Milano Serravalle Engineering

PARTE SPECIALE "B"

REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI

Storico delle modifiche

Versione	***Data approvazione***	***Causale modifiche***	***Organo***
1.0	3 febbraio 2009	Prima emissione	CdA
2.0	5 marzo 2013	Aggiornamento reati presupposto e modifiche organizzative	CdA
3.0	20 dicembre 2018	Aggiornamento reati presupposto e modifiche organizzative	AU
4.0	23 luglio 2021	Aggiornamento reati presupposto	AU
4.1	4 marzo 2022	Disapplicazione della disciplina di cui al D.lgs. n. 33/2013 (Decreto Trasparenza) a seguito dell'ingresso della Società nel perimetro delle società controllate da FNM S.p.A., società quotata in Borsa	AU

INDICE

PARTE SPECIALE "B" – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI..... **3**

1 LE FATTISPECIE DEI DELITTI INFORMATICI RICHIAMATE DAL D.LGS. N. 231/2001 3
2 LE "ATTIVITÀ SENSIBILI" AI FINI DEL D.LGS. N. 231/2001 7
3 IL SISTEMA DEI CONTROLLI 7

PARTE SPECIALE "B" – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI

1 Le fattispecie dei delitti informatici richiamate dal D.Lgs. 231/2001

La Legge 18 marzo 2008 n. 48 ha introdotto, nel testo del D.Lgs. 231/01, l'art. 24 *bis* in base al quale:

1. 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;
2. 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;
3. 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, e dei delitti di cui all'articolo 1, comma 11, del D.L. 21 settembre 2019 n. 105, convertito in Legge 133/2019, si applica all'ente la sanzione pecuniaria sino a quattrocento quote;
4. 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)".

Di seguito si riporta una descrizione dei reati richiamati dall'art. 24-bis.

1.a. Documenti informatici (art. 491-bis c.p.)

"Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- *Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)*: "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni";
- *Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)*: "Il 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, è punito con la reclusione da sei mesi a tre anni";
- *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.)*: "Il 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, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni";
- *Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)*: "Il 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, soggiace alle pene stabilite nell'articolo 476";

- *Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)*: "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni";

- *Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)*: "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, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro";

- *Falsità materiale commessa da privato (art. 482 c.p.):* "Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo";

- *Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.):* "Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi";

- *Falsità in registri e notificazioni (art. 484 c.p.):* "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 è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00";

- *Falsità in scrittura privata (art. 485 c.p.):* "Chiunque, 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, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata";

- *Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.)*: "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, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito";

- *Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.):* "Il 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, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480";

- *Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)*: "Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private";

- *Uso di atto falso (art. 489 c.p.):* "Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno";
- *Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)*: "Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente";
- *Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)*: "Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti";
- *Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)*: "Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni".

1.b. Accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.)

Commette il delitto 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.

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

Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

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.

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

Commette il delitto 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.

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

Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

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.

1.f. Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

Compie il delitto 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.

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

Il delitto, salvo che il fatto costituisca più grave reato, consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui, da chiunque posta in essere.

1.h. 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 delitto, che può essere commesso da chiunque, consiste, salvo che il fatto costituisca più grave reato, nella commissione di 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.

1.i. Danneggiamento di sistemi informatici e telematici (art. 635 quater c.p.)

Il delitto, salvo che il fatto costituisca più grave reato, è commesso da chiunque, mediante le condotte di cui all'articolo 635 - bis c.p., 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.

1.l. Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies c.p.)

Il delitto è commesso se il fatto di cui all'art. 635-quater c.p. è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

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

Commette il delitto il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

1.n. Fattispecie di cui all'art. 1, comma 11, del D.Lgs. 105/2019

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 e all'ente, responsabile ai sensi del D.Lgs. 231/2001, si applica la sanzione pecuniaria fino a quattrocento quote.

2 Le "attività sensibili" ai fini del D.Lgs. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui al precedente punto, le attività "sensibili" di MSE.

Tali attività consistono in specie nella **gestione dei sistemi informatici aziendali**.

Riguarda le attività di gestione dei profili utente e del processo di autenticazione, gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno, la gestione e protezione delle reti e degli output di sistema e dei dispositivi di memorizzazione nonché la sicurezza fisica (cablaggi, dispositivi di rete, ecc.).

3 Il sistema dei controlli

Il sistema dei controlli, perfezionato dalla Società sulla base delle indicazione fornite dalle principali associazioni di categoria, quali le Linee guida Confindustria, nonché dalle "*best practice*" internazionali, prevede con riferimento alle attività sensibili e ai processi strumentali individuati:

- principi generali degli standard di controllo relativi alle attività sensibili;
- standard di controllo "specifici" applicati alle singole attività sensibili.

Alcune delle attività sensibili individuate sono gestite da direzioni e/o unità organizzative aziendali appartenenti ad altre Società del Gruppo.

Tali attività sono svolte in forza di contratti di servizio che regolano formalmente le prestazioni di servizi *intercompany*, assicurando trasparenza in merito agli oggetti delle prestazioni erogate ed ai relativi corrispettivi, determinati sulla base dei prezzi di mercato. Tali contratti prevedono l'impegno al rispetto dei principi di organizzazione e gestione idonei a prevenire la commissione degli illeciti ex d.lgs. n. 231/2001 da parte della Società affidataria.

Gli *standard* di controllo specifici, definiti per le attività sensibili individuate, sono quelli di seguito descritti nella PR 21 Gestione Sistemi Informativi e anche nell'IO 02 Assunzioni e un Regolamento Utenti, dove si definiscono i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. Nella medesima procedura Pr21 Sistemi informativi si definiscono i ruoli e le responsabilità per l'identificazione e la classificazione degli *assets* aziendali (ivi inclusi dati e informazioni) nonché le regole per l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

La PR 21 inoltre riporta le regole per***:***

- il corretto e sicuro funzionamento degli elaboratori di informazioni;
- la protezione da software pericoloso;

- il backup di informazioni e software;
- la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
- gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
- il controllo sui cambiamenti agli elaboratori e ai sistemi;
- la gestione di dispositivi rimovibili;
- la disciplina degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni.

In particolare, tale procedura prevede:

- l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
- le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
- una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
- la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
- la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
- l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
- la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
- la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
- la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
- i piani e le procedure operative per le attività di telelavoro.

La Società ha poi predisposto tutti i documenti necessari alla protezione dei dati personali (registro trattamenti e informative privacy etc.) e ha nominato il *Data Protection Officer* oltre che l'Amministratore di sistema.

Nel caso in cui una delle sopra elencate attività sensibili sia affidata, in tutto o in parte, a soggetti terzi appartenenti o meno al Gruppo in virtù di appositi contratti di servizio occorre che in essi sia prevista, fra le altre:

- la sottoscrizione di una dichiarazione con cui i terzi attestino di conoscere e si obblighino a rispettare, nell'espletamento delle attività per conto di MSE, i principi contenuti nel Codice Etico e gli standard di controllo specifici del Modello;

- l'obbligo da parte della società che presta il servizio di garantire la veridicità e completezza della documentazione o delle informazioni comunicate alla società beneficiaria;
- il potere dell'Organismo di Vigilanza di richiedere informazioni alla società che presta il servizio al fine di verificare il suo corretto svolgimento;
- la facoltà ad MSE di risolvere i contratti in questione in caso di violazione di tali obblighi.

Tutto quanto sopra illustrato dovrà tenere opportunamente conto, ai fini applicativi, della recente acquisizione della proprietà di Milano Serravalle – Milano Tangenziali S.p.A. e, correlativamente, di MSE da parte del Gruppo FNM, quotato in Borsa, e delle conseguenti relazioni infragruppo.