Sez. II

DELITTI INFORMATICI e TRATTAMENTO ILLECITO DEI DATI (art. 24 bis)

Art. 24-*bis* *Delitti informatici e trattamento illecito di dati*	1. In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-q*uater*, 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 peri casi di frode informatica in danno dello Stato o di altro ente pubblico, 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).

1. Premessa

In relazione alla possibile commissione dei reati informatici, ai sensi dell'art. 24 bis del decreto, ai fini del presente Modello, è opportuno chiarire cosa debba intendersi rispettivamente per "sistema informatico" e "sistema telematico".

Con l'espressione **"sistema informatico"** si fa riferimento in modo generico ad un computer o un insieme di più computer o altri apparati elettronici (es. router ecc...), tra loro interconnessi in rete. Esso si compone sia di elementi *hardware* che *software*.

Con l'espressione **"sistema telematico"** si fa riferimento ad una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche.

La fattispecie di reato in questione comprende una molteplicità di condotte criminose in cui un sistema informatico risulta essere, talvolta, obiettivo stesso della condotta, talvolta, lo strumento attraverso il quale l'autore intende realizzare altre fattispecie di reato penalmente rilevanti.

2. AVIS Comunale di Legnano e sicurezza dei sistemi IT

L'AVIS Comunale di Legnano si caratterizza della presenza di 24 personal computers, dotati di meccanismi di protezione e di impostazioni standards di sicurezza al fine di:

1. tutelare e conservare i dati informatici in essi contenuti – alcuni dei quali peraltro aventi natura di dati "sensibili" (es. dati concernenti i donatori di sangue);

2. limitare, o meglio impedire, il più possibile, l'accesso da parte di terzi non autorizzati ai dati interni, impedendo dunque un accesso virtuale c.d. "abusivo", non solo con adozione di *software antivirus* ma anche con l'adozione di *meccanismi di sicurezza* quali utilizzo di password (di adeguata complessità) e crittografia dei dati. In particolare, l'AVIS Comunale di Legnano si denota di uno specifico *software meccanico "FIREWALL",* sottoposto a costante aggiornamento automatico e periodico, che impedisce l'accesso a determinati e specifici siti internet e protegge il sistema da attacchi esterni.

Al fine di perseguire i summenzionati principali obiettivi, l'AVIS Comunale di Legnano – conformemente a quanto previsto dal *Documento "Organigramma e responsabilità" (Doc. M.Q. 5.0),* dalla *Procedura Generale Gestione informatica" (PG 7.3)* e documentazione ad esse connesse - ha:

- predisposto un programma "Gestione Avis Legnano" tale da ottemperare alle esigenze associative, alle necessità della gestione dei donatori (chiamate, visite periodiche, controlli e donazioni effettuate), agli adempimenti richiesti dalla gestione dell'UdR e dalle Convenzioni poste in essere ed un programma di gestione amministrativa;

- Associato a ciascun utente ruoli e profili specifici (nella specie: la gestione informatica dei donatori spetta all'area amministrativa ed a quella infermieristica; accesso ai dati e loro elaborazione è regolato da password personale)

- Per il programma di gestione Avis Legnano: Predisposto il back up dei dati, operante due volte al giorno, con registrazione dei dati su nastro magnetico. Tali PROCEDURE di BACK UP sono regolarmente documentate e custodite: due volte al giorno, al fine di garantire la sicurezza dei dati, viene effettuato un salvataggio di tutto il programma "Gestione Avis Legnano su nastro magnetico; i nastri sono riposti in armadio chiuso (contenuti in una cassetta ignifuga) le cui chiavi sono in possesso del R.A.A. (altresì responsabile del corretto funzionamento delle apparecchiature informatiche e del sistema di sicurezza dati back up , nonché del'inserimento numerico nel data-base Avis Legnano in ordine alla pianificazione e programmazione esami di controllo e donazioni) o di un suo delegato (copia delle chiavi le ha la Direzione). Una cassetta di backup e una chiavetta di backup, aggiornati una volta al mese, sono custoditi a casa del vicepresidente per una ulteriore sicurezza contro la perdita dei dati (es. furto, incendio)

- Adottato software antivirus - quale nella specie il "Symantec Endpoint Protection" – le cui misure di sicurezza sono periodicamente aggiornate in automatico (live up date);

- Per il programma di gestione amministrativa (installato su un portatile) anch'esso protetto dall'Endpoint Protection: predisposto un salvataggio giornaliero su chiavette custodito nello stesso armadio e cassetta dei nastri magnetici.

- Individuato un Responsabile di Sicurezza IT ed un Responsabile addetto agli aggiornamenti dei software (il quale procede altresì a test sulla sicurezza);

- Configurato in modo sicuro i browser web e i programmi mail;

- Ha predisposto un Piano di Emergenza indicante tutti i casi di emergenza prevedibile (es. perdita dei dati, interruzione della funzionalità di Internet, blocca caselle di posta elettronica e così via), appositamente specificato nella *"Procedura Generale di emergenza"* (PG 7.7).

La responsabilità dell'applicativo informatico è del Direttore Generale.

Si rileva per altro una circostanza del tutto peculiare del sistema informatico delle AVIS e quindi anche dell'AVIS Comunale di Legnano consistente in particolare nell'usufruire ed accedere al ***Sistema software "EMONET"*** dotato di una propria rete di computer connessi con il server dell'ASST, con una linea diretta e una di backup, e da qui con tutti i servizi trasfusionali della regione .
Tale software, con diffusione sul territorio nazionale, si integra con i principali sistemi informativi ospedalieri ed interagisce sul territorio con le unità di raccolta del sangue e con le associazioni dei donatori.
Esso è utilizzato per la gestione completa del servizio trasfusionale e favorisce una completa tracciabilità del ciclo trasfusionale (dalla raccolta delle donazioni alla loro lavorazione, conservazione, distribuzione e trasfusione), consentendo così un "buon uso" del sangue in termini di sicurezza trasfusionale, di efficienza ed efficacia del servizio e garantendo la massima sicurezza del paziente ed agevolando il lavoro dei vari attori /operatori del processo trasfusionale.
Esso in effetti si sostanzia in una piattaforma informatica (base dati) unica nella quale confluiscono le informazioni provenienti dai diversi operatori dislocati sul territorio.

3. Identificazione della Attività Sensibili

Le attività sensibili in occasione delle quali sono astrattamente verificabili i reati ex 24 bis del Decreto corrispondono con tutti gli ambiti e funzioni associative.

In particolare, ai sensi dell'art. 6 del Decreto, ed in ragione di quanto evidenziato nel paragrafo che precede, le "Attività Sensibili" ricorribili presso l'AVIS Comunale di Legnano in relazione ai reati di cui all'art. 24 bis del Decreto, attengono alle attività realizzate per mezzo di dipendenti o in collaborazione di soggetti esterni utilizzanti le tecnologie dell'informazione e concernono in particolare:

- ✓ La Gestione di accessi, account e profili: gestione dei servizi IT (trattamento di banche dati e/o dati informatici; tenuta dei registri);
- ✓ La Gestione dei sistemi hardware e software;
- ✓ La Gestione dell' accesso ed utilizzo Sistema Software EmoNet (da parte dei dipendenti AVIS Comunale di Legnano).

4. Reati applicabili

Sulla base delle analisi condotte – rilevate le misure di sicurezza IT adottate dall'AVIS di Legnano, l'accessibilità seppur limitata e controllata ai dati interni ed esterni - sono considerati applicabili alla Associazione i seguenti delitti informatici:

 Falsità in documenti informatici (art. 419 bis c.p.)

Tale ipotesi di reato si configura nei confronti di chiunque falsifichi un documento informatico pubblico o privato.
Per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Analisi/valutazione di rischio

Livello di rischio	Processi sensibili	Contromisure (protocolli)
Medio	Accesso ad account	L'AVIS Comunale di Legnano,

Di regola l'AVIS Comunale di Legnano, essendo in possesso di pc posti nella disponibilità del personale ed usufruendo del sistema informatico è potenzialmente ed esattamente sottoposta al rischio dei reati ex at. 24 bis del decreto.		come già anticipato, provvede alla: - adozione di un sistema di controllo interno con procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche; modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione; aggiornamento regolare dei sistemi informativi in uso, procedura di rimozione delle credenziali (rimozione del diritto di accesso) al termine del rapporto di lavoro da parte dell'ufficio amministrazione. - quanto all'accesso emoNet, l'AVIS legnanese provvede alla responsabilizzazione e formazione del personale addetto.

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

Costituito dalla condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma anche minima di barriere ostative all'ingresso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.

Tale delitto si perfeziona con la violazione del "domicilio informatico" e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature utilizzanti tecnologie informatiche(caratterizzate da un'attività di codificazione e decodificazione dalla registrazione o memorizzazione attraverso impulsi elettrici, su supporti adeguati, di dati.), senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa.

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

Costituito dalla condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiavi o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

Analisi/valutazione di rischio

Livello di rischio	Processi sensibili	Contromisure (protocolli)
Medio Di regola l'AVIS Comunale di Legnano, in persona del	Accesso ad account; Accesso ai software interni ed alla documentazione oggetto	L'AVIS Comunale di Legnano, come già anticipato, provvede alla:

dipendente addetto all'accoglienza e alla trasfusione, nello svolgere la propria attività può entrare nella disponibilità di dati particolarmente sensibili del socio-donatore (si pensi alla contrazione di una malattia da parte di quest'ultimo) Rischio: -abusiva diffusione di dati tali da consentire a terzi di entrare della disponibilità di quanto sopra.	di archiviazione da parte dell'ente. Accesso al Software Emonet ed introduzione di dati errati o non veritieri	- adozione di un sistema di controllo interno con procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche; modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione; aggiornamento regolare dei sistemi informativi in uso, procedura di rimozione delle credenziali (rimozione del diritto di accesso) al termine del rapporto di lavoro. - quanto all'accesso emoNet, l'AVIS legnanese provvede alla responsabilizzazione e formazione del personale addetto.

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

Costituito dalla condotta di chi per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altre apparecchiature, dispositivi o programmi informatici.

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

Costituita dalla condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi o le impedisce o le interrompe, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

Integra la medesima fattispecie – salvo che il fatto costituisca più grave reato - anche la diffusione al pubblico, mediante qualsiasi mezzo informatico, del contenuto delle predette comunicazioni.

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

Costituito dalla condotta di chi , 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.

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

Costituito dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato (es. cancellazione di dati dalla memoria di un pc).

l'elemento psicologico di tale reato si sostanzia nella coscienza e volontà di danneggiare. detto reato sussiste anche laddove l'azione sia stata posta in essere non al diretto scopo di nuocere, bensì quale mezzo per conseguire uno scopo diverso.

 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).

Costituito dalla condotta di chi 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, salvo che il fatto non costituisca più grave reato.

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

Costituito dalla condotta di chi, mediante la condotta di cui all'art. 635 bis, ovvero attraverso l'interruzione 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, salvo che il fatto costituisca più grave reato.
Tale danneggiamento pertanto si concretizza/attua o attraverso l'introduzione o la trasmissione di dati informazioni o programmi oppure con distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici.
 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

Costituito dalla condotta descritta al precedente art. 635 quater c.p., qualora essa sia diretta a distruggere , danneggiare, rendere, in tutto o in parte, inservibili i sistemi informatici o telematici di pubblica utilità o ad ostacolare gravemente il funzionamento.

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

Costituito dalla condotta del 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.

Analisi/valutazione del rischio

Livello di rischio	Processi sensibili	Contromisure (protocolli)
Medio – Alto	Utilizzo delle prestazioni PC e del sito internet	Rispetto del DPS in merito ai collegamenti a Internet. Divieto di istallazione sul personal computer di programmi di duplicazione o asportazione di programmi installati, salvo espressa autorizzazione dei preposti. Divieto di fare uso per esigenze personali dei computer dei fax delle stampanti e delle fotocopiatrici

		aziendali. Divieto di: a)effettuare il download di software o di files musicali nè la tenuta di files nella rete interna che non abbiano stretta attinenza con lo svolgimento delle proprie mansioni cui adibiti; b) utilizzare per ragioni personali, tranne espressa autorizzazione scritta, servizi di posta elettronica o di rete né così corrispondere con gli utenti dei servizi educativi formativi o socio assistenziali senza l'autorizzazione degli esercenti la potestà sugli utenti minorenni; c) inviare messaggi di posta elettronica dalle postazioni di lavoro o riceverne nelle caselle di posta elettronica neppure ricorrendo a sistemi di web mail; d) compiere atti diretti ai sottrarsi dai controlli sull'utilizzo della posta elettronica e di Internet che l'ente possa effettuare in conformità alla legge anche saltuari od occasionali, sia in modalità collettiva che su nominativi singoli dispositivi e postazioni; e) compiere atti diretti ad impedire la continuità dell'attività lavorativa mediante l'utilizzo della posta elettronica e di internet in caso di loro assenza; f) utilizzare la posta elettronica ed internet per effettuare acquisti o impartire disposizioni di pagamento o la fatturazione a loro carico.