A.S. Roma S.p.A.

MODELLO ORGANIZZATIVO D.LGS. N. 231/01

PARTE SPECIALE 6

Delitti informatici e trattamento illecito di dati

INDICE

Premessa

La presente Parte Speciale 6 del Modello di Organizzazione, Gestione e Controllo (di seguito, anche solo 'Modello') di AS Roma S.p.A. (di seguito, anche solo 'Società') è riservata ai delitti informatici e di trattamento illecito di dati richiamati dall'art. 24 *bis* del D.Lgs. n. 231/2001 (di seguito, anche solo 'Decreto') e contiene:

- la descrizione delle fattispecie di reato rilevanti ai sensi del Decreto;
- l'indicazione delle aree/processi esposti ai rischi in materia informatica;
- l'illustrazione dei protocolli di controllo adottati dalla Società per ridurre il rischio di commissione dei reati informatici;
- i compiti dell'OdV.

Capitolo 1

I reati rilevanti ai sensi dell'art. 24 bis del D.Lgs. n. 231/2001

Ai sensi dell'art. 24 *bis* del Decreto, aggiunto dalla Legge 18 marzo 2008, n. 48, gli enti (intesi quali enti forniti di personalità giuridica, società ed associazioni prive di personalità giuridica) sono responsabili per i reati di seguito indicati.

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

Il reato sanziona chiunque si introduce abusivamente, da remoto o tramite mera accensione della macchina, in un sistema informatico o telematico protetto da misure di sicurezza. La norma sanziona altresì chi permane nel sistema contro la volontà espressa o tacita di chi sia titolare dello *ius excludendi*, perché il titolare ha revocato il consenso inizialmente prestato o perché l'agente ha compiuto operazioni diverse da quelle per le quali era stato autorizzato ad accedere (es. resta nel sistema oltre il tempo consentito oppure prende conoscenza di file ed informazioni per cui non si aveva l'autorizzazione, oppure compie operazioni diverse da quelle originariamente previste).
Il reato è aggravato se il fatto è commesso da un operatore di sistema, intendendosi per tale chi si viene a trovare, in ragione delle sue funzioni o della sua attività, in posizione di vantaggio, avendo la possibilità di accedere al sistema, alle sue aree riservate, e di controllarne le operazioni (es. un tecnico che si trova ad operare come programmatore, sistemista, analista dell'*hardware* o del *software* di un sistema

informatico o qualunque soggetto che per le funzioni svolte può intervenire su di esso).

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

Il reato sanziona 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 (ad es. *password*, chiavi meccaniche o tessere elettroniche), protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.
È prevista un'aggravante nel caso in cui il reato sia commesso da un operatore di sistema.

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

Il reato sanziona 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 (ad esempio immettendoli nella rete), comunica o consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici (quali ad esempio i virus o gli *spyware*).

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

Il reato sanziona chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe (come ad esempio nel caso di chi intercetta le comunicazioni di posta elettronica altrui ovvero di chi installa un software e lo utilizza per trasmissioni di dati

che non rientrano nello scopo per cui gli è stato assegnato un sistema informatico, provocando un rallentamento della rete informatica o il suo blocco).
Il reato è aggravato se commesso da un operatore di sistema.

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

Il reato in commento sanziona 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.
Il reato è aggravato se commesso da un operatore di sistema.

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

Il reato sanziona chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, non solo nel caso di distruzione mediante un mezzo fisico, ma anche nel caso in cui si utilizzino tecnologie informatiche quali virus e spamming.
Il reato è aggravato se commesso da un operatore di sistema.

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

Il reato sanziona chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità.
Il reato è aggravato se commesso da un operatore di sistema.

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

Il reato sanziona chiunque, mediante le condotte di cui all'art. 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.
Il reato è aggravato se commesso da un operatore di sistema.

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

La norma estende la punibilità all'ipotesi in cui il fatto di cui all'art. 635 *quater* sia diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Il reato è aggravato se commesso da un operatore di sistema.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.)

La frode informatica in danno dello Stato si configura quando, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti si ottenga un ingiusto profitto arrecando così un danno a terzi.
Il reato in parola si distingue dalla truffa in quanto l'attività fraudolenta ha a oggetto il sistema informatico e non la persona e può concorrere con il reato di accesso abusivo a un sistema informatico o telematico, previsto dall'art. 615 ter c.p.

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

Il reato sanziona 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.

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

L'art. 491 c.p. estende ai documenti informatici pubblici o privati aventi efficacia probatoria (*id est*, quelli in cui sia identificabile l'autore) i delitti in materia di falso

previsti dal capo III del Titolo VII del Libro II del codice penale, e segnatamente le seguenti fattispecie:

- Falsità materiale commessa dal Pubblico Ufficiale in atti pubblici (art. 476 c.p.) – è il reato commesso dal pubblico ufficiale che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero;
- Falsità materiale commessa dal Pubblico Ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.) – è il reato commesso dal pubblico ufficiale che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità;
- Falsità materiale commessa dal Pubblico Ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.) – si tratta del reato commesso dal pubblico ufficiale che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale;
- Falsità ideologica commessa dal Pubblico Ufficiale in atti pubblici (art. 479 c.p.) – si tratta del reato commesso dal pubblico ufficiale che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità;
- Falsità ideologica commessa dal Pubblico Ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.) – si tratta del reato commesso dal pubblico ufficiale che, nell'esercizio delle sue funzioni, attesta falsamente in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità;
- Falsità materiale commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.) – è il reato commesso da chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità;
- Falsità materiale commessa dal privato (art. 482 c.p.) – la fattispecie ricorre allorquando un privato, o un pubblico ufficiale fuori dell'esercizio delle sue funzioni, commettano uno dei reati di falso materiale previsti dagli artt. 476, 477 e 478 c.p., sopra richiamati;
- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.) – si tratta del reato commesso da chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità;

- Falsità in registri e notificazioni (art. 484 c.p.) – è il reato commesso da chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'autorità di pubblica sicurezza, o a fare notificazioni all'autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni;
- Falsità in scrittura privata (art. 485 c.p.) – è il delitto commesso da colui il quale, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera;
- Falsità in foglio firmato in bianco – atto privato (art. 486 c.p.) – è quel reato che commette chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, sempre che si faccia uso del foglio firmato;
- Falsità in foglio firmato in bianco – atto pubblico (art. 487 c.p.) – si tratta del reato commesso dal pubblico ufficiale che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato;
- Altre falsità in foglio firmato in bianco (art. 488 c.p.) – la fattispecie riguarda tutti gli altri casi di falsità su un foglio firmato in bianco diversi da quelli menzionati in un preciso articolo del codice penale;
- Uso di atto falso (art. 489 c.p.) – è il reato commesso da chiunque, senza essere concorso nella falsità, fa uso di un atto falso;
- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.) – la fattispecie ricorre nel caso in cui, in tutto o in parte, si distrugga, sopprima od occulti un atto pubblico o una scrittura privata veri.

In forza di quanto previsto dall'art. 493 c.p., le fattispecie riguardanti i pubblici ufficiali sono applicabili anche agli incaricati di pubblico servizio, relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

Capitolo 2

Le aree "a rischio reato"

Come evidenziato anche nella Parte Generale, all'esito della fase di *risk mapping* sono state identificate le cd. aree "a rischio reato", ovvero i processi e le aree aziendali in cui è stato ritenuto astrattamente sussistente il pericolo di commissione dei reati informatici e di trattamento illecito di dati richiamati dall'art. 24 *bis* del Decreto.

Qui di seguito, sono elencati sia i processi a rischio, sia i controlli vigenti in seno alla Società, ovvero gli strumenti adottati da AS Roma al fine di mitigare il rischio di commissione dei reati.

OMISSIS

Capitolo 3

Le procedure interne vigenti

Lo svolgimento delle attività nell'ambito delle aree "a rischio reato" di cui al precedente par. 6.3, deve avvenire nel rispetto, oltre che dei principi generali di comportamento di cui al successivo par. 6.5., delle procedure interne vigenti in seno alla Società.

Le procedure sono, inoltre, chiare ed efficaci, nonché adeguatamente diffuse presso tutti i livelli della Società, ivi compresi i soggetti in posizione apicale.

Le procedure sono redatte con l'eventuale supporto dei consulenti informatici esterni di AS Roma e sono soggette ad apposita revisione/aggiornamento - con cadenza annuale o comunque ogni qual volta si renda necessario in conseguenza di importanti mutamenti del sistema informatico della Società, di rilevanti novità normative ovvero di significative violazioni del Modello – a cura dell'Amministratore del Sistema IT con l'eventuale supporto dei consulenti esterni.

OMISSIS

Capitolo 4

Principi generali di comportamento

La presente Parte Speciale prevede l'**espresso obbligo**, a carico dei Destinatari del Modello:

- di osservare e rispettare tutte le leggi e regolamenti, anche di natura deontologica che disciplinano l'attività della Società, con particolare riferimento alle attività che comportano l'utilizzo di sistemi informatici o telematici;
- di garantire l'assoluto rispetto delle previsioni e delle prescrizioni del Modello, incluso per ciò che attiene i Protocolli ad esso connessi, tra cui il Codice Etico;
- di rispettare, in particolare, le procedure concernenti il corretto utilizzo dei sistemi informatici o telematici, incluse internet e la posta elettronica;
- di formalizzare per iscritto le condizioni ed i termini dei rapporti negoziali con i fornitori/appaltatori operanti nell'ambito della gestione dei sistemi informatici;
- di garantire la segretezza di password e codici identificativi degli eventuali account rilasciati da AS Roma o di cui si ha conoscenza in virtù delle attività e dei servizi svolti in nome e/o per conto di quest'ultima;
- di segnalare all'Organismo di Vigilanza qualsiasi possibile violazione del Modello o dei Protocolli connessi, incluso il Codice Etico, così come qualsiasi comportamento o condotta non conforme alle procedure/policy vigenti in materia di utilizzo dei sistemi informatici o telematici della Società.

La presente Parte Speciale prevede, conseguentemente, l'**espresso divieto** a carico dei Destinatari del Modello:

1. di porre in essere comportamenti tali da integrare le fattispecie di reato informatico previsti dall'art. 24 *bis* del Decreto;
2. di porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. di porre in essere comportamenti o condotte contrari, o comunque non conformi, alle procedure/policy della Società in materia di utilizzazione dei sistemi informatici o telematici;
4. di presentare o inviare in via telematica dichiarazioni o comunicazioni non veritiere alla Pubblica Amministrazione, o comunque di alterare in qualsiasi modo il contenuto delle dichiarazioni o comunicazioni stesse;
5. di utilizzare la user ID e/o la password di altro operatore.

A tal fine, sono previsti:

- la predisposizione e l'implementazione di specifiche procedure/policy interne concernenti l'utilizzo dei sistemi informatici o telematici della Società, e segnatamente, qualora presenti, l'utilizzo di dispositivi /apparecchiature/programmi che consentono di intercettare comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero ad impedirle o ad interromperle, ovvero a danneggiare/interrompere un sistema informatico telematico o i dati/programmi in esso contenuti;
- la conformità di tali procedure/policy rispetto al Codice in materia di Protezione dei dati personali (D. Lgs. 30 giugno 2003 n. 196) ed alle norme a tutela dei lavoratori (Legge 20 maggio 1970 n. 300);
- la nomina di un amministratore di sistema dotato dei requisiti di professionalità adeguati all'incarico conferito;
- il monitoraggio costante, a cura dell'amministratore di sistema, sull'utilizzo dei sistemi informatici e telematici della Società, volto a garantire la sicurezza dei sistemi e delle banche dati, nonché ad individuare ed inibire eventuali comportamenti illeciti;
- l'obbligo dell'amministratore di sistema di predisporre un report semestrale scritto, da inoltrare all'Organismo di Vigilanza, su eventuali criticità o anomalie concernenti l'utilizzo dei sistemi informatici o telematici della Società.

Capitolo 5

I compiti dell'Organismo di Vigilanza

OMISSIS