PARTE SPECIALE "D"

Reati Informatici e trattamento illecito dei dati

Delitti in materia di violazione del diritto d'autore

Carpi,

1. REATI RICOMPRESI NELLA PRESENTE ANALISI, PROTOCOLLI DI PREVENZIONE E DI SUCCESSIVO CONTROLLO

La Parte Speciale "D" trova applicazione per le tipologie specifiche di reati previste ai sensi degli artt. 24*bis e 25nonies* del decreto, ossia per i delitti informatici, di illecito trattamento di dati e per i delitti in materia di violazione del diritto d'autore.
Per i reati di cui sopra all'ente si applicano le seguenti sanzioni pecuniarie:

- per il delitto di falsità in un documento informatico pubblico o avente efficacia probatoria previsto dall'art. 491 bis c.p., la sanzione pecuniaria sino a quattrocento quote;
- per il delitto di accesso abusivo ad un sistema informatico o telematico previsto dall'art. 615 ter c.p., la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici previsto dall'art. 615 quater c.p., la sanzione pecuniaria sino a trecento quote;
- per il delitto di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico previsto dall'art. 615 quinquies c.p., la sanzione pecuniaria sino a trecento quote;
- per il delitto di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche previsto dall'art. 617 quater c.p., la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di danneggiamento do informazioni, dati e programmi informatici previsto dall'art. 635 bis c.p., la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità previsto dall'art. 635 ter c.p., la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di danneggiamento di sistemi informatici o telematici previsto dall'art. 635 quater c.p., la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità previsto dall'art. 635 quinquies c.p., la sanzione pecuniaria da cento a cinquecento quote;
- per il delitto di frode informatica del soggetto che presta servizi di certificazione di firma elettronica previsto dall'art. 640 quinquies c.p., la sanzione pecuniaria sino a quattrocento quote;
- in relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a bis) e terzo comma, 171 bis, 171 ter, 171 septies, 171 octies della legge 22 aprile 1941 n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore

ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941.

****

n.	RIFERIMENTO	REATO PRESUPPOSTO
1	**Art.24bis D.Lgs. 231/2001**	**Art. 491 bis c.p. (Falsità in un documento pubblico o avente efficacia probatoria)**
ANALISI FATTISPECIE	Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.	

La norma, facendo rimando alla definizione che di tale atto fornisce l'art. 1, lett. p), d.lgs. 7 marzo 2005, n. 82, contenente il codice dell'amministrazione digitale, attribuisce la natura di documento informatico ad ogni "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", a prescindere dal supporto (disco fisso, floppy disk, nastro, CD, disco ottico, mail, cloud…) in cui sono contenuti i dati. La tutela penale del documento informatico è circoscritta a quelli aventi <<efficacia probatoria>>, caratteristica rinvenibile negli artt. 20 e seguenti del codice dell'amministrazione digitale, ove vengono dettagliati gli effetti giuridici e la rilevanza probatoria dei documenti informatici, formati nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore e l'integrità del documento.

Per quanto riguarda la definizione di documento informatico pubblico è importante ricordare che agli effetti delle norme sul falso documentale il concetto di atto pubblico è più ampio rispetto a quello che si desume nell'art. 2699 c.c., in quanto comprende non soltanto quei documenti che sono redatti con le richieste formalità da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede, ma anche i

documenti formati dal pubblico ufficiale o dall'incaricato di un pubblico servizio nell'esercizio delle sue funzioni, attestanti fatti da lui compiuti o avvenuti in sua presenza ed aventi attitudine ad assumere rilevanza giuridica.

L'elemento soggettivo richiesto si differenzia a seconda della natura, pubblica o privata, dell'atto oggetto di falsificazione. Nel primo caso è sufficiente il dolo generico, bastando cioè la consapevolezza e volontà di alterare la veridicità dei dati presenti nell'atto, senza che venga richiesto né l'*animus nocendi*, né *l'animus decipendi*, in quanto il reato è perfetto anche quando la falsità sia compiuta senza l'intenzione di nuocere ed addirittura anche quando la sua commissione sia accompagnata dalla convinzione di non procurare un vantaggio a sé o ad altri (o di arrecare un danno ad altri) o addirittura con lo scopo di rimediare ad un precedente errore. Quando l'atto ha natura di documento privato, invece, per la punibilità a titolo di falso occorre il dolo specifico, giacchè l'azione falsificatoria del colpevole dev'essere determinata dal fine di procurare a sé o ad altri un vantaggio o recare ad altri un danno.

L'ente può essere ritenuto responsabile solo nel caso in cui il reato sia stato posto in essere nel "suo interesse e vantaggio" da parte di soggetti apicali o sottoposti alla direzione e vigilanza di quest'ultimi, ovvero da uno dei soggetti che rientrano nelle categorie indicate negli artt. 6 e 7, d.lgs. 231/2001. Di talchè la necessità di accertare il soggetto che abbia commesso la falsificazione dei documenti informatici è il profilo tecnico più problematico, a causa della loro tendenziale <<accessibilità>> da parte di una pluralità di utenti non facilmente identificabili.

Il trattamento sanzionatorio prevede l'applicazione all'ente, in caso di riconosciuta responsabilità, della sanzione pecuniaria sino a quattrocento quote nonché delle sanzioni interdittive del divieto di contrattare con la pubblica amministrazione, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi o la revoca di quelli già concessi ed il divieto di pubblicizzare beni o servizi.

Ad esempio, un componente del Consiglio di Amministrazione di Valvole Italia potrebbe rubare la smart card necessaria per utilizzare la firma digitale di un amministratore delegato di un'azienda concorrente, al fine di modificare un documento informatico avente valore legale.

n.	RIFERIMENTO	REATO PRESUPPOSTO
2	**Art. 24bis D.Lgs. 231/2001**	**Art. 615-ter c.p. (Accesso abusivo ad un sistema informatico o telematico)**
ANALISI FATTISPECIE	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, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.	

La norma de quo prevede la punizione:

- di colui che si introduce abusivamente, cioè senza il consenso del titolare dello *ius excludendi* in un sistema informatico o telematico munito di sistemi di sicurezza (es. password, firewall);

- di colui che permane in collegamento con il sistema stesso continuando a fruire dei servizi resi o ad accedere alle informazioni in esso custodite, nonostante il titolare abbia esercitato, sia pur tacitamente, lo *ius excludendi*.

Per "sistema informatico" si intende qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati (si è ritenuto, ad esesmpio, che anche un personal computer o uno smartphone possono essere considerati veri e propri sistemi, per la ricchezza dei dati contenuti).

Per “sistema telematico”, invece, si deve intendere qualsiasi rete di telecomunicazione sia pubblica sia privata, locale, nazionale o internazionale, operante da o per l’Italia. Di conseguenza rientrano nell’oggetto tutelato anche le reti aziendali (LAN).

Il bene giuridico tutelato è la riservatezza informatica, ovvero, più precisamente, il <<domicilio informatico>> inteso quale spazio fisico ed ideale che è di pertinenza della sfera individuale personale tutelata dalla Costituzione, con riferimento a dati di carattere sia personale che patrimoniale.

Il reato si consuma e deve ritenersi perfetto al momento dell’abusiva introduzione ovvero dell’indebito trattenimento nel sistema informatico o telematico, senza che sia necessario che l’agente duplichi o acquisisca dati o informazioni.

Per la sussistenza dell’illecito è necessario che il sistema <<vulnerato>> risulti protetto da misure di sicurezza, anche se non sono necessarie specifiche misure di protezione informatica così come non occorre che le misure di sicurezza siano attive, ritenendo la giurisprudenza sufficienti anche misure di carattere organizzativo, che cioè disciplinino le modalità di accesso ai locali in cui il sistema è ubicato ed indichino le persone abilitate al suo utilizzo. Anche forme di protezione <<fisica>> (dalla semplice chiave per l’accensione del computer o il badge per accedere ai locali a sistemi più sofisticati quali l’impronta digitale, il timbro della voce o il riconoscimento dell’iride) rappresentano pertanto misure di sicurezza la cui violazione è idonea ad integrare il reato.

L’elemento psicologico richiesto per il perfezionarsi del reato è il dolo generico, consistente nella consapevolezza ed intenzionalità dell’ingresso o della permanenza in un sistema informatico protetto nonostante il soggetto agente fosse a conoscenza dalla contraria volontà, espressa o tacita, dell’avente diritto.

Fra le aggravanti richiamate dall’art. 615 ter c.p. particolare rilevanza ha quella consistente nell’abuso dell’operatore di sistema, di cui al 2° comma, n.1, ultima parte. Tale aggravio di pena è previsto poiché il *system operator* si viene a trovare, in ragione della sua attività, in un’evidente posizione di vantaggio, potendo accedere al sistema, ad aree riservate dello stesso e controllarne le operazioni, così da rendere più semplice la commissione del reato.
Trattasi di reato comune che in quanto tale può essere commesso da chiunque.

La sanzione prevista è quella pecuniaria da cento a cinquecento quote ed è inoltre prevista l’applicazione delle sanzioni interdittive dell’interdizione dell’esercizio dell’attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia potrebbe accedere, anche indirettamente tramite un apposito programma (“spyware”), al computer di un’azienda concorrente al fine di visualizzare i termini dell’offerta che quest’ultima intende presentare ad una gara d’appalto alla quale anche Valvole talia intende partecipare.

n.	RIFERIMENTO	REATO PRESUPPOSTO
03	Art.24bis D.Lgs. 231/2001	Art. 615-quater c.p. (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)
ANALISI. FATTISPECIE	Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164,00. La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.	

Trattasi di reato di pericolo che reprime, in un'ottica preventiva, l'abusiva acquisizione o diffusione, con qualsiasi modalità, dei mezzi o codici di accesso ad un sistema informatico o telematico protetto da misure di sicurezza

Con il termine "procurarsi" il Legislatore ha voluto far riferimento sia all'appropriarsi fisico della chiave meccanica o della scheda magnetica sia all'individuazione dei codici di accesso attraverso procedimenti logici tipici del computer.

Con il termine "riprodurre" il Legislatore ha voluto far riferimento alla realizzazione di una copia abusiva di un codice di accesso, idonea all'uso.

Il bene giuridico tutelato dall'art. 615 quater c.p. va identificato nella libera ed esclusiva disponibilità delle procedure che consentono l'accesso ai sistemi informatici da parte dell'avente diritto, evitando indebite intrusioni da parte di terzi.

Rispetto al delitto di cui all'art. 615 ter c.p., che pure tutela il domicilio informatico, vi è un'ulteriore anticipazione della soglia di tutela poiché il reato in parola sanziona condotte che riguardano i codici di accesso e non direttamente i sistemi informatici che con tali codici possono essere violati.

E' prevista una sanzione pecuniaria fino a trecento quote, oltre all'applicazione delle sanzioni interdittive della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia si potrebbe procurare un codice d'accesso (password, smart card, ecc.) idoneo ad introdursi da remoto nella rete aziendale di una società concorrente.

04	Art.24bis D.Lgs.231/2001	Art. 615-quinquies c.p. (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)
ANALISI FATTISPECIE	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, è punito con la reclusione fino a due anni e con la multa sino a € 10.329,00.	

La norma punisce la condotta di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Il bene giuridico tutelato è individuato nel diritto a godere in maniere completa e indisturbata di sistemi e programmi informatici senza che gli stessi rischino di subire danni illeciti quali, ad esempio, quelli provocati dalla diffusione dei cosiddetti "virus", che minano la funzionalità dei sistemi nei quali riescono ad introdursi. La protezione del bene giuridico avviene in via preventiva, in quanto si puniscono condotte prodromiche al danneggiamento del sistema anche se il programma nocivo non ha ancora prodotto i suoi effetti.

Il reato richiede, sotto il profilo soggettivo, il dolo specifico, nel senso che le condotte sono vietate e punite solo se poste in essere allo scopo – alternativo – di danneggiare illecitamente un sistema informatico o telematico o i dati ivi contenuti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento del sistema.

E' un reato comune e quindi può essere commesso da chiunque.

La sanzione prevista è quella pecuniaria fino a trecento quote, oltre all'applicazione delle sanzioni interdittive della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia potrebbe diffondere, all'interno del sistema informatico appartenente all'azienda concorrente, un programma virus

n.	RIFERIMENTO	REATO PRESUPPOSTO
05	Art.24bis D.Lgs. 231/2001	Art. 617-quater c.p. (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)
ANALISI FATTISPECIE	Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. 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. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2. da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3. da chi esercita anche abusivamente la professione di investigatore privato.	

contenuto in un supporto rimovibile (chiave USB, CD, DVD), o tramite posta elettronica, in grado di danneggiare o alterare le funzionalità di detto sistema.

Tale ipotesi di reato si configura nel caso in cui un rappresentante o un Collaboratore della Società intercetti fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa. Il reato si configura altresì qualora si riveli, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle predette comunicazioni.

La norma tutela:

- la libertà di comunicare;

- il diritto alla riservatezza delle comunicazioni.

Qualora l'autore sia un pubblico ufficiale o un incaricato di pubblico servizio con abuso di poteri o con violazione di doveri funzionali ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Le condotte tutelate sono:

- l'intercettazione che riguarda l'attività di captazione del contenuto delle comunicazioni informatiche o telematiche in corso di svolgimento tra operatori abilitati del sistema;

- l'interruzione di un sistema informatico o telematico;

- l'impedimento del regolare funzionamento di un sistema informatico o telematico.

E' un reato comune e quindi può essere commesso da chiunque.

La sanzione prevista è quella pecuniaria da cento a cinquecento quote, oltre all'applicazione delle sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia potrebbe inviare continuamente messaggi di posta elettronica (spam) ad un'azienda concorrente al fine di rallentare o bloccare le loro reti e i loro servizi di posta elettronica.

06	**Art. 24bisD.Lgs. 231/2001**	**Art. 617-quinquies c.p. (Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche)**
ANALISI FATTISPECIE	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, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.	

La norma punisce chiunque installi strumenti idonei ad intercettare, impedire o interrompere le comunicazioni di un sistema informatico o telematico.

Trattasi di reato comune che in quanto tale può essere commesso da chiunque.

E' prevista una sanzione pecuniaria da cento a cinquecento quote, oltre all'applicazione delle sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio un Collaboratore di Valvole Italia potrebbe installare in alcuni terminali aziendali di un competitor un software ("trojan horse" o "spyware"") che contiene una scheda che consente di intercettare informazioni riservate utili per la società.

n.	RIFERIMENTO	REATO PRESUPPOSTO
07	Art.24bis D.Lgs. 231/2001	Art. 635-bis c.p. (Danneggiamento di informazioni, dati e programmi informatici)
ANALISI FATTISPECIE	Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.	

La norma punisce chiunque distrugga, deteriori, cancelli, alteri o renda inservibili, anche parzialmente, informazioni, dati o programmi informatici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.

Soggetti passivi del reato possono essere considerati il concessionario, il legittimo utilizzatore, il concedente, il proprietario, l'operatore del sistema, nonché i partners commerciali o di lavoro di un'impresa o di un professionista, rispetto ad informazioni da essi forniti per determinate finalità operative.

Trattasi di reato comune che, in quanto tale, può essere commesso da chiunque.

La sanzione prevista è quella pecuniaria da cento a cinquecento quote, oltre all'applicazione delle sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un dirigente di Valvole Italia potrebbe assoldare un hacker (o cracker) che modifica il sito web dell'azienda concorrente (cosiddetto "web defacing"), facendo apparire informazioni false o tali da compromettere la reputazione dell'azienda stessa.

08	Art.24bis D.Lgs. 231/2001	Art. 635-ter c.p. (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)
ANALISI FATTISPECIE	Salvo che il fatto costituisca più grave reato, 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, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.	

La norma tutela il danneggiamento di dati di pubblica utilità, cioè sistemi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Il reato de quo è un reato comune e quindi può essere commesso da chiunque.

E' prevista una sanzione pecuniaria da cento a cinquecento quote, oltre all'applicazione delle sanzioni interdittive dell'interdizione dall'esercizio dell'attività della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

n.	RIFERIMENTO	REATO PRESUPPOSTO
09	Art.24bis D.Lgs. 231/2001	Art. 635-quater c.p. (Danneggiamento di sistemi informatici o telematici)

ANALISI FATTISPECIE	Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Tale ipotesi di reato si configura nel caso in cui un rappresentante o un Collaboratore della Società distrugga, danneggi, deteriori, o renda inservibili, anche parzialmente, sistemi informatici o telematici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.

E' un reato comune e pertanto può essere commesso da chiunque.

La sanzione prevista è quella pecuniaria da cento a cinquecento quote, oltre all'applicazione delle sanzioni interdittive dell'interdizione dall'esercizio dell'attività della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia potrebbe trasmettere una e-mail contenente virus ai sistemi informatici appartenenti ad un'azienda concorrente, provocando un malfunzionamento dei sistemi informatici utilizzati dalla stessa azienda, paralizzandone l'attività lavorativa.

n.	RIFERIMENTO	REATO PRESUPPOSTO
10	Art.24bis D.Lgs. 231/2001	Art.635-quinquies c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità)

ANALISI FATTISPECIE	
	Se il fatto di cui all'articolo 635-quater 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, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Il reato punisce chiunque distrugga, danneggi, deteriori, renda inservibili, anche parzialmente, i sistemi informatici o telematici di pubblica utilità, ovvero ne ostacoli il corretto funzionamento. Se il fatto è commesso con abuso della qualità di amministratore del sistema, si configura una circostanza aggravante.

E' prevista una sanzione pecuniaria da cento a cinquecento quote, oltre all'applicazione delle sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia potrebbe inserire dei virus nei sistemi informatici appartenenti alla società fornitrice di energia elettrica, provocando un malfunzionamento del sistema di rendicontazione dei Kw consumati dalla stessa Valvole Italia.

n.	RIFERIMENTO	REATO PRESUPPOSTO
11	Art. 24bis D.Lgs.231/2001	Art. 640 quinquies c.p. (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)

ANALISI FATTISPECIE	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, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00.

Tale ipotesi di reato si configura nel caso in cui il soggetto che presta servizi di certificazione di firma elettronica violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri un danno. Trattandosi di un reato proprio, lo stesso sarà configurabile in relazione a Valvole Italia qualora la condotta venga posta in essere in concorso con il soggetto "che presta servizi di certificazione delle firme elettroniche".

La sanzione prevista è quella pecuniaria sino a quattrocento quote, oltre all'applicazione delle sanzioni interdittive del il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi nonchè del divieto di pubblicizzare beni o servizi.

Ad esempio, un Collaboratore di Valvole Italia potrebbe corrompere un certificatore al fine di ottenere un certificato in realtà appartenente ad una persona fittizia.

n.	RIFERIMENTO	REATO PRESUPPOSTO
12	**Art. 25, D.lgs. 231/2001**	**Art. 171, comma 1, lettera a bis) e terzo comma L.D.A.** **Art. 171 bis L.D.A.** **Art. 171 ter L.D.A.** **Art. 171 septies L.D.A.** **Art. 171 octies L.D.A.**
ANALISI FATTISPECIE	Le varie fattispecie in esame puniscono le condotte di abusivo utilizzo, detenzione, vendita, messa in commercio, introduzione nel territorio dello stato, duplicazione, messa a disposizione di terzi anche via internet di opere dell'ingegno protette dalle disposizioni a tutela del diritto d'autore, di programmi per elaboratore, di banche di dati, di opere musicali o di trasmissioni televisive o servizi criptati e decodificati al fine di trarne profitto.	

Possibili condotte illecite dei reati sopra analizzati

Oltre agli esempi di condotte specifiche sopra riportati, gli illeciti informatici possono generalmente integrarsi a seguito dei seguenti comportamenti:

- accessi abusivi presso altri sistemi informatici, da parte di chi, ad esempio, per abilità informatiche o conoscenze private, riesce a decodificare i codici di accesso;
- diffusione di virus tramite il servizio di web–mail;
- applicazione di software capaci di intercettare i flussi informatici altrui;
- diffusione di codici di acceso a sistemi protetti, abusivamente intercettati;
- "scaricamento" (downloading) o "caricamento" (uploading) di brani musicali/software o altro, protetti dal diritto d'autore;
- scaricamento di documenti pubblici per una successiva attività contraffattiva (ad esempio, un decreto autorizzativo del Comune);
- personale dell'Ente accede non virtualmente (collegandosi via internet dall'hardware dell'Azienda) bensì fisicamente (inserendo, ad esempio, una chiave usb) ad un sistema informatico altrui, captando dati sensibili o comunque riservati.

Analisi della realtà aziendale e indice di rischio

A seguito delle interviste condotte e delle risposte ottenute dai referenti aziendali, ai quali sono state sottoposte check list ricognitive, è emerso che Valvole Italia è dotata di un sistema informatico che, se usato in modo non corretto potrebbe portare alla commissione dei delitti sopra individuati.
Sebbene le postazioni informatiche siano collocate all'interno dei luoghi ove viene esplicata l'attività lavorativa, non è da escludere che per il tramite di quelle postazioni un utente possa accedere alle strutture informatiche altrui, anche utilizzando Internet.
Pertanto, ad esempio, possono essere consumati accessi abusivi presso altri sistemi informatici, da parte di chi, per abilità informatiche o conoscenze private, riesce a decodificare i codici di accesso; possono essere diffusi virus tramite il servizio di web–mail; possono essere applicati software capaci di intercettare i flussi informatici altrui; possono essere diffusi i codici di acceso a sistemi protetti abusivamente intercettati; possono essere "scaricati" (downloading) o "caricati" (up-loading) brani musicali/software o altro, protetti dal diritto d'autore; possono essere scaricati documenti pubblici per una successiva attività contraffattiva.
La principale difesa avverso i rischi di tipo informatico sono – ovviamente – le procedure informatiche, capaci di filtrare, monitorare e/o proibire "all'origine" i flussi informatici indesiderati.
Inoltre, la tendenza alla c.d. "dematerializzazione" dei documenti, sempre più applicata anche dalla pubblica amministrazione, impone alle realtà imprenditoriali - e non solo - di conservare i documenti sensibili o "fidefacenti", cioè conservati a fini di prova (dichiarazione dei redditi, buste paga, scritture contabili, libri matricola), all'interno del sistema informatico.
Se prima quei documenti venivano conservati "analogicamente", ovvero su supporto cartaceo, oggi la politica gestionale è quella di conservare la documentazione su supporto informatico.

Analizzando la realtà aziendale, è emerso che Valvole Italia:

- dispone di una rete informatica con diverse postazioni fisse e mobili;

- ogni utente ha una password ed un codice di accesso alle banche dati aziendali;

- tutti i pc ed i server sono aggiornati automaticamente con le patch di sicurezza rilasciate da Microsoft;

- ogni utente ha software configurabili (per processo clienti), che consentono di svolgere funzioni adatte alla singola specifica applicazione tramite l'impostazione di parametri operativi (es. i software di super visione e/o controllo degli impianti, i software dei sistemi di gestione dei laboratori, i software dei sistemi gestionali;

- ogni utente ha pacchetti software personalizzati (sviluppati appositamente) per soddisfare le esigenze specifiche della Società;

- i dati in rete sono regolati da specifici permessi di accesso;

- solo l'utente "administrator" può accedere a tutte le cartelle;

- tutti i programmi installati sono licenziati;

- c'è un censimento ed inoltre c'è un controllo periodico da parte dei soggetti gestori dei domini;

- è dotata di un sistema firewall;

- sul firewall può accedere per effettuare la manutenzione esclusivamente l'Amministratore di Sistema;

- è attivo un accesso remoto per il collegamento alla reta interna attraverso un applicativo con credenziali riconosciute solo da parte di utenti autorizzati:

    - utenti aziendali con connessione vpn con credenziali;

    - consulenti esterni con accesso via teamviewer che non viene comunque mai lasciato in esecuzione (quindi l'accesso da parte di utenti esterni all'Azienda deve essere prima concordato e poi autorizzato dal reparto IT);

- sono presenti due diversi software antivirus, Avira e Windows Defender per rilevare i programmi malevoli che possono essere scaricati durante la navigazione internet dagli utenti;

- la posta elettronica è stata esternalizzata con Google For Business;

- sui vari Pc sono presenti antivirus differenti;

- vi è un antivirus sul firewall che è Zyxlic – Bun110-1, Bundle Servizi Protezione incluso sul firewall;

- è presente un sistema di backup dei dati, che permette il ripristino da Disaster Recovery tramite software diversi;

- è prevista una procedura di emergenza nel caso in cui il sistema di controllo vada in avaria (Disaster Recovery), non scritta ma che comunque prevede che

"*l'Amministratore di Sistema ha l'incarico del ripristino software, dati o hardware, al di fuori dell'orario lavorativo se il problema non è bloccante per l'Azienda*";

- i server hanno tutti dei sistemi di backup che permettono il ripristino del disaster recovery;

- il ripristino avviene tramite software diversi;

- è presente una sala server autonoma, protetta da una porta chiusa a chiave nell'Ufficio Reparto IT;

- i supporti contenente i backup vengono riposti nell'ufficio reparto IT, protetto da serratura;

- i backup vengono periodicamente portati fuori dalla sede;

- la sala server è condivisa con la sala metrologica e si trova in officina;

- la sala è chiusa a chiave, con armadi rack chiusi a chiave;

- la sala server è climatizzata ed è dotata di un gruppo di continuità;

- l'accesso agli armadi rack è consentito solo al reparto IT;

- ha previsto credenziali per l'utilizzo delle web mail;

- ha previsto credenziali per l'utilizzo delle web mail e ha marcato le mail con il dominio dell'Ente;

- ai dipendenti non è concesso l'utilizzo di domini di posta differenti da quelli dell'Ente;

- ha previsto che solo i dipendenti possono accedere ad internet.

Presidi di tutela

In ragione di quanto previsto dal Modello Organizzativo e dei risultati ottenuti dall'analisi di cui sopra si ritiene che la Società - qualora adotti i presidi di tutela sottoindicati - potrà ridurre il rischio di commissione dei reati ex D.L. 231/01 a quel livello di accettabilità, (il rischio è accettabile se l'evento si verifica solo in caso di elusione fraudolenta del modello), tale da escludere la responsabilità della Società stessa.

I presidi di tutela sono:

- regole di condotta;
- protocolli;
- controlli da parte dell'Organismo di Vigilanza.

Regole di condotta

Sotto il profilo dei collaboratori della Società ognuno deve:

- rispettare scrupolosamente quanto previsto dalle policy di sicurezza aziendali, anche al fine di non compromettere la funzionalità e la protezione dei sistemi informatici;

- non inviare messaggi di posta elettronica minatori ed ingiuriosi, comunque non attinenti alla propria attività lavorativa o dannosi per l'immagine dell'Azienda;

- custodire e non rivelare a terzi non autorizzati la propria password personale ed il proprio codice di accesso alle banche dati aziendali;

- non riprodurre per uso personale i software aziendali né utilizzare per fini privati gli strumenti in dotazione;

- non registrare sugli elaboratori aziendali software non autorizzati e "file" informatici dal contenuto non strettamente connesso all'attività lavorativa o illegali;

- non navigare su siti web dal contenuto non strettamente connesso all'attività lavorativa;

- non utilizzare i sistemi di comunicazione aziendali (e-mail, intranet, ecc.) per negoziare l'acquisto la vendita di beni e servizi estranei all'esercizio dell'attività lavorativa né per consultare o diffondere materiale indecoroso, offensivo o dannoso per l'azienda o per i terzi;

- non utilizzare domini di posta elettronica personale;

- non utilizzare le chiavi crittografiche destinate ad altre persone nonché le credenziali di accesso al sistema destinate ad altre persone;

- non installare programmi provenienti dall'esterno delle rete aziendale senza l'autorizzazione della direzione;

- non utilizzare le unità di rete aziendali nonché tutti i sistemi informatici aziendali (ivi compresi porte usb o notebook o altri PC portatili aziendali) per scopi diversi dall' attività lavorativa;

- non utilizzare i supporti magnetici (cd, floppy-disk, cassette, cartucce) per finalità differenti rispetto a quelle aziendali;

- non caricare e scaricare (upload e/o download) files e/o programmi software, anche gratuiti, se non per esigenze strettamente aziendali e fatti salvi comunque i casi di esplicita autorizzazione aziendale;

- non effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla direzione e con il rispetto delle normali procedute per gli acquisti;

- non partecipare a Forum non aziendali, utilizzare chat (esclusi gli strumenti autorizzati dalla direzione), utilizzare bacheche elettroniche o effettuare la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, utilizzare qualunque utilizzo di servizi internet, attuali o futuri, non strettamente inerenti l'attività dell'ente;

- non lasciare i pc ed altri dispositivi elettronici incustoditi;

- non accedere a sistemi informatici altrui abusivamente, ovvero senza autorizzazione o oltre il termine per cui si è stati autorizzati;

- non accedere alla sala server od ai supporti di backup se non espressamente autorizzati.

Protocolli preventivi

La Società ha adottato le seguenti procedure aziendali:

a) **sotto il profilo tecnico:**

Protezione dall'esterno (Firewall):

1. è presente un sistema firewall;
2. sul firewall può accedere per effettuare la manutenzione esclusivamente l'Amministratore di Sistema;
3. è attivo un accesso remoto per il collegamento alla reta interna attraverso un applicativo con credenziali riconosciute solo da parte di utenti autorizzati:

- utenti aziendali con connessione vpn con credenziali;

- consulenti esterni con accesso via teamviewer che non viene comunque mai lasciato in esecuzione (quindi l'accesso da parte di utenti esterni all'Azienda deve essere prima concordato e poi autorizzato dal reparto IT);

Protezione della perdita dei dati (antivirus):

1. sono presenti due diversi software antivirus, Avira e Windows Defender per rilevare i programmi malevoli che possono essere scaricati durante la navigazione internet dagli utenti;
2. la posta elettronica è stata esternalizzata con Google For Business;
3. sui vari Pc sono presenti antivirus differenti;
4. vi è un antivirus sul firewall che è Zyxlic – Bun110-1, Bundle Servizi Protezione incluso sul firewall;

Salvataggio dei dati (Backup):

1. è presente un sistema di backup dei dati, che permette il ripristino da Disaster Recovery tramite software diversi;
2. è prevista una procedura di emergenza nel caso in cui il sistema di controllo vada in avaria (Disaster Recovery), non scritta ma che comunque prevede che "*l'Amministratore di Sistema ha l'incarico del ripristino software, dati o hardware, al di fuori dell'orario lavorativo se il problema non è bloccante per l'Azienda*";

3. presente una sala server autonoma, protetta da una porta chiusa a chiave nell'Ufficio Reparto IT;

4. i backup vengono periodicamente portati furi dalla sede.

Gestione dei dati e dei dispositivi (Server/Pc/Rete):

1. la Società dispone di una rete informatica con diverse postazioni fisse e mobili;
2. ogni utente ha una password ed un codice di accesso alle banche dati aziendali;
3. ogni utente ha software configurabili (per processo clienti),che consentono di svolgere funzioni adatte alla singola specifica applicazione tramite l'impostazione di parametri operativi (es. i software di super visione e/o controllo degli impianti, i software dei sistemi di gestione dei laboratori, i software dei sistemi gestionali;
4. ogni utente ha pacchetti software personalizzati (sviluppati appositamente) per soddisfare le esigenze specifiche della Società.

Protezione fisica dei dati (Server):

1. la sala server è condivisa con la sala metrologica e si trova in officina;
2. la sala è chiusa a chiave, con armadi rack chiusi a chiave;

3. la sala server è climatizzata ed è dotata di un gruppo di continuità;
4. l'accesso agli armadi rack è consentito solo al reparto IT;

b) <u>sotto il profilo dei collaboratori, ognuno di loro deve:</u>

1. rispettare scrupolosamente quanto previsto dalle policy di sicurezza aziendali, anche al fine di non compromettere la funzionalità e la protezione dei sistemi informatici;
2. non inviare messaggi di posta elettronica minatori ed ingiuriosi, comunque non attinenti alla propria attività lavorativa o dannosi per l'immagine dell'Azienda;
3. custodire e non rivelare a terzi non autorizzati la propria password personale ed il proprio codice di accesso alle banche dati aziendali;
4. non riprodurre per uso personale i software aziendali né utilizzare per fini privati gli strumenti in dotazione;
5. non registrare sugli elaboratori aziendali software non autorizzati e "file" informatici dal contenuto non strettamente connesso all'attività lavorativa o illegali;
6. non navigare su siti web dal contenuto non strettamente connesso all'attività lavorativa;
7. non utilizzare i sistemi di comunicazione aziendali (e-mail, intranet, ecc.) per negoziare l'acquisto la vendita di beni e servizi estranei all'esercizio dell'attività lavorativa né per consultare o diffondere materiale indecoroso, offensivo o dannoso per l'azienda o per i terzi;
8. non utilizzare domini di posta elettronica personale.

Per gestire con maggiore efficienza ed ottenere un effettivo controllo sulle suesposte procedure Valvole Italia ha istituito all'interno del proprio organico la figura dell'Amministratore di Sistema con il compito di supervisionare tutte le procedure e operazioni inerenti al sistema informatico della Società, avendo accesso esclusivo al sistema firewall, al cloud contenente i report inviati dai software antivirus, a tutti i dati in rete ed alle password di tutte le caselle mail, oltre ad essere l'unico soggetto abilitato ad accedere alla sala server, di cui possiede le chiavi. Tale figura può pertanto riscontrare e segnalare – al fine di porvi rimedio – eventuali violazioni alle regole di condotta o alle procedure adottate dalla Società.

Altri protocolli preventivi

- Informazione e formazione specifica del personale
- Sistema disciplinare
- Gestione delle risorse umane
- Previsione di divieti nel Codice Etico

Controlli da parte dell'organismo di vigilanza

All'Organismo di Vigilanza è fatto obbligo di svolgere controlli con le modalità indicate nella procedura controlli ODV, a cui si rimanda.