili.

I protocolli comportamentali prevedono obblighi (Area del fare) e/o divieti specifici (Area del non fare) che i Destinatari della presente Parte Speciale del Modello devono rispettare, uniformando la propria condotta ad essi in

corrispondenza delle attività sensibili sopra rilevate. Tali principi riprendono, specificandole o, se del caso, integrandole, le norme del Codice Etico e della Parte Generale del Modello. In forza di apposite pattuizioni contrattuali, i principi in esame si applicano anche ai Soggetti Esterni coinvolti nello svolgimento delle attività sensibili identificate.

Nel presente capitolo, è delineato, infine, il sistema delle procure e deleghe in essere per la parte dello stesso che contribuisce alla gestione dei rischi-reato inerenti le attività sensibili in esame, quello delle procedure e dei flussi informativi nei confronti dell'OdV.

4.1 AREA DEL FARE

Tutte le attività sensibili devono essere svolte conformandosi alle leggi vigenti, alle norme del Codice Etico, ai principi generali di comportamento enucleati sia nella Parte Generale che nella Parte Speciale del presente Modello, nonché ai protocolli, ale policies e procedure definite e implementate nell'ambito del Sistema ISO 27001 di cui si dirà appresso (e alle eventuali altre procedure organizzative esistenti) posti a presidio dei rischi-reato identificati.

La Società è consapevole del fatto che, per l'attività svolta, la protezione delle infrastrutture IT, dei sistemi informatici/telematici e delle applicazioni, dei dati e delle informazioni ivi contenuti presentano particolare criticità.

In particolare, la Società è consapevole che, per il raggiungimento dei propri obiettivi di *business* e nell'interesse dei suoi *stakeholders*, è necessario che, mediante un approccio globale, sia garantita la sicurezza delle informazioni, siano attribuite espressamente e formalmente le responsabilità per la sicurezza delle informazioni, venga valutato il livello di sicurezza dei sistemi informatici/telematici con conseguente valutazione e rivalutazione costante del livello di rischio, gestione del rischio medesimo (con l'obiettivo di eliminarlo, mitigarlo o ridurlo comunque al livello ritenuto accettabile) mediante apposite policies, procedure finalizzate alla prevenzione attiva e di rilevamento degli incidenti di sicurezza informatica, nonché adeguata attività di controllo e monitoraggio.

Per tale motivo la Società si è dotata di particolari policies e procedure basate sulle *best practices* internazionali e in conformità agli standard internazionali di *Information Security Management System* ISO/IEC 27001.

Tale sistema fornisce un modello per la definizione, l'implementazione, il controllo, il monitoraggio e il miglioramento continuo del livello di affidabilità e di funzionamento dei sistemi informatici/telematici aziendali, della protezione delle infrastrutture IT, del patrimonio informativo aziendale e di tutti i dati, ivi comprese le credenziali di accesso, di dipendenti, clienti/utenti e terzi soggetti.

I vantaggi di implementazione di questo sistema di gestione "olistica" della sicurezza informatica/telematica, rappresentati, come detto, da una riduzione dei rischi in termini di probabilità di verificazione e/o di impatto di "incidenti", costituiscono un adeguato presidio anche con riferimento al rischio di commissione dei reati di cui alla presente Parte Speciale.

Per tale motivo, per il raggiungimento degli obiettivi di prevenzione relativi a questa Parte Speciale, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare e attenersi con il massimo rigore a tutte le policies aziendali e procedure facenti parte dell'ISMS basato sullo standard ISO/IEC 27001.

In particolare:

- la Società definisce, aggiorna, approva formalmente le *policies* aziendali e le procedure in materia di sicurezza informatica/telematica e ne assicura la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione;
- quanto detto al punto precedente, con particolare riferimento a:
  - ✓ piano di business continuity, ivi compreso il disaster recovery;
  - ✓ back up (modalità, frequenza, etc.);
  - ✓ accesso remoto da parte di terzi soggetti;
  - ✓ requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e formalizzazione e tracciatura di tutte autorizzazioni, registrazioni, modifiche e cancellazioni di

profili di autenticazione, ivi compresi quelli di clienti/utenti; divieti o limitazioni di accesso a sistemi informatici/telematici, applicazioni o reti;

- ✓ generazione, protezione e conservazione dei "log" di sistema, di applicazione e di database;
- ✓ concessione di adeguati livelli di privilegio;
- ✓ formale assegnazione di particolari livelli di privilegio e formale assunzione della relativa responsabilità;
- ✓ controllo e tracciatura di variazioni significative (quantitative e qualitative) di dati e informazioni e altri anomali inserimenti, modificazioni o cancellazioni;
- ✓ implementazione, gestione e manutenzione di reti (attribuzione di responsabilità; controlli finalizzati a garantire la separazione delle singole teri, la protezione e la riservatezza dei dati e delle informazioni ivi contenute, o in transito (vulnerability assessment, penetration test etc.); monitoraggio del traffico;
- ✓ gestione e manutenzione hardware (ivi compresi inventario e divieti o limitazioni di utilizzo);
- ✓ installazione, gestione e manutenzione software e banche dati (ivi compresi inventario, verifica di validità, operatività, scadenza e limiti di licenze e certificazioni di software e banche dati di terzi o loro utilizzo in conformità alle norme sul diritto d'autore e altri diritti connessi al suo esercizio; divieti o limitazioni di installazione/utilizzo);
- ✓ regolamentazione accesso fisico ai locali in cui risiedono le infrastrutture IT (attribuzione di facoltà di accesso, misure di sicurezza e di vigilanza e assunzione della relativa responsabilità);
- ✓ creazione, protezione mediante crittografia (ivi compresa la definizione, distribuzione/segretezza, sostituzione e archiviazione dei relativi algoritmi e chiavi), emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti

informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;

- ✓ regolamentazione dell'utilizzo della firma digitale con formale attribuzione e formale assunzione della relativa responsabilità.
- ✓ Gestione delle attività di trasmissione di dati e informazioni (e.g. tabulati telefonici) all'Autorità Giudiziaria, con particolare riferimento all'individuazione e al formale incarico delle risorse a ciò delegate e all'impegno delle stesse a non divulgare a terzi alcuna notizia in merito alla richiesta dell'Autorità Giudiziaria né il contenuto dei dati e informazioni oggetto della predetta trasmissione;
- ✓ Gestione delle operazioni tecniche dirette a consentire all'Autorità Giudiziaria, anche a mezzo degli Organi di P.G., operazioni di intercettazione di comunicazioni informatiche o telematiche, con particolare riferimento all'individuazione e al formale incarico delle risorse a ciò delegate e all'impegno delle stesse a non divulgare a terzi alcuna notizia in merito alle intercettazioni o al contenuto delle stesse.
- ✓ Nomina di amministratore/i di sistema e amministratore/i di database con atto formale, definizione di compiti e attribuzioni ed espressa assunzione della relativa responsabilità;
- ✓ Attività di trasmissione di dati e informazioni alle Autorità Governative in materia di perimetro nazionale di sicurezza cibernetica;

Per quanto attiene alla sicurezza dei dati personali di tutti i soggetti con i quali intrattiene rapporti a vario titolo, la Società ha adeguato il suo sistema organizzativo ai principi e obblighi di cui alla normativa vigente in materia e, in particolare, del Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), ivi compresa la nomina del Responsabile del trattamento, e garantisce che il trattamento dei dati medesimi si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché

della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

I sistemi informatici/telematici, i programmi informatici, nonché policies e procedure IT della Società garantiscono che il trattamento dei dati personali avvenga nel rispetto dei principi e norme di cui sopra, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

4.2 Area Del Non Fare

E' fatto espresso divieto ai Destinatari di porre in essere comportamenti in violazione o comunque non conformi alle policies e procedure definite e implementate nell'ambito dell'ISMS basato sullo standard ISO/IEC 27001, nonché comportamenti tali da integrare, anche solo potenzialmente e anche a titolo di concorso o di tentativo, le fattispecie di reato di cui alla presente Parte Speciale.

In particolare, premesso che:

- la definizione di "concorso" di persone del reato data dal codice penale ricomprende nel "contributo obiettivamente rilevante" ogni forma di collaborazione, anche "morale", idonea, cioè, determinare o a rafforzare il proposito criminoso di altri soggetti (e.g. istigazione),
- per documento informatico deve intendersi qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, di natura pubblica o privata, qualora dotato di "efficacia probatoria", cioè con firma elettronica qualificata o emesso nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità,

ai Destinatari è fatto divieto di:

- Formare o concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare documenti informatici falsi o alterare atti veri;
- Contraffare o alterare o concorrere con un p.u. o i.p.s. nel contraffare o alterare certificati o autorizzazioni amministrative contenute in un documento informatico, o a contraffare o alterare le condizioni richieste per la loro validità;

- Concorrere con un p.u. o i.p.s. a formare e rilasciare una copia in forma legale su documento informatico di un atto pubblico o privato inesistente o una copia diversa dall'originale;
- Contraffare o concorrere con un p.u. o i.p.s. nel contraffare un attestato;
- Concorrere con un p.u. o i.p.s. nella falsa attestazione da parte di quest'ultimo in un documento informatico che un fatto è stato da lui compiuto o che è avvenuto in sua presenza, ovvero nell'attestazione da parte dello stesso in un documento informatico di aver ricevuto dichiarazioni non rese o nell'omissione o alterazione di dichiarazioni da lui ricevute;
- Concorrere con un p.u. o i.p.s. nella falsa attestazione, in atti, in certificati o autorizzazioni amministrative sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità;
- Concorrere con un esercente una professione sanitaria o forense o altro servizio di pubblica necessità nell'attestare falsamente, in un certificato sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità;
- Attestare falsamente, oralmente o per iscritto, ad un p.u. in un atto pubblico, sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità;
- Scrivere o lasciare scrivere false indicazioni nelle registrazioni, sotto forma di documento informatico, soggette all'ispezione dell'Autorità di P.S. o nelle notificazioni, sotto forma di documento informatico, alla stessa Autorità, riguardanti operazioni industriali, commerciali o professionali;
- Formare in tutto o in parte scritture private false, sotto forma di documento informatico, o alterazione di scritture private vere, utilizzandole o lasciando che altri le utilizzino;
- Scrivere o far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un

atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino;

- Scrivere o far scrivere, ovvero concorrere con un p.u. nello scrivere o nel far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello a cui il p.u. stesso era obbligato o autorizzato;
- Distruggere, sopprimere, occultare in tutto o in parte una scrittura privata o un atto pubblico veri, sotto forma di documento informatico;
- Utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo.

E'altresì vietato:

- Introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza;
- Procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo;
- Procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione apparecchiature dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico o le informazioni, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento;
- Intercettare illegittimamente o abusivamente, impedire, interrompere fraudolentemente o illegittimamente comunicazioni informatiche o telematiche.
- Installare illegittimamente o abusivamente apparecchiature atte ad intercettare, impedire, interrompere comunicazioni informatiche o telematiche;

- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui, o utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- Distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero ostacolarne gravemente il funzionamento mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi;
- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o introduzione o trasmissione di dati, informazioni o programmi al fine distruggere, danneggiare, o causare l'inutilizzabilità in tutto o in parte di sistemi informatici o telematici ovvero al fine di ostacolarne gravemente il loro funzionamento.

4.3 Sistema Di Deleghe E Procure

Il sistema di deleghe e procure concorre insieme agli altri strumenti del presente Modello ai fini della prevenzione dei rischi-reato nell'ambito delle attività sensibili identificate.

La "procura" è il negozio giuridico unilaterale con cui la Società attribuisce poteri di rappresentanza nei confronti dei terzi.

Per "delega" si intende qualsiasi atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

I responsabili di funzione per lo svolgimento dei loro incarichi sono dotati di "*procura funzionale*" o "*delega*" formalizzata e scritta, di estensione adeguata e coerente con le funzioni, le responsabilità e i poteri attribuiti agli stessi titolari. Tutte le procure e deleghe conferite fissano espressamente per natura e/o limite di importo, l'estensione dei poteri di rappresentanza o di quelli delegati.

I responsabili di funzione, riguardo alle attività sensibili da queste ultime svolte, hanno l'onere di assicurare che tutti coloro (i Destinatari e eventualmente anche i Soggetti Esterni) che agiscono per conto della Società

e, soprattutto, che impegnano legalmente la Società, intrattenendo rapporti con la P.A. o altri soggetti pubblici siano dotati di apposita procura o delega.

Le procure e le deleghe, devono essere predisposte dall'Ufficio Legale, o comunque sottoposte all'approvazione dello stesso; devono trasferire attribuzioni, poteri e responsabilità nei limiti previsti dalle norme giuridiche vigenti e applicabili e, in particolare, non devono violare disposizioni normative inderogabili; devono essere coerenti con il Sistema di Controllo Interno, con il Codice Etico e con il Modello; definiscono in modo specifico ed inequivoco i poteri del procuratore o del delegato e il soggetto cui quest'ultimo riporta. I poteri gestionali assegnati e la loro attuazione sono coerenti con gli obiettivi aziendali e la struttura organizzativa della Società.

La Società è dotata di organigrammi e comunicazioni organizzative (adeguatamente divulgate all'interno della Società e nei confronti delle altre società del Gruppo) per mezzo delle quali sono:

- delimitati i ruoli, con una descrizione dei compiti di ciascuna funzione e dei relativi attribuzioni e poteri;
- descritte le linee di riporto.

5. FLUSSI INFORMATIVI IN FAVORE DELL'ODV

Al fine di fornire all'Organismo di Vigilanza gli strumenti per esercitare le sue attività di monitoraggio e di verifica puntuale della efficace esecuzione dei controlli previsti dal presente Modello e, in particolare, dalla presente Parte Speciale, nelle procedure sono descritti i flussi informativi che devono essere assicurati al predetto Organismo, in conformità a quanto disposto nella Parte Generale del Modello medesimo. In particolare, a prescindere dagli altri obblighi di segnalazione, tutti i soggetti interessati sono tenuti a comunicare il manifestarsi di eventi legati al rischio-reato e ai controlli attesi. Lo strumento di comunicazione è rappresentato prevalentemente da una e-mail da inviarsi all'indirizzo organismodivigilanza@it.tiscali.com con la specificazione nell'oggetto del reference del flusso informativo cui si riferisce la comunicazione medesima.

6. POLICIES E PROCEDURE A PRESIDIO DEI RISCHI-REATO

La Società ha definito, implementato e diffuso policies e procedure nell'ambito del suo sistema di gestione della sicurezza dei sistemi informatici/telematici, basato sullo standard ISO/IEC 27001 e sulle *best practices* internazionali.

Tali procedure costituiscono adeguati presidi e strumenti di gestione del rischio con riferimento alle tipologie di reato di cui alla presente Parte Speciale.

La Società, comunque, definisce, implementa e diffonde un organigramma contenente gli ambiti e le responsabilità di ciascuna funzione, nonché, ove necessario, ulteriori *policies* e procedure aziendali in materia di sicurezza dei sistemi di cui sopra, ad integrazione di quelle esistenti, che si aggiungono - unitamente alle indicazioni sopra fornite - a costituire il *driver* per lo svolgimento delle attività sensibili considerate, e di quelle ad esse strumentali o comunque collegate, nonché per i relativi controlli, e, soprattutto, definiscono in dettaglio, ove ciò non sia già previsto, il sistema di riporto e i flussi informativi nei confronti dell'OdV.

In particolare, le procedure esistenti e quelle eventuali integrative devono garantire:

- chiarezza e precisione dei vari ruoli, compiti, attribuzioni, poteri e responsabilità;
- l'individuazione di un responsabile per ciascuna attività sensibile o per ciascuna fase della stessa;
- chiarezza e precisione delle varie linee di riporto;
- segregazione delle funzioni (separazione per ciascun processo tra il soggetto che decide, quello che autorizza, quello che esegue e quello che controlla);
- tracciabilità di tutte le fasi del processo e dei relativi soggetti;
- adeguati controlli (preventivi, concomitanti o successivi; automatici o manuali; continui o periodici; analitici o a campione), di tutte le fasi critiche del processo.
- flussi informativi nei confronti dell'OdV.