INDICE

Chimec S.p.A.

Modello di Organizzazione, Gestione e Controllo *ex* D. Lgs. n. 231 del 8 giugno 2001

PARTE SPECIALE "E"

I REATI INFORMATICI

Approvato dal Consiglio d'Amministrazione CHIMEC S.p.A. il 25 ottobre 2016
Aggiornamento del 12 novembre 2020

1. – I Reati informatici: profili generali

Oggetto della presente Parte Speciale sono quelle fattispecie di reato poste a tutela del c.d. "domicilio informatico", inteso quale luogo contenente dati appartenenti alla sfera individuale, nei confronti del quale è preclusa l'indebita ingerenza altrui.

Il domicilio informatico viene concepito come una espansione ideale dell'area di pertinenza del soggetto interessato (il legislatore riconosce lo *jus excludendi* del titolare che caratterizza il domicilio fisico) nel quale il titolare ha diritto a esplicare liberamente qualsiasi attività lecita all'interno del luogo informatico.

In ragione di un bene giuridico siffatto, i reati informatici vengono generalmente ricompresi nella categoria relativa ai delitti contro la persona o il patrimonio, ad eccezione della fattispecie di cui all'art. 491-*bis* c.p., la quale mira a tutelare (oltre il complesso dei dati afferente ad un determinato domicilio informatico) anche la genuinità del valore probatorio degli atti e dei dati contenuti in detto sistema.

Trattasi di delitti a natura dolosa, quindi sussistono necessariamente in capo all'agente i due requisiti cardine: consapevolezza del reato che si vuole commettere e volontà di realizzarlo (intesa come proposito di introdursi in un sistema precluso all'altrui accesso e/o accompagnato dall'intento di alterarne, distruggerne o diffonderne illegittimamente il contenuto).

2. – Reati di cui all'art. 24-*bis* D.Lgs. n. 231/2001

2.1. - Documenti informatici (art. 491-*bis* c.p.)

La norma - contenuta nel Libro II, Titolo VII, Capo III del codice penale che contempla i delitti contro la fede pubblica ovvero si riferisce ai c.d. reati di falso, nella forma materiale[1] o ideologica[2] (artt. 476 e ss c.p.) - stabilisce che "s*e 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*".

Il legislatore ha previsto tale ipotesi di reato per garantire il carattere probatorio di alcuni atti, quali quelli a c.d. fede privilegiata di cui agli artt. 2699 ss. c.c., nonché quello di qualsiasi documento cui l'ordinamento attribuisce un valore probante meritevole di tutela in virtù del contenuto dello stesso.

Ciò premesso, la fattispecie di cui all'art. 491-*bis* c.p. estende la punibilità prevista per i reati c.d. di falso anche quando, oggetto della condotta alternativa materiale o ideologica, siano i documenti informatici di appartenenza pubblica o privata.

2.2. - Accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.)

La norma punisce "*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*"

Il legislatore intende proteggere l'integrità del sistema, dei dati e dei programmi in esso contenuti, nonché – elemento più importante - la riservatezza dei dati e dei programmi contenuti nel sistema stesso.

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.

---

[1] Per "falsità materiale" (artt. 476 e 482 c.p.) deve intendersi quella condotta che alteri l'atto in un momento successivo alla sua formazione (ad. esempio: le modifiche, le aggiunte al documento oppure quando vi sia difformità tra l'autore apparente e quello reale).

[2] Per "falsità ideologica" (artt. 479 e 483 c.p.) deve intendersi quella condotta contraffattiva mediante l'apposizione di dichiarazioni o attestazioni non veritiere all'interno dell'atto.

Qualora i fatti sopra descritti 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.

La condotta materiale che il legislatore persegue consiste nell'introduzione o nel mantenimento abusivo - ovvero contro la volontà del titolare del domicilio informatico o di chi può escludere accessi indesiderati - all'interno di un sistema informatico o telematico protetto da *password* o altri titoli volti a permettere l'accesso solo agli utenti autorizzati in quanto muniti di apposite credenziali.

Sotto quest'ultimo profilo, va precisato che il reato in esame si configura anche quando i soggetti muniti di credenziali, accedano o si mantengano all'interno del sistema in violazione delle prescrizioni e dei limiti imposti dal titolare del domicilio informatico di riferimento.

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

La norma in esame sanziona l'abusiva acquisizione e diffusione, in qualsiasi modalità, dei mezzi o codici di accesso preordinati a consentire a soggetti non legittimati l'introduzione ad un sistema informatico o telematico altrui protetto da misure di sicurezza, disponendo "*chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo*".

La condotta dell'agente consistente nella ricezione, diffusione o riproduzione di *password* o credenziali in maniera abusiva ovvero senza il consenso del titolare - unico soggetto munito della facoltà di escludere taluno dall'utilizzo dell'impianto predetto - del sistema informatico violato e deve essere sorretta dallo specifico scopo di perseguire un profitto o, alternativamente, di cagionare un altrui danno.

2.4. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.)

La norma in esame prevede che "*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*".

Ai fini della configurabilità del presente reato è necessario che l'autore delle condotte tipizzate (commesse attraverso apparecchiature, dispositivi o programmi informatici) persegua lo specifico scopo di danneggiare o alterare illecitamente un sistema informatico o telematico.

2.5. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.)

La norma sanziona "*chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe*" e 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 punto precedente.

La norma estende la tutela della segretezza, libertà e riservatezza delle comunicazioni telefoniche e telegrafiche di cui all'art. 617 alle comunicazioni relative ad un sistema informatico o telematico o intercorrente tra più sistemi.

Si tratta di un reato a forma libera, quindi configurabile ogniqualvolta l'agente operi in maniera fraudolenta ovvero intenzionalmente intercetti - nel momento dinamico della loro trasmissione - comunicazioni intercorrenti tra più sistemi informatici o telematici.

Le altre due condotte punibili consistono nell'impedimento e nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, realizzati mediante il compimento di atti tali da impedire che una comunicazione abbia inizio e a farne cessare una in corso.

Il secondo comma punisce un altro tipo di condotta consistente nell'indebita divulgazione dei dati o dei fatti contenuti nelle comunicazioni non richiedendo come presupposto del reato l'intercettazione di comunicazioni tra due o più sistemi, pertanto essendo sufficiente che l'agente riveli, mediante qualsiasi mezzo, notizie riservate.

2.6. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.)

La norma punisce "*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*".

Tale norma riprende pedissequamente lo schema già adottato dal reato di pericolo di cui all'art. 617-*bis*, offrendo una tutela anticipata al bene che intende tutelare ovvero la segretezza e libertà delle comunicazioni informatiche o telematiche la cui offesa è sanzionata nel precedente articolo.

Le condotte punite connotate da dolo generico sono quelle prodromiche alla realizzazione di intercettazione, impedimento ed interruzione, quali ad esempio, la predisposizione di specifiche apparecchiature non autorizzate al fine di intercettare, ovvero intromettersi o interrompere qualsivoglia scambio di informazioni tra sistemi informatici.

É un reato di pericolo concreto (richiede l'accertamento giudiziale dell'effettiva potenzialità lesiva del materiale istallato) a consumazione anticipata, pertanto, si perfeziona nel momento in cui l'impianto illecito viene predisposto o installato sul sistema preso di mira dall'agente.

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

Salvo che il fatto costituisca più grave reato, è punito a querela della persona offesa "*chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui*."

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Il bene giuridico al quale la norma intende apprestare tutela è l'inviolabilità del possesso e della disponibilità dell' oggetto materiale della condotta ovvero l'integrità dei contenuti e dei *software*.

La condotta idonea a integrare il delitto in esame è a forma libera nel senso che può consistere in qualsiasi comportamento che alteri un sistema informatico, ovvero ne modifichi lo stato originario, renda inservibile l'elaboratore a nulla rilevando la possibilità che lo stesso possa essere ripristinato.

2.8. - Danneggiamento di informazioni, dati o 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, è punito "*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*".

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 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 struttura del delitto in oggetto si differenzia da quello di cui all'art. 635-*bis* c.p. esclusivamente per la circostanza che i sistemi informatici o telematici, presi di mira dall'agente e su cui si estende la condotta criminosa, sono utilizzati o appartengono allo Stato o ad altro Ente pubblico o comunque di pubblica utilità.

2.9. - Danneggiamento di sistemi informatici (art. 635-*quater* c.p.)

La norma punisce, 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*".

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 di reato si configura come un delitto a forma vincolata, incentrato sulla determinazione dell'inservibilità del sistema ovvero su una grave compromissione del suo funzionamento.

Il delitto in esame è realizzabile attraverso un'ampia pluralità di condotte di danneggiamento con un rinvio espresso a quanto descritto dall'art. 635-*bis* nonché attraverso l'introduzione, la trasmissione di dati, informazioni o programmi, mediante programmi virus o dati maligni introdotti nella rete in grado di rendere totalmente o parzialmente inservibili i sistemi informatici e telematici altrui.

Al fine della configurazione del delitto in esame, non sarà necessario che i dati aggrediti vengano totalmente distrutti, ma sarà sufficiente che ne venga alterato in maniera irreversibile l'ordinaria funzione e che la condotta posta in essere dall'agente renda irregolare e frammentario il funzionamento del sistema e dei servizi cui sono destinati.

2.10. - Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.)

La fattispecie in rubrica, richiamando la condotta analizzata nel paragrafo che precede, aggrava il trattamento sanzionatorio, quando la condotta sopra descritta sia "*diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.*"

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 scelta del legislatore è stata quella di garantire ai dati e ai sistemi di "pubblica utilità" una protezione più forte contro i danneggiamenti informatici, rispetto a quella stabilita per i dati e sistemi privati.

2.11. - Art. 640-*quinquies* c.p. (frode informatica del soggetto che presta servizi di certificazione di firma elettronica)

Tale reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Come risulta evidente si tratta di reato c.d. proprio, ovvero realizzabili solo da soggetti che possiedano la qualifica richiesta dalla norma.

2.12. - Trattamento sanzionatorio per le fattispecie di cui all'art. 24-*bis* del Decreto

In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

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

In relazione alla commissione dei delitti di cui agli articoli 491-*bis* e 640-*quinquies* del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

3. - Aree a rischio

Tenuto conto dell'attività principalmente svolta da Chimec, sono state individuate le seguenti aree a rischio:

- le attività svolte da tutti i Destinatari mediante l'utilizzo di sistemi informatici, del servizio di posta elettronica e dell'accesso ad Internet;
- le procedure di monitoraggio e d'intervento per la manutenzione e il funzionamento dei sistemi informatici di pertinenza di Chimec;
- le attività di controllo e di garanzia della sicurezza degli impianti informatici dell'Azienda;
- l'utilizzo di *software* e banche dati da parte di tutti i Destinatari;
- l'organizzazione e la gestione dei flussi informatici e telematici interni e/o esterni alla Società.

Le aree indicate assumono rilevanza anche nell'ipotesi in cui le attività sopra elencate siano eseguite, in tutto o in parte, da persone fisiche o giuridiche in nome e per conto di Chimec, in virtù di apposite deleghe o per la sottoscrizione di specifici rapporti contrattuali, dei quali deve essere tempestivamente informato l'OdV.

4. – Principi generali di comportamento e modalità di attuazione.

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da adottare per scongiurare la concretizzazione del rischio di commissione dei reati oggetto di analisi, dai quali deriverebbe l'attivazione del sistema sanzionatorio previsto dal Decreto ove venisse accertata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari[3] e, in particolare, ai soggetti esterni alla Società, nonché a tutti coloro che svolgono le proprie mansioni nelle aree di rischio segnalate nel paragrafo che precede.

La diffusione e l'attuazione di detti sistemi sono rimessi al Consiglio di Amministrazione di Chimec, in collaborazione con l'OdV.

Tutti i Destinatari sono tenuti a conoscere e rispettare le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico;
- il sistema disciplinare;
- le procedure afferenti i programmi di gestione per il corretto funzionamento dei sistemi informatici aziendali;
- i protocolli per la sicurezza dei flussi di comunicazione tra i sistemi aziendali interni ed esterni;
- i precetti relativi all'utilizzo di *software* e delle banche dati;
- le procedure interne a garanzia della sicurezza dei sistemi informatici e/o telematici.

E' fatto espresso divieto a tutti i Destinatari e i collaboratori esterni a Chimec - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di reati informatici.

È, altresì, vietato:

- diffondere le *password* o altre credenziali per l'accesso ai sistemi informatici di Chimec a chiunque – interno o esterno all'Azienda - non sia autorizzato all'utilizzo di detti impianti;
- possedere o utilizzare *software* e/o *hardware* che potrebbero danneggiare o compromettere la sicurezza dei sistemi e dei dati in essi contenuti;
- accedere e/o intrattenersi all'interno del sistema per scopi diversi da quali prettamente lavorativi e/o in violazione delle prescrizioni imposte dal titolare dell'impianto informatico;

[3] Per la definizione di "Destinatari", si rinvia alla Parte Generale del Modello, Glossario.

- modificare i *software* e/o gli *hardware* delle postazioni di lavoro in violazione dei precetti aziendali, ovvero senza autorizzazione della Società;
- sfruttare *password* e/o credenziali per manomettere le misure di sicurezza previste dal sistema per accaparrarsi dati o notizie riservate;
- alterare i dati pubblicati sul sito internet di Chimec;
- inviare dal proprio sistema informatico dati falsificati nel loro contenuto o in qualunque modo alterati;
- esercitare attività di *spamming* o qualsiasi risposta alla medesima;
- diffondere, a seguito di accesso non autorizzato nel sistema informatico dell'Azienda, informazioni o dati per i quali è vietata la pubblicazione.

Chimec si impegna a disporre, periodicamente, corsi di formazione e aggiornamento al fine di permettere, a tutti i Destinatari, la diffusione e la conoscenza di tutti i protocolli adottati dall'Azienda in relazione alla gestione e al funzionamento dei sistemi informatici.

Si impegna, altresì, a predisporre un apparato di controllo interno al fine di vigilare sulla sicurezza del sistema contro manomissioni o qualsivoglia comportamento lesivo di detti impianti e dei dati in esso contenuti.

Il Consiglio di Amministrazione di Chimec potrà prevedere ulteriori misure a maggiore tutela delle aree di rischio individuate e ad integrazione dei comportamenti sopra elencati.