

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

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

**1. La tipologia dei reati informatici (art. 24 bis del D.Lgs. n. 231 del 2001)**

La presente Parte Speciale si riferisce ai reati informatici e al trattamento illecito dei dati. Si descrivono brevemente qui di seguito le singole fattispecie contemplate all'art. 24 *bis* del Decreto.

**Accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.)**

L'articolo in esame punisce con la reclusione fino a tre anni 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.

La pena è aumentata, qualora i fatti 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.

**Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (articolo 615 *quater* c.p.)**

L'art. 615-*quater* c.p. punisce chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, 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.

### **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617 *quater* del c.p.)**

Il reato viene commesso da chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.

Salvo che il fatto costituisca più grave reato, allo stesso modo viene punito chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni indicate al periodo precedente.

### **Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (articolo 617 *quinquies* c.p.)**

Il reato in questione punisce chiunque, fuori dei 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 a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

### **Danneggiamento di informazioni, dati e programmi informatici (articolo 635 *bis* c.p.)**

Viene punito, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o



programmi informatici altrui.

### **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635 *ter* c.p.)**

Viene considerato responsabile per il delitto in questione, 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.

Il reato di cui all'art. 635-ter c.p. si configura, ad esempio, allorché un dipendente della Fondazione riesca ad introdursi nel sistema informatico dell'Agenzia delle Entrate al fine di cancellare una cartella esattoriale a suo carico.

### **Danneggiamento di sistemi informatici o telematici (articolo 635 *quater* c.p.)**

Salvo che il fatto costituisca più grave reato, viene punito 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.

### **Danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635 *quinqües* 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 il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

La fattispecie criminosa in esame è integrata, ad esempio, allorché un dipendente della Fondazione si introduce nel sistema informatico di una Pubblica Amministrazione e danneggia, rendendole inutilizzabili, le informazioni ivi contenute attestanti irregolarità commesse dalla Fondazione.

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

Commette il delitto 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.

### **Delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, riguardante la sicurezza nazionale cibernetica**

Il Decreto legge in questione istituisce il perimetro di sicurezza nazionale cibernetica, 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 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.

In funzione di quanto sopra, con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica, vengono individuate le amministrazioni pubbliche e gli operatori nazionali, pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti in materia.

I soggetti di cui trattasi sono tenuti in particolare a predisporre, aggiornare e trasmettere ai ministeri competenti, con cadenza almeno annuale, un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza.

Costituisce reato la condotta di chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

\*\*\*\*\*

L'art. 24-bis, comma 3, del D.Lgs. 231/2001, richiama il reato di cui all'art. 491-bis del codice penale (Documenti informatici), a norma del quale "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". Devono essere, quindi, ricompresi anche se non citate direttamente ma indirettamente nell'elenco dei reati informatici i seguenti reati come segue:

### **Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)**

È un reato che può essere commesso dal pubblico ufficiale il quale, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un documento pubblico (informatico) falso ovvero altera un documento pubblico (informatico) vero.

Si pensi, ad esempio, ad un pubblico ufficiale che interviene sulle domande relative al condono edilizio, alternandole e sostituendo la documentazione allegata in modo da far conseguire la sanatoria per opere realizzate dopo la presentazione delle domande ovvero per superfici superiori a quelle

originariamente indicate.

### **Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)**

Il reato può essere commesso dal 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.

Il delitto di cui all'art. 477 c.p. si configura, ad esempio, nell'ipotesi di falso di carta d'identità, posto che la carta di identità rientra tra i documenti tutelati da detta norma, trattandosi di un certificato la cui specifica finalità è quella di consentire l'esatta identificazione delle persone.

### **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.)**

È un reato che può essere commesso dal 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.

Un esempio potrebbe essere rappresentato dal notaio (pubblico ufficiale) che rilascia al legale rappresentante dell'Ente una copia autentica di un atto pubblico difforme dall'originale.

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

È un reato che può essere commesso dal 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.

Tale ipotesi delittuosa si configura, ad esempio, nel caso in cui il medico del lavoro, nel redigere la cartella clinica informatica di un dipendente della Fondazione, attesti falsamente l'idoneità o l'inidoneità al lavoro di quest'ultimo.

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

Commette il reato 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.

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

Commette il reato 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.

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

Consiste nella commissione dei fatti previsti dagli articoli 476, 477 e 478 c.p. da parte di un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni.

### **Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)**

Commette il reato chiunque attesti falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità.

### **Falsità in registri e notificazioni (art. 484 c.p.)**

È un reato che può essere commesso da chi, per legge, è 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, e consiste nello scrivere o lasciar scrivere false indicazioni.

### **Falsità in foglio firmato in bianco. Atto pubblico (artt. 487 e 488 c.p.)**

Il reato può essere un commesso dal 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.

### **Uso di atto falso (art. 489 c.p.)**

È un reato che può essere commesso da chiunque e consiste nell'utilizzo di un documento (informatico) falso senza essere concorso nella falsità.

Si configura, ad esempio, allorquando, al fine di giustificare un inadempimento contrattuale, il datore di lavoro produce al cliente falsa documentazione medica telematica fornitagli dal dipendente, giustificante l'assenza dello stesso.

### **Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)**

È un reato che può essere commesso da chi, 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.

Si configura ad esempio un dipendente della Fondazione distrugge un atto pubblico informatico avente efficacia probatoria al fine di eliminare la prova dell'esistenza dello stesso.

### **Falsità in testamento olografo, cambiale o titoli di credito (art. 491 c.p.)**



Se alcuna delle falsità previste dagli articoli precedenti riguarda un testamento olografo, ovvero una cambiale o un altro titolo di credito trasmissibile per girata o al portatore, e il fatto è commesso al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, si applicano le pene rispettivamente stabilite nella prima parte dell'articolo 476 e nell'articolo 482 c.p.

### **Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)**

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.

### **Falsità commesse da pubblici impiegati incaricati di un servizio pubblico (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.

## **2. Aree a rischio**

Nell'ambito della presente sezione vengono definite "Aree a rischio" tutte quelle aree operative 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
<p>Presidente</p> <p>Comitato Tecnico Scientifico</p> <p>CNAP</p> <p>Ufficio dirigenziale di Presidenza</p> <p>Internal Audit e Risk Management</p> <p>Direttore Generale</p> <p>Direttore Scientifico</p> <p>Area Affari Generali</p> <p>Ufficio Risorse Umane</p> <p>Ufficio ICT</p> <p>Ufficio di Sviluppo e Trasferimento Tecnologico</p> <p>Area Legale, Compliance e Privacy</p> <p>Ufficio Contratti e Contenzioso</p> <p>Ufficio Compliance e Privacy</p>	<p>Attività di gestione dei profili utente e del processo di autenticazione</p> <p>Attività di duplicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nei pc, tablet, smartphone, ecc...</p> <p>Attività di predisposizione ed invio telematico di domande, di attestazioni, certificazioni</p> <p>Sicurezza fisica, quali sicurezza cablaggi, dispositivi di rete...</p> <p>Attività inerente alla gestione e alla protezione delle reti</p> <p>Gestione dell'architettura informatica della Fondazione</p> <p>Gestione dell'infrastruttura tecnologica della Fondazione e cura dei rapporti con i fornitori IT interni ed esterni</p> <p>Definizione le procedure interne per l'utilizzo dei</p>	<p>Accesso abusivo ad un sistema informatico o telematico (articolo 615-ter c.p.)</p> <p>Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (articolo 615 - quater c.p.)</p> <p>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617- quater del c.p.)</p> <p>Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o</p>	<p><b>BASSA</b></p>

	<p>dati</p> <p>Gestione delle banche dati interne</p> <p>Attività di gestione ed utilizzo di strumenti di memorizzazione quali supporti USB, CD...</p>	<p>interrompere comunicazioni informatiche o telematiche (articolo 617-quinquies c.p.)</p> <p>Danneggiamento di informazioni, dati e programmi informatici (articolo 635-bis c.p.)</p> <p>Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635-ter c.p.)</p> <p>Danneggiamento di sistemi informatici o telematici (articolo 635-quater c.p.)</p> <p>Danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635-quinquies c.p.)</p> <p>Frude informatica del soggetto che presta servizi di certificazione di firma elettronica</p>	
--	--	--	--

		<p>(art. 640-quinquies c.p.)</p> <p>Delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, riguardante la sicurezza nazionale cibernetica.</p> <p>Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)</p> <p>Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)</p> <p>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.)</p> <p>Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)</p> <p>Falsità ideologica commessa dal pubblico ufficiale</p>	
--	--	---	--

		<p>in certificati o autorizzazioni amministrative (art. 480 c.p.)</p> <p>Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)</p> <p>Falsità materiale commessa da privato (art. 482 c.p.)</p> <p>Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)</p> <p>Falsità in registri e notificazioni (art. 484 c.p.)</p> <p>Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)</p> <p>Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)</p> <p>Uso di atto falso (art. 489 c.p.)</p> <p>Soppressione,</p>	
--	--	---	--

		<p>distruzione e occultamento di atti veri (art. 490 c.p.)</p> <p>Falsità in testamento olografo, cambiale o titoli di credito (art. 491 c.p.)</p> <p>Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)</p> <p>Falsità commesse da pubblici impiegati incaricati di un servizio pubblico (art. 493 c.p.)</p>	
--	--	--	--

Le funzioni considerate più specificatamente a rischio in relazione ai reati di cui alla presente sezione sono ritenute le seguenti:

- Attività di gestione dei profili utente e del processo di autenticazione.
- Attività di duplicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nei pc, tablet, smartphone, ecc...
- Attività di predisposizione ed invio telematico di domande, di attestazioni, certificazioni.
- Attività di gestione ed utilizzo di strumenti di memorizzazione quali supporti USB, CD.
- Sicurezza fisica, quali sicurezza cablaggi, dispositivi di rete.
- Attività inerente alla gestione e alla protezione delle reti.
- Gestione delle banche dati interne.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere previste dagli organi direttivi della Fondazione "Biotechnopolo di Siena", ai quali viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

### **3. Principi generali del sistema organizzativo e di comportamento nelle aree di attività a rischio**

La presente Parte Speciale richiama i principi generali di comportamento previsti dal Codice Etico adottato dalla Fondazione "Biotechnopolo di Siena", alla cui osservanza tutti gli amministratori, direttori, dirigenti e dipendenti della Fondazione sono tenuti.

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.

### **4. Procedure per le aree a rischio**

#### **4.1 Individuazione dei responsabili delle aree a rischio reato**

Occorre dare debita evidenza delle operazioni svolte nelle aree a rischio di cui al precedente paragrafo. A tal fine amministratori esecutivi e non, il Direttore Generale e/o il Direttore Scientifico ed i responsabili delle Aree e/o Uffici, all'interno dei 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.

Detti responsabili divengono i soggetti referenti dell'operazione a rischio.

Sulle operazioni in questione, l'Organo di Vigilanza (OdV) potrà predisporre ulteriori controlli dei quali verrà data evidenza scritta.

#### **4.2 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 nonché le misure di prevenzione adottate dalla Fondazione "Biotechnopolo di Siena" si articolano nei seguenti regolamenti:

COD.0	Codice Etico
REG.1	Regolamento di organizzazione e funzionamento
REG.2	Regolamento sulle modalità di reclutamento e di gestione del personale
REG.3	Regolamento delle missioni degli organi
REG.4	Regolamento di contabilità
REG.5	Regolamento per la gestione delle situazioni di conflitto di interesse e di incompatibilità
REG.6	Regolamento di organizzazione e funzionamento del Consiglio
REG.7	Regolamento e Modulo per la concessione dei patrocinii

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