PARTE SPECIALE "H"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE

Approvazione AD 1 dicembre 2017
Luigi Ferraris

INDICE

PARTE SPECIALE "H"

DEFINIZIONI 3

H.1 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto) E DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-nonies del Decreto) 6

H.1.1 LE TIPOLOGIE DI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto) 6

H.1.2 LE TIPOLOGIE DI DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-*nonies* del Decreto) 13

H.2 AREE A RISCHIO 16

H.3 DESTINATARI DELLA PARTE SPECIALE: PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE 18

H.4 PRINCIPI PROCEDURALI SPECIFICI 22

H.5 ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA 28

DEFINIZIONI

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale "H" qui di seguito indicate:

Amministratore della Macchina (AdM): Assegnatario della Postazione di Lavoro informatica (PdL) con privilegi di Amministratore locale.

Amministratori di basi di dati, Amministratori di reti e di apparati di sicurezza e Amministratori di applicazioni: non sono amministratori di sistema, ma godono di privilegi alti in relazione all'attività svolta. Sono, pertanto, equiparabili agli AdS dal punto di vista dei rischi relativi alla protezione dei dati.

Application *Owner*: figura aziendale con ampie responsabilità decisionali su un'applicazione, individuato di norma nel Process Owner o in un suo delegato.

Amministratore di Sistema (AdS): figura professionale finalizzata alla gestione tecnica ed alla manutenzione di un sistema di elaborazione o di sue componenti. Essendo Amministratore della Macchina su tutte le Postazioni di Lavoro può entrare in contatto con dati personali e/o riservati.
L'amministratore di Sistema possiede un livello di privilegio di accesso elevato alle risorse informatiche perché deve garantire la continuità di servizio e deve poter effettuare attività di amministratore e/o di operatore di sistema (es. amministratore di reti, di sistema operativo, di database, di applicazione, di controllo accessi, ecc.) necessarie alla gestione dell'infrastruttura sottesa ad un'applicazione/servizio (profilo sistemistico) o alla gestione dell'applicazione (profilo applicativo).
Le figure professionali alle quali sono concessi tali diritti amministrativi sono formalmente incaricate dall'azienda a mezzo di comunicazione scritta e sono altresì segnalate al team aziendale interno di Information Security.

Credenziali: l'insieme degli elementi identificativi di un utente o di un *account* (generalmente *UserID* e *Password*).

Dati Informatici: qualunque rappresentazione di fatti, informazioni, o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

Delitti in Violazione del Diritto d'Autore: i reati di cui all'art. 25 *nonies* del Decreto.

Delitti Informatici: i reati di cui all'art. 24-*bis* del Decreto.

Documento/i Informatico/i: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

L.A. o Legge sul Diritto d'Autore: Legge 22 aprile 1941 n. 633 sul diritto d'autore.

***Password*:** sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.

***Peer to Peer*:** meccanismo di condivisione di contenuti digitali tramite una rete di *personal computer,* di regola utilizzati per scambio di *file* con contenuti audio, video, dati e *software*.

Piano di Sicurezza: documento che definisce un insieme di attività coordinate che devono essere intraprese per implementare la politica di sicurezza del sistema.

Postazione di Lavoro: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.

Sicurezza Informatica: l'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.

Sistemi Informativi: l'insieme della rete, dei sistemi, dei *data base* e delle applicazioni aziendali.

***Spamming*:** invio di numerosi messaggi indesiderati, di regola attuato attraverso l'utilizzo della posta elettronica.

***Virus*:** programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.

H.1 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto) E DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-*nonies* del Decreto)

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati nella presente Parte Speciale "H", così come indicati agli artt. 24-bis e 25-nonies del Decreto. A tal riguardo si sottolinea che, nonostante le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

H.1.1 LE TIPOLOGIE DI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto)

- ***Falsità in documenti informatici (art. 491-bis cod. pen.)***

La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. 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 (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).

In particolare, si precisa che si ha "falsità materiale" quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente o sottoscrittore, con divergenza tra autore apparente e autore reale del documento (contraffazione) ovvero quando il documento è artefatto (e,

quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.

Si ha, invece, "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere.

Nel falso ideologico, dunque, è lo stesso autore del documento che attesta fatti non rispondenti al vero.

I Documenti Informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

A titolo esemplificativo, integra il delitto di falsità in Documenti Informatici la condotta di chi falsifichi documenti aziendali oggetto di flussi informatizzati o la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati "sensibili" in vista di una possibile attività ispettiva.

- **Accesso abusivo ad un sistema informatico o telematico (art. 615-ter cod. pen.)**

Tale reato si realizza quando un soggetto si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

A tal riguardo si sottolinea come il legislatore abbia inteso punire l'accesso abusivo ad un sistema informatico o telematico tout court, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

La suddetta fattispecie delittuosa si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema 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 informatici di proprietà di terzi (outsider hacking), per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, o 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 della società stessa.

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

Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.

L'art. 615-quater cod. pen., 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.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, Password o schede informatiche (quali badge o smart card).

Tale fattispecie si configura sia nel caso in cui il soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615-quater cod.pen., inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Potrebbe rispondere del delitto, ad esempio, il dipendente della società (A) che comunichi ad un altro soggetto (B) la Password di accesso alle caselle e-mail di un proprio collega (C), allo scopo di garantire a B la possibilità di controllare le attività svolte da C, quando da ciò possa derivare un determinato vantaggio o interesse per la società.

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

Tale reato si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Tale delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un Virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art.617-quater cod. pen.)**

Tale ipotesi di reato si configura qualora 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.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato potrebbe configurarsi, ad esempio, con il vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.

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

Questa fattispecie di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

La condotta vietata dall'art. 617-quinquies cod. pen. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.

Il reato si integra, ad esempio, a vantaggio della società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

- **Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen.)**

Tale fattispecie di reato si realizza quando un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

Il danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

- **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen.)**

Tale reato si realizza quando un soggetto commetta 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.

Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste 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.

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della società.

- **Danneggiamento di sistemi informatici o telematici (art. 635-quater cod. pen.)**

Questo reato si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis cod. pen., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.

Pertanto 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 cod. pen.

- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen.)**

Questo reato si configura quando la condotta di cui al precedente art. 635-quater cod. pen. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter cod.pen, quel che rileva è in primo luogo che il

danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

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

Questo 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 di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato cd. proprio in quanto può essere commesso solo da parte dei certificatori qualificati, o meglio, i soggetti che prestano servizi di certificazione di Firma Elettronica qualificata.

*****

Si precisa in ogni caso che la commissione di uno dei Delitti Informatici sopra descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno del dato/informazioni/programma/sistema informatico o telematico, possa determinare un interesse o vantaggio per TERNA.

Pertanto, nell'ambito della descrizione delle singole fattispecie criminose, così come nella successiva descrizione del Delitti in Violazione del Diritto d'Autore, si è tenuto conto di tale rilevante aspetto per l'elaborazione dei casi pratici proposti.

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei Delitti Informatici possono essere di natura pecuniaria, da 100 a 500 quote (considerato che il valore di ogni quota può essere determinato, sulla base delle condizioni economiche e patrimoniali dell'Ente, tra un minimo di Euro 258 ed un massimo di Euro 1549 e le stesse possono variare da un minimo di circa Euro 26.000 ad un massimo di circa Euro 800.000) e di natura interdittiva, che variano a seconda della fattispecie criminosa realizzata.

H.1.2 LE TIPOLOGIE DI DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-*nonies* del Decreto)

L'art. 25-novies contempla alcuni reati previsti dalla Legge sul Diritto d'Autore (e, in particolare, dagli artt. 171, 171-bis, 171-ter, 171-septies e 171-octies) quali, ad esempio, l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE; la riproduzione o il reimpiego del contenuto di banche dati; l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Da un'analisi preliminare è emersa l'immediata inapplicabilità a TERNA e alle Società del Gruppo delle fattispecie di cui agli artt. 171-ter, 171- septies e 171-octies L.A.

Si provvede pertanto a fornire qui di seguito una breve descrizione delle due fattispecie di cui all'art. 25-nonies del Decreto ritenute prima facie rilevanti per la Società, previste dagli artt. 171 comma 1 lett. a bis e comma 3, e 171 bis L.A.

- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 comma 1 lett. a bis e comma 3 L.A.)**

In relazione alla fattispecie delittuosa di cui all'art. 171, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

i. la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa;

ii. la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

Tale reato potrebbe ad esempio essere commesso nell'interesse di TERNA o di un'altra Società del Gruppo qualora venissero caricati sui siti *Internet* della Capogruppo o di una delle Società del Gruppo dei contenuti coperti dal diritto d'autore.

- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 bis L.A.)**

La norma in esame è volta a tutelare il corretto utilizzo dei *software* e delle banche dati.

Per i *software*, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".

Il reato in ipotesi si configura nel caso in cui chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.

Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Il secondo comma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati ovvero distribuisce, vende o concede in locazione una banca di dati.

Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicchè assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un *software* originale.

*****

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei Delitti in Violazione del Diritto d'Autore consistere possono essere di natura pecuniaria fino a 500 quote (e dunque fino ad un massimo di circa Euro 800.000) e di natura interdittiva, quali l'interdizione dall'esercizio dell'attività o la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito per una durata non superiore ad un anno.

H.2 AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, anche in relazione alle attività svolte per le altre Società del Gruppo, le aree ritenute più specificamente a rischio risultano essere, le seguenti:

Con specifico riferimento ai reati informatici:

1. gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica;
2. gestione dei flussi informativi elettronici con la pubblica amministrazione;
3. Approvvigionamento dei servizi IT e di ogni risorsa esterna il cui contratto inglobi l'utilizzo di una licenza informatica e/o di un servizio informatico (ad es. servizi cloud di tipo *software as a service – SaaS*) e/o preveda un'interazione con un sistema informatico di TERNA, da parte di strutture Terna che non abbiano al loro intero responsabilità in materia informatica;

Con specifico riferimento ai reati in violazione del diritto d'autore:

1. gestione dei contenuti del sito Internet di TERNA e dei *social media*, nonché gestione e organizzazione degli eventi.

Tutte le Aree a Rischio sopra individuate assumono rilevanza anche nell'ipotesi in cui le attività che ne costituiscono l'oggetto siano espletate – in tutto o in parte- in nome e/o per conto della Capogruppo dalle Società in virtù della sottoscrizione di contratti o di specifiche deleghe.

Per le attività espletate in nome e/o per conto della Capogruppo le Società devono effettuare le segnalazioni secondo le modalità nella Parte Generale e nelle singole Parti Speciali.

Nelle Aree a Rischio della Capogruppo vengono mappate – in via prudenziale- anche quelle attività che non sono effettuate in nome e/o per conto della Capogruppo e sono espletate dalle Società senza ingerenza nell'autonomia decisionale da parte della Capogruppo.

Tale scelta è ispirata a principi di massima prudenza per

assicurare che il Modello della Capogruppo copra aree di rischio anche per attività che vengono svolte dalle Società controllate.

In particolare si precisa che la Capogruppo riconosce alle Società, anche se sottoposte a direzione e coordinamento, piena autonomia gestionale, restando in capo alla responsabilità delle singole Società la piena rispondenza dei singoli modelli alla previsione di legge.

Le Società sono tenute ad evidenziare alla Capogruppo se nell'attività d'indirizzo strategico della stessa vengano formulati indirizzi che comportino criticità nell'applicazione del modello adottato.

Eventuali integrazioni delle Aree a Rischio potranno essere disposte dall'Amministratore Delegato di TERNA al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

H.3 DESTINATARI DELLA PARTE SPECIALE: PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE

Obiettivo della presente Parte Speciale è che i Destinatari si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di TERNA e delle Società del Gruppo – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici e di quelli commessi in violazione del diritto d'autore.

In particolare, la presente Parte Speciale ha la funzione di:

a. fornire un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

b. fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, gli Esponenti Aziendali sono tenuti, in generale, a rispettare tutte le regole e i principi contenuti, per le parti di proprio interesse, nei seguenti documenti:

1. Codice Etico;
2. Organigramma aziendale e schemi organizzativi;
3. Linea Guida LG018 sull'*Information Security Policy* – Indirizzi Strategici e relative applicazioni:
    - Glossario IS (R00LG018)
    - Uso accettabile delle risorse informative (R01LG018)
    - Avvio dell'Information Security Framework (R02LG018)
    - Creazione e mantenimento della postura di Sicurezza
    - dell'Information Security Framework (R03LG018)
    - Controllo degli accessi logici alle risorse informative (R04LG018)
    - Sicurezza della rete e delle comunicazioni (R05LG018)
    - Sicurezza fisica ed ambientale dei sistemi informativi (R06LG018)
    - La sicurezza delle informazioni nel "ciclo di vita" dei

dipendenti e nei rapporti con Terzi (R07LG018)
- Sicurezza degli asset IT (R08LG018)
- Security Incident Management (R09LG018)

4. Istruzione operativa che indica le modalità di Catalogazione della Tipologia delle Informazione (IO510SA);
5. Definizione delle attività Dell'*Information security Assessment* (IO515SA);
6. Nota interna che mappa i ruoli e le figure aziendali a cui sono assegnati Responsabilità e compiti nel Gruppo per la sicurezza delle Informazioni (NI067SA);
7. Regolamento sul ruolo, responsabilità e sui principali riporti dello Chief Risk Officer del Gruppo TERNA (LG044);
8. Linea guida che disciplina le modalità e l'*iter* autorizzativo da seguire per l'Approvvigionamento dei servizi IT (LG027);
9. Istruzione operativa che descrive le modalità di acquisizione dei servizi professionali informatici con utilizzo di Accordi Quadro e Contratti Chiusi, finalizzati alle attività di sviluppo del software applicativo, alle manutenzioni evolutive e all'esercizio (IO110RE);
10. Linea Guida che definisce i criteri per l'assegnazione e la gestione delle risorse informatiche e di comunicazione aziendale (LG015);
11. Istruzione operativa che descrive le modalità di gestione (creazione, modifica, revisione periodica e disabilitazione) delle credenziali di accesso ai servizi, agli applicativi, ai database ed ai sistemi operativi (IO317SI);
12. Istruzione operativa sulla Gestione delle Abilitazioni (IO309SI);
13. istruzione operativa sulla modalità di Gestione del *backup*, *restore* e dei supporti removibili (IO326SI);
14. Nota interna per l'identificazione dei Referenti nell'ambito della Direzione ICT (NI-ICT);
15. Manuale sulla gestione degli *Incident, Change, Problem Solving* nelle richieste di attività e manutenzione nelle

postazioni di lavoro e nella gestione dell'infrastruttura di competenza (IO311PM);

16. Istruzione operativa sul "Controllo Accessi – modalità di accesso alle sedi aziendali" (IO410SA);
17. Istruzione operativa che definisce gli adempimenti di gestione che interessano le c.d. figure di Amministratore di Sistema (IO513SA);
18. Istruzione operativa sulla Sicurezza della navigazione in internet e della posta elettronica (IO414SA);
19. Linea Guida sull'uso dei Social Media da parte del Personale del Gruppo Terna (LG045);
20. Linea Guida sull'affidamento di consulenze e incarichi per prestazioni professionali a terzi (LG025);
21. Linea Guida sull'affidamento ad operatore economico predeterminato (LG030).

Si sottolinea, inoltre, come TERNA abbia attribuito la massima rilevanza alla corretta individuazione e adozione di misure adeguate di sicurezza – di natura organizzativa, fisica e logica – in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o di distruzione delle risorse informatiche.

Al fine di raggiungere tale obiettivo, TERNA ha, infatti, adottato un approccio strutturato che si fonda in primo luogo sul documento "*Information Security Policy* – Indirizzi Strategici", approvato dall'Amministratore Delegato, che fissa tra l'altro gli obiettivi di sicurezza di TERNA, da sviluppare e perseguire attraverso uno schema omogeneo ed organico di documenti organizzativi ispirato alle *best practice* internazionali ed in particolare alle "aree di controllo" dello standard ISO/IEC 27000 e del NIST 800.

L'insieme organico di tali documenti - che determina, per le diverse aree di intervento, le regole a cui gli Esponenti Aziendali nonché i soggetti esterni, in funzione del rapporto che li lega a TERNA devono conformarsi – deve regolamentare rispettivamente:

- Il governo della sicurezza delle informazioni (relativo ad esempio, alla stesura dei Piani di Sicurezza dei sistemi informativi, alla segnalazione ed agli gestione degli

incidenti di sicurezza delle informazioni, alla formazione e sensibilizzazione per la sicurezza delle informazioni, etc.);

- I controlli di sicurezza specifici da applicare agli asset informativi (piattaforme e sistemi, applicazione, *database*, etc.);
- controlli di sicurezza indipendenti dalla tipologia di *asset*, volti ad indirizzare i comportamenti e le azioni operative degli Esponenti Aziendali (ad esempio in relazione all'uso accettabile delle risorse informative, alla gestione dei diritti di accesso alle risorse, alla tracciabilità degli eventi, etc.).

Accanto al rispetto dei principi procedurali specifici di cui al successivo paragrafo H.4, tutti i Destinatari sono pertanto tenuti al rispetto dei principi di comportamento contenuti nei documenti organizzativi al fine di prevenire la commissione dei Reati di cui agli artt. 24 -*bis* 25-*nonies* del Decreto.

H.4 PRINCIPI PROCEDURALI SPECIFICI

Al fine di garantire adeguati presidi nell'ambito delle singole Aree a Rischio, si prevedono qui di seguito le regole che devono essere rispettate da TERNA, dagli Esponenti Aziendali nonché dagli altri soggetti eventualmente autorizzati nell'ambito delle suddette aree, fermo restando che l'attuazione delle stesse è contenuta nelle *policy*, procedure aziendali e documenti organizzativi indicati, a titolo esemplificativo, al precedente paragrafo H.3.

In particolare, è vietato:

1) connettere ai sistemi informatici di TERNA, *personal computer*, periferiche e altre apparecchiature o installare *software* senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
2) procedere ad installazioni di prodotti *software* in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
3) modificare la configurazione *software* e/o *hardware* di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
4) acquisire, possedere o utilizzare strumenti *software* e/o *hardware* – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali *software* e/o *hardware* siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le Credenziali, identificare le vulnerabilità, decifrare i *file* criptati, intercettare il traffico in transito, etc.);
5) ottenere Credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate da TERNA;
6) divulgare, cedere o condividere con personale interno o esterno a TERNA e alle altre Società del Gruppo le proprie Credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

7) accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri Dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;

8) manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

9) sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

10) acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;

11) accedere abusivamente al sito Internet della Società al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali (immagini, infografica, video, ecc.) in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili;

12) comunicare a persone non autorizzate, interne o esterne a TERNA, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

13) mascherare, oscurare o sostituire la propria identità e inviare *e-mail* riportanti false generalità o inviare intenzionalmente *e-mail* contenenti *Virus* o altri programmi in grado di danneggiare o intercettare dati;

14) lo *Spamming* come pure ogni azione di risposta al medesimo;

15) inviare attraverso un sistema informatico aziendale informazioni o dati falsificati o, in qualunque modo, alterati.

TERNA si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1) informare adeguatamente i Dipendenti, nonché gli *stagisti* e gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, dell'importanza di:
   - mantenere le proprie Credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
   - utilizzare correttamente i *software* e banche dati in dotazione;
   - non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle *policy* aziendali;
2) prevedere attività di formazione e addestramento periodico in favore dei Dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore degli *stagisti* e degli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
3) definire nell'ambito del Codice Etico e delle *policy* di *Information Security* i comportamenti accettabili per l'utilizzo corretto dei *software* e delle banche dati;
4) far sottoscrivere ai Dipendenti, nonché agli *stagisti* e agli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;
5) informare i Dipendenti, nonché gli *stagisti* e gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla Postazione di Lavoro, con i propri codici di accesso;
6) impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

7) limitare gli accessi alle stanze *server* unicamente al personale autorizzato;

8) proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

9) dotare i sistemi informatici di adeguato *software firewall* e *antivirus* e far sì che, ove possibile, questi non possano venir disattivati;

10) impedire l'installazione e l'utilizzo di *software* non approvati da TERNA e non correlati con l'attività professionale espletata per la stessa;

11) informare gli utilizzatori dei sistemi informatici che i *software* per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;

12) limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di *Virus* capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti ad individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le Funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;

13) impedire l'installazione e l'utilizzo, sui sistemi informatici di TERNA, di *software Peer to Peer* mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, *Virus*, etc.) senza alcuna possibilità di controllo da parte di TERNA;

14) qualora per la connessione alla rete Internet si utilizzino collegamenti *wireless*, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a TERNA, possano illecitamente collegarsi alla

rete Internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai Dipendenti;

15) prevedere un procedimento di autenticazione mediante l'utilizzo di Credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti, degli *stagisti* e degli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;

16) limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Dipendenti, degli *stagisti* e degli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;

17) provvedere senza indugio alla cancellazione degli *account* attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;

18) prevedere, nei rapporti contrattuali con i Fornitori di servizi *software* e banche dati sviluppati in relazione a specifiche esigenze aziendali, clausole di manleva volte a tenere indenne TERNA da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi. Prevedere che negli stessi rapporti vengano sottoscritti specifici documenti con cui si impegnino al corretto utilizzo e alla tutela delle risorse informative aziendali con cui entrano in contatto.

Con specifico riferimento all'area a rischio di cui al capitolo H.2, punto 4), TERNA ha regolamentato le richieste di acquisizione di risorse esterne il cui contratto inglobi l'utilizzo di un servizio informatico (ad es. servizi *cloud* di tipo software as a service – SaaS) da parte di strutture TERNA che non abbiano al loro interno responsabilità in materia informatica. In particolare, le LG025 e LG030 prevedono l'inserimento di un *flag* che il richiedente deve spuntare ove il servizio richiesto preveda un'interazione o inglobi un servizio informatico con il conseguente invio di una richiesta di autorizzazione alle strutture ICT e Tutela Aziendale. Tale previsione garantisce, oltre che una

segregazione delle funzioni, anche un corretto *iter* autorizzativo e di acquisizione delle risorse esterne.

Per ciò che specificamente attiene i controlli aziendali, TERNA ha istituito – nell'ambito di Tutela Aziendale– la struttura *Security Operations Center (SOC)* con il compito di:

- monitorare centralmente in tempo reale, in collaborazione con le Direzioni/Funzioni interessate, lo stato della sicurezza operativa delle varie piattaforme ICT (sistemi e reti) di processo e gestionali del Gruppo, attraverso strumenti diagnostici e coordinare le relative azioni di gestione;
- monitorare centralmente in tempo reale i sistemi anti-intrusione e di controllo degli accessi ai siti aziendali e gestire le autorizzazioni;
- gestire progressivamente l'intero processo di identificazione ed autorizzazione all'accesso alle risorse ICT aziendali;
- gestire i processi/procedure di *escalation* interne ed esterne in occasione di situazioni di emergenza e/o crisi, con il supporto delle strutture responsabili interessate;
- produrre *report* a supporto del vertice aziendale;
- effettuare il monitoraggio dei sistemi di protezione attiva e passiva delle risorse umane e materiali del Gruppo.

H.5 ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui all'art. 24 -*bis* e 25-*nonies* del Decreto sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui all'art. 24 *bis* e 25 *nonies* del Decreto. Con riferimento a tale punto l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti di TERNA eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sui Delitti Informatici e/o sui Delitti in Violazione del Diritto d' Autore, ovvero in occasione di mutamenti nell'organizzazione aziendale e nell'attività in relazione al progresso scientifico e tecnologico;
- proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

TERNA garantisce l'istituzione di flussi informativi proceduralizzati tra l'OdV, i responsabili delle strutture competenti, i Referenti 231 ed ogni altro Esponente Aziendale ritenuto necessario che, in ogni caso, potranno essere sentiti dall'OdV ogni volta ritenuto opportuno.

In particolare, il *Data Protection Officer*, con cadenza annuale, trasmette all'OdV un apposito flusso informativo avente ad oggetto le misure adottate per garantire un livello di sicurezza adeguato al rischio, ai sensi del Reg. UE/2016/679, le eventuali criticità riscontrate e la formazione erogata in materia.

In ogni caso, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi

procedurali specifici contenuti nel capitolo H.4 della presente Parte Speciale ovvero violazioni sostanziali alle procedure, *policy* e normative aziendali attinenti alle aree sensibili sopra individuate.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti aziendali rilevanti per lo svolgimento dei propri compiti.