TARQUINIA MULTISERVIZI SRL

PARTE SPECIALE L - MAPPA RISCHI:
REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.

ALLEGATO L CORRELAZIONE AREE A RISCHIO-PROCEDURE, APPLICAZIONE DEL MODELLO CON RIGUARDO AI *REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI* .

1. La tipologia dei reati previsti dall'art. 24-bis del D.Lgs n. 231/01 (articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs n. 7 e 8 del 2016 e dal D.L. n. 105/2019)

La presente Parte Speciale si riferisce ai reati previsti dall'art. 24 bis del Decreto, in quanto individuati da Tarquinia Multiservizi Srl, nell'ambito dell'attività svolta, come reati di possibile commissione. Si descrivono brevemente qui di seguito le predette fattispecie contemplate dal suddetto articolo.

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.):
Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.
Pertanto i documenti informatici sono equiparati a tutti gli effetti ai documenti tradizionali.

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.):
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di

chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
La suddetta fattispecie si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema. Secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il proseguimento di finalità differenti da quelle per le quali era stato autorizzato.

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

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, 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 lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da euro 5.000,00 a 10.000,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater. Il legislatore ha introdotto tale reato al fine di prevenire le ipotesi di accesso abusivo a sistemi informatici. Pertanto sono punite

tali condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.
La fattispecie si configura sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.):
Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente 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, è punito con la reclusione sino a due anni e con la multa sino a euro 10.000,00. Tale reato si realizza quando qualcuno si procuri, produca, riproduca importi, diffonda, comunichi, consegni o metta a disposizione di altri apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema informatico o telematico.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.): chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a 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:
• 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;

• 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;

• da chi esercita anche abusivamente la professione di investigatore privato

Questo reato si realizza quando qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o metta a disposizione di altri apparecchiature, dispositivi o programmi.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617- quinquies c.p.):
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 4. La condotta vietata è pertanto costituita dalla mera installazione delle apparecchiature quando le stesse abbiano una potenzialità lesiva.

Danneggiamento di informazioni, dati e programmi informatici (art. 635- bis c.p.): Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.):
Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro

anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata. Tale reato si realizza, anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse pubblico.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.):
Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e` commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.):
Se il fatto di cui all'articolo 635- quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata. Tale reato si realizza, anche nel caso in cui si tratti di sistemi informatici o telematici di proprietà di privati ma destinati al soddisfacimento di un interesse pubblico.

2. Aree a rischio

2.1 Individuazione delle aree a rischio

Nell'ambito della presente sezione vengono definite "Aree a rischio" tutte quelle aree aziendali in cui i soggetti ad esse afferenti, per lo svolgimento della propria attività, possono supportare la commissione di reati di cui alla presente parte speciale.
Sono state, pertanto, individuate le seguenti macroaree ritenute più specificamente a rischio per aree e funzioni:

AREA	FUNZIONI A RISCHIO	REATI	ESPOSIZIONE AL RISCHIO
Amministratore Unico Revisore Unico Responsabile Ufficio Amministrazione Soggetti sottoposti al controllo dai Responsabili di cui sopra Settore Farmacia	Sistema informativo Progettazione e gestione dei sistemi informatici Sicurezza logica e fisica dei sistemi informatici	Art. 491-bis c.p Art. 615-ter c.p. Art.615-quater c.p. Art. 615 quinquies c.p. Art. 617 quater c.p. Art. 617 quinquies c.p. Art. 635 bis c.p. Art. 635 ter c.p. Art. 635 quater c.p. Art. 635 quinquies c.p.	**MEDIO ALTA**

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere previste dall'organo amministrativo della Tarquinia Multiservizi Srl, al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

2.2 Aree a rischio - Principi generali del sistema organizzativo

La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal presente Modello adottato da Tarquinia Multiservizi Srl, alla cui osservanza tutti i dirigenti e dipendenti della società sono tenuti.
Le attività della Tarquinia Multiservizi Srl nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.
Nell'ambito dello svolgimento delle normali attività aziendali potrebbero in ipotesi configurarsi i reati informatici innanzi indicati e, più in particolare, quelli inerenti l'alterazione di documenti aventi efficacia probatoria, la gestione degli accessi ai sistemi informativi interni o di concorrenti terzi e la diffusione di virus o programmi illeciti.
Il Modello, prevede l'espresso divieto di:
- porre in essere, collaborare o dare causa all'adozione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, tutte le fattispecie di reato rientranti tra quelle sopra considerate e previste dall'art. 24 bis del Decreto;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo in quanto idonei e diretti in modo univoco alla loro commissione.

Ai fini della prevenzione le norme generali devono dare attuazione a quanto segue:
• devono essere definiti processi adeguati alle dimensioni aziendali ed ai profili di operatività della società;
• le credenziali di accesso ai sistemi siano prontamente eliminate per il personale dimesso e ogni utente disponga di una *username* e password personale;

• bisogna assicurarsi che i terminali devono oscurarsi o scollegarsi dopo un periodo di inattività;
• l'utenza ed il profilo di accesso attribuito all'utente siano periodicamente rivisti per verificare se sussistono ancora le condizioni che hanno portato alla relativa attivazione;
• se necessario e/o tecnicamente possibile, le attività ritenute maggiormente critiche sono "registrate" in opportuni log, regolarmente ispezionati per garantire che gli utenti effettuino solo le attività per cui sono stati autorizzati.
• i backup dei dati residenti sui server siano salvati con frequenza giornaliera ed i supporti adeguatamente conservati;
• funzioni "privilegiate" devono essere concesse solo se ne esiste una reale necessità, sulla base di un'esigenza specifica e il loro utilizzo deve essere controllato;
• devono essere definiti dei controlli sulle applicazioni di sistema per verificare che non vi siano state delle modifiche non autorizzate;
• agli utenti deve essere fornita un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali e dei sistemi applicativi.

3. Procedure per le aree a rischio

3.1 Individuazione dei responsabili delle aree a rischio reato, principi di comportamento.

Occorre dare debita evidenza delle operazioni svolte nelle aree a rischio di cui al precedente paragrafo. A tal fine gli amministratori, i dirigenti ed i responsabili delle funzioni, dipendenti all'interno delle quali vengano svolte operazioni a rischio, divengono responsabili di ogni singola operazione da loro direttamente svolta o attuata nell'ambito della funzione a loro facente capo.
I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione della strumentazione informatica della Tarquinia Multiservizi Srl devono attenersi alle modalità di utilizzo degli strumenti aziendali e, in generale, alle norme aziendali che danno attuazione ai seguenti principi:
• utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
• custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della società, evitando che terzi soggetti possano venirne a conoscenza;
• aggiornare periodicamente le password, secondo le regole indicate dalla società;

• garantire la tracciabilità dei documenti prodotti attraverso l'archiviazione delle varie versioni dei documenti o comunque garantire meccanismi di tracciabilità delle modifiche;

• assicurare meccanismi di protezione dei file, quali password, conversione dei documenti in formato non modificabile.

Ai destinatari è fatto espresso divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra indicate;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato sopra indicate, possano potenzialmente diventarlo;
- utilizzare le risorse informatiche (es. personal computer fissi o portatili) assegnate dalla Tarquinia Multiservizi Srl per finalità diverse da quelle lavorative;
- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- accedere, senza averne la autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);
- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure nel fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici 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, l'alterazione del suo funzionamento (il divieto include la trasmissione di virus con lo scopo di danneggiare i sistemi informativi di enti concorrenti);
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;

- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici (il divieto include l'intrusione non autorizzata nel sistema informativo di società concorrente, con lo scopo di alterare informazioni e dati di quest'ultima);
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici 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 o ostacolarne gravemente il funzionamento;
- distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ostacolarne gravemente il funzionamento;
- installare software/programmi aggiuntivi rispetto a quelli esistenti e/o autorizzati dalla funzione aziendale centrale dei Sistemi Informativi;
- introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione della Direzione o altra funzione responsabile;
- modificare la configurazione di postazioni di lavoro fisse o mobili.

È inoltre sancito l'espresso obbligo di:
- tenere comportamenti in linea con i principi espressi nel Codice Etico e nel presente Modello Organizzativo;
- rispettare le procedure adottate;
- rispettare la normativa;

Individuazione dei processi per le aree a rischio reato

Con riferimento alle aree e funzioni a rischio di cui alla presente Parte Speciale, i controlli interni si articolano nei seguenti documenti:

Doc.	Piano Anticorruzione e Trasparenza
Doc.	Codice di Comportamento dei Dipendenti
Doc.	Mansionario e Regolamento Aziendale – Sistema disciplinare

La procedura e le specifiche attività che fanno parte di ciascuno di tali processi sono esposte in Allegato – "Processi" al Modello e ne costituiscono parte integrante unitamente a tutti i richiami normativi, procedurali e/o i rinvii esterni a manuali, circolari, prontuari, ecc.