PARTE SPECIALE

- B -

REATI INFORMATICI

Versione approvata dal Consiglio di Amministrazione in data 22 ottobre 2024

PARTE SPECIALE "B" - REATI DI CRIMINALITÀ INFORMATICA

B.1. Le tipologie dei reati di criminalità informatica (art. 24-bis del decreto)

La Legge 48/2008 recante la *"Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"* ha introdotto nel Decreto l'art. 24 bis, che ha inserito i reati informatici fra i reati presupposto del Decreto stesso.

La tematica è rilevante, considerata l'ormai enorme diffusione degli strumenti informatici e la circostanza che le aziende siano spesso esposte ad attacchi/violazioni dei propri sistemi informativi. Peraltro, con il recente aumento dell'utilizzo dello *smart working*, le aziende sono ancora più esposte al rischio di violazione delle misure tecniche adottate: l'uso di dispositivi e/o di connessioni di rete personali può, infatti, creare l'occasione per la commissione dei reati c.d. di criminalità informatica, che, come noto, ai sensi del Decreto, possono comportare la responsabilità della Società, ove gli stessi siano commessi nell'interesse o a vantaggio dell'ente.

Inoltre, il D.L. 105 del 21 settembre 2019, convertito in L. 18 novembre 2019, n. 133 ha istituito il c.d. *"perimetro di sicurezza nazionale cibernetica"*, volto ad 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 (art. 1, comma 1, del D.L. sopra citato). In ragione di quanto sopra è stato introdotto nel codice penale il nuovo reato presupposto di cui all'art. 640-quinquies c.p. *(Frode informatica del certificatore di firma elettronica)*, che però non risulta rilevante ai fini della presente Parte Speciale in quanto Consip S.p.A. non rientra nel perimetro di sicurezza cibernetica di cui alla normativa in esame (cfr. tabella sotto).

In aggiunta, si evidenzia che l'art. 19 della Legge n. 238 del 23 dicembre 2021, avente ad oggetto *"Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020"*, ha apportato delle modifiche al codice penale che hanno interessato i "*Delitti informatici e trattamento illecito di dati*" contemplati dall'art. 24-bis del D.Lgs.n.231/01. In particolare, le modifiche riguardano:

- l'ampliamento della descrizione delle condotte dei reati di: i) detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.); ii) detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.) e di iii) detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a

intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.) e conseguente modifica della rubrica delle norme;

- l'aumento di pena per il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.).

Infine, si segnala la legge n. 90/2024 recante *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"*, che, con l'art. 24, ha modificato l'art. 24 bis del Decreto, in materia di delitti informatici e trattamento illecito di dati. Con tale intervento il Legislatore inasprisce la sanzione pecuniaria applicata all'ente che commette i delitti di cui agli artt. 615 ter, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater e 635 quinquies del codice penale, e introduce quale nuovo reato presupposto, il delitto di estorsione, di cui all'art. 629 terzo comma del codice penale, commesso mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies.

Nella presente Parte Speciale "B", si provvede dunque a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24-bis del Decreto, e suddivisi tra:

→ reati potenzialmente realizzabili;

→ reati la cui commissione, per quanto non si possa escludere *del tutto*, è stata ritenuta remota/non ipotizzabile in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente gestita nel rispetto dei principi e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società;

→ reati non applicabili alla Società.

Nello specifico:

REATO	RIFERIMENTO	REALIZZABILITÀ
Falsità in un documento informatico pubblico	491-bis c.p.	possibile
Accesso abusivo ad un sistema informatico o telematico	615-ter c.p.	possibile
Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici	615-quater c.p.	possibile
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	617-quater c.p.	possibile
Detenzione, diffusione e installazione abusiva di	617-quinquies c.p.	possibile

apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche		
Estorsione	629-comma 3 c.p.	possibile
Danneggiamento di informazioni, dati e programmi informatici	635-bis c.p.	possibile
Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico	635-ter c.p.	possibile
Danneggiamento di sistemi informatici o telematici	635-quater c.p.	possibile
Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	635 quater.1 c.p.	possibile
Danneggiamento di sistemi informatici o telematici di pubblico interesse	635-quinquies c.p.	possibile
Frode informatica del certificatore di firma elettronica	640-quinquies c.p.	non applicabile
Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica	art. 1, comma 11, D.L. 21 settembre 2019, n. 105 convertito con modificazioni dalla L. 18 novembre 2019, n. 133	non applicabile

* * *

I reati che sono stati considerati potenzialmente realizzabili sono dunque i seguenti:

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 due a dieci 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 minaccia o 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 ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare 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 tre a dieci anni e da quattro a dodici anni.

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

Il reato in esame si realizza quando un soggetto si introduce abusivamente (o vi si mantiene, sempre abusivamente) in un sistema informatico o telematico protetto da misure di sicurezza. In merito si evidenzia come il Legislatore abbia inteso punire il mero accesso abusivo ad un sistema informatico o telematico cui non deve necessariamente seguire il danneggiamento di dati. Tale fattispecie delittuosa si realizza anche nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, utilizzi il sistema stesso per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato. Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso, in vista del compimento di atti ulteriori nell'interesse o a vantaggio della società stessa.

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

"Chiunque, al fine di procurare a sé o ad altri un vantaggio 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 ad due anni e con la multa sino a € 5.164,00.

La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma."

Il reato in esame si realizza nel caso in cui un soggetto abusivamente si procuri, detenga, riproduca, diffonda, importi, comunichi, consegni o comunque metta a disposizione di altri, codici, dispostivi di protezione (quali password, badge, ecc.) o altri mezzi idonei all'accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca

indicazioni idonee a raggiungere tale scopo a terzi. L'art. 615-quater c.p., pertanto, punisce le 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. Tale fattispecie può configurarsi sia nel caso in cui il soggetto, in possesso legittimamente dei dispositivi di protezione di cui sopra, li comunichi senza autorizzazione a terzi, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615-quater c.p. punisce altresì chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza: ad esempio, il dipendente che comunichi ad un terzo soggetto la password di accesso alla posta elettronica di un proprio collega, allo scopo di garantire al terzo la possibilità di controllare le attività svolte dal collega, quando da ciò possa derivare un determinato vantaggio o interesse per la società.

Estorsione (art. 629 comma 3 c.p.)

" *Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità."*

Con l'introduzione di questo nuovo comma, il Legislatore ha previsto un'autonoma fattispecie di reato avente ad oggetto la condotta di chi, compiendo o minacciando di compiere i delitti di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, costringe taluno a fare o ad omettere qualcosa, procurando a sé un ingiusto profitto, a danno di terzi: deve dunque sussistere un rapporto strumentale tra la condotta posta in essere (o minacciata) dal soggetto agente, la costrizione della vittima (ad un *facere* o ad un *non facere*) e la realizzazione dell'ingiusto profitto, in danno di altri.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

"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 due a sei anni. La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato."*

Il reato in esame si realizza qualora un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. Il danneggiamento potrebbe essere

commesso a vantaggio della società nel caso in cui, ad esempio, l'alterazione o l'eliminazione di alcuni file o del programma informatico, siano volte a nascondere dati aziendali ritenuti compromettenti per la società o a celare la prova del credito da parte di un fornitore della società (es. *fee*) o a contestare il corretto adempimento delle obbligazioni da parte di quest'ultimo.

Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (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 di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni. La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)."

Tale delitto si distingue dal precedente (art. 635-bis c.p.) poiché, in questo caso, il danneggiamento ha ad oggetto beni pubblici o di interesse pubblico; ne consegue, dunque, che il delitto 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 di natura pubblica.

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 due a sei anni. La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato."

Il reato in esame si realizza quando un soggetto, mediante le condotte di cui all'art. 635-*bis* c.p., distrugga, danneggi, renda (in tutto o in parte) inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Ne deriva che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p..

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater. 1 c.p.)

"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.
La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).
La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma."

Il Legislatore, con la novella in commento, ha dunque riprodotto, al primo comma, la fattispecie di cui all'art. 615-quinquies c.p. (contestualmente abrogata dall'art. 14, comma 1, lett. d) della legge 90/2024), introducendo, inoltre, due circostanze aggravanti: la prima (mediante il richiamo all'art. 615-ter secondo comma, numero 1), qualora il fatto sia commesso da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema; la seconda (con richiamo all'art. 615-ter, terzo comma), qualora il fatto sia commesso su 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.

Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies.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, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.
La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;*
3) *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 quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).

Il reato in esame si configura quando la condotta di cui al precedente art. 635-bis c.p. sia diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblico interesse o ad ostacolarne gravemente il funzionamento. Rileva in questo reato che il sistema sia utilizzato per il perseguimento di pubblico interesse, indipendentemente dalla proprietà privata o pubblica dello stesso.

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 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 quattro a dieci anni se il fatto è commesso:

1) *in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma;*
2) *in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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."*

Tale ipotesi di reato può configurarsi quando un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione. Lo scopo è quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

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

"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.
Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.
Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni."

Falsità in documenti informatici (art. 491-bis c.p.)

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

La norma in esame dispone che tutti i delitti relativi alla "falsità in atti" disciplinati dal codice penale di cui al Capo III, Titolo VII, Libro II, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo, bensì un documento informatico, pubblico o privato, avente efficacia probatoria.

* * *

Nel seguito il reato ritenuto non applicabile:

Frode informatica del certificatore 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 € 51,00 a € 1.032,00."

Il reato in esame si realizza quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato di firma. Il reato è, dunque, qualificabile come reato "proprio" in quanto può essere commesso solo da parte dei certificatori qualificati, vale a dire i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1 comma 11, D.L. 21 settembre 2019, n. 105 convertito con modificazioni dalla L. 18 novembre 2019, n. 133)

"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, è punito con la reclusione da uno a tre anni."

B.2 Attività a Rischio Reato

L'attività a rischio reato rappresenta "*un'attività riferita ad uno o più processi aziendali - nel cui ambito si potrebbero in linea di principio configurare le condizioni, le occasioni o i mezzi per la commissione di reati, anche in via strumentale alla concreta realizzazione della fattispecie*". Nell'ambito del Risk assessment integrato (RAI) - svolto dalle strutture interne competenti ed aggiornato annualmente, anche attraverso interviste alle risorse delle Divisioni/Aree interessate, a conoscenza dello specifico ambito analizzato - sono individuate tutte le attività a rischio reato inerenti la presente parte speciale e riferite ai macro-processi ed ai processi aziendali. Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte speciale "B", sono:

Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
R_191	Accesso sistemi informativi interni	Accesso illegittimo ai sistemi informativi aziendali al fine di: – estrarre dati / informazioni / documenti riservati da utilizzare/ diffondere a terzi – danneggiare/alterare i dati ivi contenuti o il sistema (es per coprire inefficienze o comportamenti illeciti nell'autorizzazione degli acquisti interni) – effettuare un trasferimento illecito di denaro, di valore monetario o di valuta virtuale per avvantaggiare un dipendente o la Società	– *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)* – *Estorsione (art. 629 comma 3 c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1)* – *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater)*

Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
			– *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies)* – *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)* – *Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies.c.p.)*
R_192	Accesso sistemi informativi gestiti dalla società	Accesso illegittimo ai sistemi informativi gestiti dalla società (es. piattaforma e-procurement) al fine di: – estrarre o alterare la documentazione/ le informazioni ivi contenute – danneggiare il sistema, per avvantaggiare uno o più partecipanti ad una gara (es. venendo a conoscenza delle offerte degli altri partecipanti prima di sottoporre la propria o annullando una gara che non sta evolvendo come immaginato)	– *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)* – *Estorsione (art. 629 comma 3 c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1)* – *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater)* – *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies)* – *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)* – *Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies.c.p.)*

Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
R_193	Controllo accessi sistemi informativi interni/gestiti dalla società	Mancato controllo sugli accessi al sistema da parte degli amministratori di sistema e mancata tracciabilità degli stessi	– *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)* – *Estorsione (art. 629 comma 3 c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1)* – *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)*
R_194	Gestione banche dati e software aziendali	Abusiva duplicazione o detenzione di programmi per elaboratori o illecito utilizzo di banche dati, con lo scopo di consentire un risparmio alla Società in termini di costi legati al mancato acquisto di prodotti informatici o banche dati muniti di regolare licenza	- *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)*
R_195	Gestione / acquisto banche dati e software aziendali	Abusivo utilizzo/detenzione di banche dati/software con lo scopo di commettere attività illecite	– *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)*
R_196	Gestione, sviluppo Sistemi informativi interni	Non corretta gestione / sviluppo / danneggiamento di sistemi informativi interni anche al fine di avvantaggiare terzi o la Società (es. danneggiare il sistema accessi per impedirne la consultazione o sviluppare un software per commettere attività illecite)	– *Estorsione (art. 629 comma 3 c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1)* – *Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)*

Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
			– *Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.p.)* – *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater)* – *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies)* – *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)* – *Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies.c.p.)*
R_197	Disponibilità sistemi informativi gestiti dalla Società	Non corretta gestione / sviluppo / danneggiamento di sistemi informatici o telematici gestiti dalla Società (es. al fine di renderli, in tutto o in parte, inservibili) anche al fine di avvantaggiare uno o più partecipanti ad una gara	– *Estorsione (art. 629 comma 3 c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1)* – *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)* – *Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.p.)* – *Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)* – *Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies.c.p.)*
R_198	Configurazione gara	Errata configurazione della gara – anche ASP - sul sistema e-procurement (es. errato inserimento dei parametri) anche al fine di avvantaggiare uno o più partecipanti ad una gara	– *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri*

Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
			mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)
R_199	Sviluppo formula anomalia dell'offerta	Errato sviluppo della formula dell'anomalia all'interno del Mepa e del sistema di E-procurement, anche al fine di avvantaggiare uno o più partecipanti ad una gara	– *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)*
R_216	Gestione della Crisi all'interno dell'Azienda	Mancata/ non corretta gestione di situazioni di emergenza che possono verificarsi all'interno delle aziende	– *Estorsione (art. 629 comma 3 c.p.)* – *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1)* – *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)* – *Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.p.)* – *Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)* – *Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies.c.p.)*

Per i dettagli inerenti l'evento di rischio ed i presidi di controllo si rimanda alle singole schede di rischio, elaborate per le singole attività, nelle quali sono dettagliatamente indicati:

- ✓ ***Anagrafica evento rischio***: (i) attività a rischio e descrizione; (ii) Risk owner, contributor; (iii) Macro processo, Processo e Fase; (iv) Area e Sotto Area;
- ✓ ***Dettaglio rischio***: (v) Fattori abilitanti; (vi) Conseguenze; (vii) Riferimenti normativa interna;
- ✓ ***Controlli***: (viii) Sintesi misure di controllo; (ix) Misure generali; (x) Misure specifiche.

B.3 Principi di comportamento

I Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte Speciale, sono tenuti ad osservare i seguenti principi di comportamento:

- rispettare le norme in tema di trasparenza, nel rispetto di quanto indicato nel PTPC;
- garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
- garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
- garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;
- garantire la piena collaborazione agli organi di controllo e alla Divisione Internal Audit nell'ambito degli audit/controlli inseriti nel PIC, oltre che nell'ambito di eventuali indagini/accertamenti da parte di organi esterni;
- garantire la corretta applicazione del Sistema disciplinare, in caso di mancato rispetto dei principi e dei protocolli contenuti nel Modello;
- prestare una fattiva collaborazione e rendere dichiarazioni veritiere ed esaustivamente rappresentative dei fatti nei rapporti con l'Autorità Giudiziaria;
- attenersi alle istruzioni impartite ai sensi del Regolamento UE/2016/679 e D.Lgs 196/03 in tema di trattamento dei dati personali e, in generale, a quanto definito nel Sistema Privacy Consip e nelle Istruzioni Operative;
- attenersi a quanto disposto dalle procedure aziendali e linee guida in materia di:
  - ✓ utilizzo del personal computer;
  - ✓ utilizzo della rete aziendale;
  - ✓ utilizzo della piattaforma di *e-procurement*;
  - ✓ gestione delle password;
  - ✓ utilizzo dei supporti magnetici e dei PC portatili;
  - ✓ utilizzo della posta elettronica;
  - ✓ utilizzo della rete internet e dei relativi servizi;
  - ✓ protezione dei dati personali e riservatezza del *know-how* della Società e delle Pubbliche Amministrazioni con cui la Società si trova ad operare;
  - ✓ ogni altra attività svolta mediante strumentazioni, piattaforme o sistemi informatici;
- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società e per le specifiche finalità assegnate;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;

- in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società o delle Pubbliche Amministrazioni coinvolte, informare tempestivamente il responsabile della funzione competente alla gestione dei relativi sistemi/dispositivi informatici e attenersi alla Procedura gestione delle violazioni dei dati personali (*data breach notification*);
- utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- impiegare sulle apparecchiature di Consip soltanto prodotti ufficialmente acquisiti dalla Società;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni di Consip.;
- in ogni caso osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici;
- non divulgare in alcun modo le notizie relative alle attività dei Sistemi Informatici dell'Amministrazione di cui i dipendenti di Consip vengano a conoscenza in relazione all'esecuzione delle Convenzioni in essere, ivi comprese le informazioni che transitano su apparecchiature di elaborazione dei dati;
- definire ed adottare opportune misure volte a garantire la massima riservatezza sulle informazioni raccolte negli archivi dei Sistemi Informativi, nonché le misure necessarie a garantire la sicurezza fisica e logistica dei Sistemi Informativi.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

- alterare documenti informatici, pubblici, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici e privati con cui Consip intrattiene rapporti nell'ambito della propria attività, al fine di alterare e /o cancellare dati e/o informazioni;
- detenere, utilizzare, diffondere, installare abusivamente apparecchiature, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di soggetti pubblici o privati con i quali la Società intrattiene rapporti nell'ambito della propria attività, al fine di acquisire informazioni riservate;
- detenere, utilizzare, diffondere, installare abusivamente apparecchiature, codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico o telematico di Consip o delle Pubbliche Amministrazioni al fine di acquisire informazioni riservate;

- svolgere attività di approvvigionamento, e/o produzione e/o diffusione, installazione di apparecchiature e/o software allo scopo di (a) danneggiare (*i*) un sistema informatico o telematico di soggetti pubblici o privati con i quali la Società intrattiene rapporti nell'ambito della propria attività, nonché (*ii*) le informazioni, i dati o i programmi in esso contenuti; ovvero allo scopo di (b) favorire l'interruzione, totale o parziale, o l'alterazione del loro funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, con i quali la Società intrattiene rapporti nell'ambito della propria attività, al fine di acquisire informazioni riservate;
- detenere, diffondere, installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o di soggetti pubblici o comunque di pubblico interesse;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblico interesse;
- introdurre e/o conservare applicazioni/software che non siano state preventivamente sottoposte al vaglio del responsabile della funzione competente alla gestione del relativo sistema informatico o la cui provenienza sia dubbia o sconosciuta;
- trasferire all'esterno di Consip e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà di Consip, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio superiore gerarchico;
- lasciare accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (parenti, amici, ecc.);
- utilizzare password di altri utenti aziendali, neppure per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile della funzione competente;
- utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

B.4 Owner del rischio: Referente aziendale

Sulla base della metodologia adottata per la costruzione del Modello, fondata sull'analisi dei processi per rischio-reato, ciascun referente aziendale è responsabile dell'effettiva applicazione

delle attività di controllo poste in essere per l'elenco dei reati previsti dal Decreto che, a livello teorico, è possibile siano commessi dai dipendenti di Consip, come riportato nell'Allegato "Matrice Rischio reato/referenti".

Tali referenti sono individuati nei responsabili delle Direzioni / Aree / coinvolte in ciascuna area a rischio-reato individuata.

B.5 Presidi di controllo e ruolo dell'Organismo di Vigilanza

Al fine di mitigare i rischi connessi alla realizzazione delle fattispecie di reato previste dal Decreto, la Società, nell'ambito del sistema di presidi di controllo, prevede l'attività di monitoraggio dell'Organismo di Vigilanza, che vigila sulla efficacia del Modello e sul rispetto delle prescrizioni ivi contenute.

L'OdV, nello svolgimento delle proprie funzioni, ha la facoltà, ove lo ritenga opportuno, di verificare il rispetto dei canoni comportamentali e dei protocolli aziendali da parte dei Destinatari, oltre che di richiedere tutte le informazioni e la documentazione ritenute necessarie per tali attività. A tal fine, l'OdV riceve anche appositi flussi informativi dalle strutture aziendali individuate sia nel Modello e relative Parti speciali, sia nelle procedure aziendali di riferimento.

Le attività di controllo sono condotte in un'ottica di integrazione e di coordinamento tra gli organi di controllo (Collegio sindacale - OdV – RPCT – DPO – GSOS); viene pertanto definito il Piano Integrato dei Controlli correttamente bilanciato tra i vari organi, che tiene conto degli audit effettuati dall'Internal Audit e delle verifiche verticali effettuate dai diversi organi di controllo, alternando la tipologia di analisi; tale Piano prevede una gestione integrata delle raccomandazioni e dei follow-up nonché controlli ciclici dei maggiori centri di rischio.