PARTE SPECIALE E

Criminalità Informatica
-Reati informatici e trattamento illecito di dati -
- Art. 171 bis legge 633/1941 -

Approvato dal Consiglio di Amministrazione il 9 ottobre 2015
Primo aggiornamento adottato con delibera CdA del 21 ottobre 2016
Secondo aggiornamento adottato con delibera CdA del 15 febbraio 2019
Terzo aggiornamento adottato con delibera CdA del 29 gennaio 2021

1. Premessa

Il D.lgs. 231/01 prevede alcune fattispecie criminose che possono essere realizzate attraverso l'ausilio di sistemi informatici o telematici alcune delle quali sono state oggetto di valutazione in altre parti speciali del modello organizzativo.

Il Centro Ortopedico di Quadrante ha ritenuto opportuno indicare le misure adottate al fine di scongiurare il verificarsi di comportamenti illeciti connessi alla disponibilità di mezzi informatici, in quanto la sicurezza dei sistemi informatici è ritenuta elemento essenziale del sistema di controllo del Centro.

Oltre al reato di frode informatica di cui all'art. 640 ter c.p., già considerato nella parte speciale A, il legislatore ha inserito successivamente ulteriori ipotesi delittuose che rilevano ai fini della presente sezione nei limiti in cui siano commesse nell'interesse o a vantaggio della Società.

L'ipotesi che la commissione di talune fattispecie integri il suddetto requisito è un rischio alquanto marginale ma si è ritenuto opportuno inserire una sezione *ad hoc* in ragione del fatto che il sistema informatico prevede la gestione di tutti i dati del COQ ed occorre, pertanto, un corretto utilizzo dello stesso.

2. Fattispecie di reato e principi normativi

La conoscenza della struttura e delle modalità realizzative delle fattispecie di reato, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del D.Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'Ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

L'art. 24-*bis* che prevede i "*Delitti informatici e trattamento illecito di dati*" è stato introdotto dalla Legge n. 48/08, legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, convenzione redatta a Budapest il 23 novembre 2001.

Fondamentale per il corretto inquadramento delle fattispecie di reato contemplate dall'art. 24-*bis* è la definizione di sistema informatico.

Tale deve intendersi ogni sistema di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione di dati su supporti adeguati, per mezzo di impulsi elettronici.
In ragione dell'oggetto della presente sezione si richiamano inoltre i reati di cui all'art. 25 *novies* "Delitti in materia di violazione del diritto d'autore".
Si riportano, pertanto, i riferimenti normativi e le descrizioni dei reati oggetto della presente Parte Speciale.

2.1. Reati informatici

491 bis – Documenti informatici

"*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private*".

La norma sopra citata conferisce valenza penale alla commissione di reati di falso che si realizzino su un documento informatico; i reati di falso richiamati sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)
  "*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*".
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)
  "*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*".
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)

"*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*".

- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)

  "*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*".
- Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)

  "*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*".
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)

  "*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*".
- Falsità materiale commessa da privato (art. 482 c.p.)

  "*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".

- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.):
  "*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*".
- Falsità in registri e notificazioni (art. 484 c.p.)
  "*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*".
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.):
  "*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*".
- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)
  "*Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dall' articolo 487, si applicano le disposizioni sulle falsità materiali in atti pubblici*".
- Uso di atto falso (art. 489 c.p.)
  "*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*".
- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)

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

- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)
  "*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*".

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

"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".
Il reato consiste nell'introduzione abusiva con qualsiasi strumento in un sistema informatico o telematico protetto da misure di sicurezza ovvero nella permanenza contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
Pare opportuno evidenziare che il delitto è procedibile d'ufficio solo qualora esso sia stato commesso nella sua forma aggravata, ovvero quando il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, da chi esercita anche abusivamente la professione di investigatore privato, con abuso della qualità di operatore del sistema, ovvero se per commettere il fatto viene usata violenza sulle cose o alle persone o ancora 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.

<u>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art.615-quater c.p.)</u>
"Chiunque, al fine di procurare a sè 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 5.164 Euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater".

<u>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)</u>

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

La fattispecie è un reato di pericolo, essendo irrilevante, ai fini della sua sussistenza, il danneggiamento di sistemi informatici.

La soglia di tutela è anticipata al mero "procurarsi".

Inoltre, il reato contempla non soltanto i *malware*, ma anche gli *hardware* che i prestino ad un utilizzo illecito.

<u>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)</u>

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

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

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

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

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

Installazione di apparecchiature atte ad intercettare, impedire od 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".

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".

La condotta criminosa si realizza attraverso la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o software altrui.

Si precisa che il reato è procedibile a querela della persona offesa, mentre è procedibile d'ufficio se il fatto viene commesso con violenza alla persona o con minaccia, ovvero con abuso della qualità di operatore del sistema.

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".
La norma anticipa la tutela considerando integrato il reato da fatti diretti 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, anche qualora dalla condotta posta in essere non derivi la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, che viene considerata una mera circostanza aggravante.

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 è 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)
"*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".

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

"Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro".

2.2. Delitti in materia di violazione del diritto d'autore (legge 633/1941)

Art. 171 – reati presupposto evidenziati in maiuscolo

"Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter, è punito con la multa da Euro 51 a Euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nel territorio dello Stato esemplari prodotti all'estero contrariamente alla legge italiana;

A-BIS) METTE A DISPOSIZIONE DEL PUBBLICO, IMMETTENDOLA IN UN SISTEMA DI RETI TELEMATICHE, MEDIANTE CONNESSIONI DI QUALSIASI GENERE, UN'OPERA DELL'INGEGNO PROTETTA, O PARTE DI ESSA ;

b) rappresenta, esegue o recita in pubblico o diffonde con o senza variazioni od aggiunte, una opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di produrre o di rappresentare;
e) (Omissis);
f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.
Chiunque commette la violazione di cui al primo comma, lettera a-bis), e' ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.
LA PENA È DELLA RECLUSIONE FINO AD UN ANNO O DELLA MULTA NON INFERIORE AD EURO 516 SE I REATI DI CUI SOPRA SONO COMMESSI SOPRA UN'OPERA ALTRUI NON DESTINATA ALLA PUBBLICAZIONE, OVVERO CON USURPAZIONE DELLA PATERNITÀ DELL'OPERA, OVVERO CON DEFORMAZIONE, MUTILAZIONE O ALTRA MODIFICAZIONE DELL'OPERA MEDESIMA, QUALORA NE RISULTI OFFESA ALL'ONORE OD ALLA REPUTAZIONE DELL'AUTORE.
La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da Eur 1.032 a Euro 5.164".

Art. 171 bis

"*Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da Euro 2.582 ad Euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a*

protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a Euro 15.493 se il fatto è di rilevante gravità.
Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da Euro 2.582 ad Euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa ad E uro 15.493 se il fatto è di rilevante gravità".

Art. 171 ter

"*E' punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da Euro 2.582 ad Euro 15.493chiunque per trarne profitto:*
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi

procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale.

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del

pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. E' punito con la reclusione da uno a quattro anni e con la multa da Euro 2.582 ad Euro 15.493chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma l;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;

e) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici".

Art. 171 septies

"*La pena di cui all'articolo 171-ter, comma 1, si applica anche:*

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge".

Art. 171 octies

"*Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da Euro 2.582ad Euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.*

La pena non è inferiore a due anni di reclusione e la multa ad Euro 15.493 se il fatto è di rilevante gravità"

3. Destinatari e obiettivi della Parte speciale E

La Parte Speciale E disciplina i comportamenti posti in essere da amministratori, dirigenti e dipendenti del Centro Ortopedico di Quadrante nell'utilizzo dei sistemi informatici o telematici.

Finalità della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei Reati oggetto della presente Parte Speciale.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- fornire le «regole di comportamento» e le procedure che gli amministratori, i dirigenti ed i dipendenti, sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- fornire ai responsabili delle funzioni aziendali ed all'Organismo di Vigilanza gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

4. Processi sensibili

Il COQ utilizza un sistema informatico di tipo tradizionale basato su un'architettura client – server (cd. architettura 1-tier) che consente di gestire i processi registrando le operazioni in tempo reale, permettendo la tracciabilità e l'identificazione degli autori.

In ragione dell'attività svolta possono essere esclusi i rischi connessi ai seguenti reati presupposto:

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);
- Art. 171 ter;
- Art. 171 septies;
- Art. 171 octies.

Per le restanti categorie di reato si ritiene che i rischi, seppur astratti, sono propri di ogni contesto, aziendale e sanitario, che utilizza le tecnologie informatiche (a titolo esemplificativo si considerino l'area amministrativa, le Direzioni, l'area personale, ecc.).

I reati sopra considerati hanno, infatti, come presupposto la disponibilità di un terminale e la concreta disponibilità di accesso alle postazioni di lavoro; per tale ragione le aree di attività ritenute più specificamente a rischio sono quelle che comportano l'utilizzo di un personal computer, l'accesso alla posta elettronica, l'utilizzo di programmi informatici e l'accesso a internet.

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati nella presente Parte Speciale, sono collegate a tutte le attività di gestione e utilizzo dei sistemi informatici e delle informazioni del Centro Ortopedico (c.d. "patrimonio informativo"), nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi verso l'esterno;
- gestione e protezione delle reti;
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.) dei sistemi informatici;

È possibile, inoltre, ravvisare attività sensibili nella gestione delle autorizzazioni e delle licenze di programmi software e banche dati.

5. Principi generali di comportamento

Ai fini della prevenzione dei reati sopra indicati, il Modello prevede l'espresso divieto a carico dei destinatari di porre in essere, o concorrere in qualsiasi forma, nella realizzazione di comportamenti tali da integrare le fattispecie considerate nella presente Parte Speciale.

A tal fine, più specificamente, il COQ pone, a carico del destinatari, l'espresso divieto di :

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati delCentro, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di altri soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

- utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio virus, worm, troian, spyware,dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati.

Nell'ambito delle suddette regole, è previsto, in particolare, l'obbligo di:

a) comportarsi in conformità alle norme di legge, di regolamento, alle procedure esistenti in ogni attività che comportino l'utilizzo di un terminale e l'accesso a sistemi informatici. Ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (ad esempio personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività e non possono essere cedute a terzi. Tali risorse devono essere conservate in modo appropriato ed i responsabili del Centro dovranno essere tempestivamente informati di eventuali furti o danneggiamenti;
b) ogni dipendente/amministratore del sistema è tenuto alla segnalazione alla Direzione di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente;
c) osservare altresì rigorosamente tutte le norme poste dalla legge a tutela della Privacy e di agire sempre nel rispetto delle procedure interne che su tali norme si fondano. A tal fine è previsto un piano organico di protezione dei dati;

d) di garantire ed agevolare ogni forma di controllo, svolta nel rispetto dell'art. 4 dello Statuto dei Lavoratori, diretta a impedire la commissione di fattispecie delittuose.
e) evitare di introdurre e/o conservare a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente autorizzate;
f) evitare di trasferire all'esterno del COQ e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà del Centro, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
g) evitare l'utilizzo di *passwords* di altri utenti, neanche per l'accesso ad aree protette per conto degli stessi, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;
h) evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
i) utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento. L'accesso a internet dovrà avvenire per ragioni esclusivamente lavorative salva diversa autorizzazione rilasciata dalla funzione competente. Non è consentito accedere da terminali in qualsiasi modo legati all'attività lavorativa svolta per il Centro a siti e pagine web contenenti materiale vietato dalla legge (ad es. pedopornografici) o che possano costituire pericolo per la sicurezza della rete informatica. A tal fine il COQ provvede a rendere operativo un blocco totale verso i siti internet di cui sopra, blocco che non dovrà in alcun modo subire tentativi di aggiramento;
j) rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
k) impiegare sulle apparecchiature del Centro solo prodotti ufficialmente acquistati dallo stesso;

l) astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
m) astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
n) osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni del COQ;
o) osservare scrupolosamente quanto previsto dalle politiche di sicurezza per la protezione e il controllo dei sistemi informatici.

I responsabili delle funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

6. Procedure specifiche

Il Centro Ortopedico di Quadrante ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni del Codice della privacy, per prevenire e controllare i rischi in tema di tecnologia dell'informazione, a tutela del proprio patrimonio informativo e dei dati personali dei soggetti interessati.

E' stato adottato il un Documento di Sicurezza (allegato 1) in cui sono contenute le misure adottate al fine di evitare e prevenire usi illeciti o non corretti, accessi non autorizzati, ovvero potenziali conseguenze dannose di virus informatici.

Le misure di sicurezza ricomprendono, a protezione dell'accesso a programmi riservati, la previsione di password, ovvero codici di accesso riservati nominativi o numerici, la cui disponibilità di utilizzo è riservata agli utenti del sistema informatico, la rigorosa custodia delle credenziali di accesso alle postazioni di lavoro, un sistema di controllo degli accessi alle banche dati, l'individuazione di un responsabile per settore, la sensibilizzazione del personale e una protezione antivirus.

Le misure sopra descritte sono sintetizzate nella tabella che segue.

Misure	Descrizione	Rischi contrastati
Sistema di aggiornamento continuo password	Il COQ ha istituito un sistema di autenticazione, attribuendo un codice identificativo (username, user ID) strettamente personale per l'utilizzazione dei personal computer. I codici identificativi sono aggiornati e modificati mensilmente.	Sottrazione di credenziali di autenticazione
Antivirus	È stato adottato un sistema antivirus con scansione in tempo reale ed aggiornamento settimanale, installato su tutti gli strumenti elettronici in dotazione.	Azione di virus o di programmi suscettibili di recare danno
Piano di disaster recovery e back up dei dati	Al fine di garantire non solo la integrità ma anche la pronta disponibilità dei dati, il COQ si è dotata di strumenti e procedure di back up, con cadenza periodica. Le copie di back up non sono conservate nello stesso luogo fisico ove si trovano gli strumenti elettronici con cui si gestiscono i dati	Azione di virus o di programmi suscettibili di recare danno
Firewall	Con funzione di filtro di tutti i pacchetti entranti ed uscenti, da e verso la rete ed i computer	Accessi esterni non autorizzati

7. Il sistema di controllo: compiti e poteri dell'OdV

Il sistema di controllo predisposto dal Centro Ortopedico di Quadrante prevede la supervisione ad opera dell'Organismo di Vigilanza, soggetto istituzionalmente preposto alla verifica dell'idoneità ed efficacia del modello.

L'OdV, pertanto, effettua periodicamente specifici controlli sulle attività connesse ai "processi sensibili" al fine di verificare il rispetto dei Principi Generali di comportamento e delle procedure e delle istruzioni operative come sopra indicate.

E' stata all'uopo redatta specifica procedura che regolamenta i flussi informativi nei confronti dell'OdV, al fine di fornire allo stesso le informazioni necessarie per l'espletamento dell'attività di verifica e controllo (*Procedura "Flussi informativi nei confronti dell'OdV"*).

In ogni caso all'OdV vengono garantiti autonomi poteri di iniziativa e controllo e potrà avere accesso in qualunque momento a tutta la documentazione ritenuta rilevante.

Nell'ambito dei propri poteri potrà indire, a sua discrezione, riunioni specifiche con i soggetti deputati alla gestione dei "processi sensibili" e potrà attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello.

8. Sanzioni disciplinari

L'inosservanza dei principi e delle procedure previste nella presente parte speciale è passibile di sanzione disciplinare secondo quanto indicato nella parte generale alla sezione "Sistema disciplinare".