ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

Responsabilità degli enti e reati informatici

David D'Agostini, Antonio Piva

1. Introduzione

L'articolo 27 della Costituzione sancisce il principio secondo il quale la responsabilità penale è personale. La conseguenza è che, mentre il danno provocato da un reato potrà essere risarcito anche da un altro soggetto (si pensi ai genitori per i fatti commessi dai figli), la sanzione penale potrà (e dovrà) essere inflitta solamente al colpevole, dopo una sentenza definitiva.
Collegare la responsabilità per un reato in maniera univoca a una persona fisica comporta ulteriori effetti, uno dei quali è l'impossibilità di procedere penalmente nei confronti di società, associazioni, enti e persone giuridiche in generale. Non a caso la scienza penalistica italiana aveva coniato il celebre detto "*societas delinquere non potest*", ossia una società non può commettere delitti (che eventualmente saranno commessi dai dipendenti, dai dirigenti o dagli amministratori, ma non dall'ente astratto).
Questo principio è stato in parte superato dal decreto legislativo 231/2001 che, dando esecuzione a una serie di convenzioni e accordi internazionali, ha introdotto nel nostro ordinamento la possibilità di irrogare sanzioni per una responsabilità diretta (chiamata "amministrativa") dell'ente.
Questa nuova concezione sta cambiando radicalmente l'approccio delle società a determinate problematiche, con importanti ricadute anche in riferimento alle nuove tecnologie, all'uso dei computer in azienda, alla commissione di reati informatici sul luogo di lavoro.

2. Il decreto legislativo 231/01

Il decreto legislativo 8 giugno 2001 n.231 disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni (d'innanzi denominati semplicemente "enti" per brevità); pur senza approfondire gli aspetti giuridici di tale complessa normativa, al fine di apprezzarne la forza innovativa è opportuno chiarire per sommi capi le principali disposizioni.
In primo luogo si precisa che l'ente è punibile solamente per i reati commessi alternativamente dai seguenti **soggetti**:
1. persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (cosiddetti **soggetti in posizione apicale**);
2. persone sottoposte alla direzione e alla vigilanza di tali soggetti (cosiddetti **soggetti sottoposti**).
Inoltre l'illecito deve essere commesso nell'**interesse** o nel **vantaggio** dell'ente, che quindi non risponde se il colpevole ha agito nell'interesse esclusivo proprio o di terzi.
Il concetto di interesse va interpretato nel senso di politica d'impresa, pertanto, il fatto compiuto da una persona deve essere ricondotto anche

all'ente, qualora questo abbia indirizzato, con una politica di impresa più o meno esplicita, l'autore dell'illecito a commettere il reato[1].
Nel caso di commissione di reato, il d.lgs. 231/01 prevede la possibilità che l'ente venga esonerato da responsabilità, se dimostra che:
a. l'organo dirigente ha adottato ed efficacemente attuato **modelli di organizzazione e di gestione** idonei a prevenire reati come quello verificatosi;
b. il compito di verificare il funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un **organismo di vigilanza** dotato di autonomi poteri di iniziativa e di controllo;
c. le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
d. non vi è stata omessa o insufficiente controllo da parte dell'organismo di vigilanza.
Al contrario, se l'ente viene ritenuto responsabile di un illecito amministrativo dipendente da reato, le sanzioni che potranno essere irrogate sono di quattro tipi:
1. sanzioni pecuniarie;
2. confisca;
3. sanzioni interdittive;
4. pubblicazione della sentenza.

La **sanzione pecuniaria** si applica sempre e viene misurata in "quote" (da cento a mille per ciascun reato); il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente, nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.
L'importo di una quota va da un minimo di 260 a un massimo di 1.550 € e viene stabilito dal giudice sulla base delle condizioni economiche e patrimoniali dell'ente, allo scopo di assicurare l'efficacia della sanzione.
Sono, inoltre, previsti casi di riduzione della sanzione pecuniaria (per esempio, se l'ente non ha ricavato vantaggio dal reato o se il danno è di particolare tenuità); in ogni caso, la sanzione pecuniaria non può essere inferiore a 10.330 €.
Con la sentenza di condanna viene automaticamente disposta la **confisca** del profitto del reato ovvero di somme di denaro, beni o altre utilità di valore equivalente.
Le **sanzioni interdittive**, che per il loro contenuto possono essere ben più afflittive della pena pecuniaria, sono:
a. l'interdizione dall'esercizio dell'attività;
b. la sospensione o la revoca delle autorizzazioni, licenze o concessioni;
c. il divieto di contrattare con la pubblica amministrazione;
d. l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e. il divieto di pubblicizzare beni o servizi.
Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni e si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni:
a. l'ente ha tratto dal reato un profitto di rilevante entità;
b. in caso di reiterazione degli illeciti.
Anche in questo caso il giudice determina tipo e durata della sanzione sulla base dei criteri sopra indicati (gravità del fatto, grado di responsabilità ecc.), tenendo conto dell'idoneità delle singole sanzioni a prevenire altri illeciti.
Quando nei confronti dell'ente viene applicata una sanzione interdittiva può anche essere disposta la **pubblicazione** della sentenza di condanna, per estratto o per intero, in uno o più giornali indicati dal giudice, nonché mediante affissione nel comune ove l'ente ha la sede principale.
Chiariti i presupposti per la punibilità degli enti e le relative sanzioni, è necessario precisare che la responsabilità amministrativa disciplinata dal d.lgs. 231/01 non si estende genericamente a tutti i reati previsti nel nostro ordinamento, bensì solo a quelli espressamente elencati nel decreto stesso (i cosiddetti "*reati presupposto*"); si tratta di circa un centinaio di delitti, tra i quali alcuni di indubbio interesse per chi si occupa di ICT.

3. Reati presupposto: computer crimes

La legge 18 marzo 2008 n.48, con la quale è stata ratificata la Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, ha introdotto nel d.lgs. 231/01 l'art. 24bis "*delitti informatici e trattamento illecito di dati*".

[1] A tal fine, il vantaggio si rileva come profitto, arricchimento economico o beneficio patrimoniale che l'ente ha ottenuto direttamente dal reato.

Tale norma prevede l'applicazione a carico dell'ente della sanzione pecuniaria **da cento a cinquecento quote** (ciascuna, si ricorda, di importo compreso tra 260 e 1.550 €) in relazione alla commissione dei seguenti delitti:

- accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);
- installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 q*uinquies* c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);
- 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.);
- danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.).

Vengono, invece, punite con la sanzione pecuniaria **fino a quattrocento quote** le seguenti ipotesi:

- falsificazione di documenti informatici (art. 491 *bis* c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica art. 640 *quinquies* c.p.).

Infine, la sanzione pecuniaria giunge **fino a trecento quote** per i reati:

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.).

A seconda del tipo di reato informatico commesso, sarà inoltre possibile l'irrogazione di sanzioni interdittive (e, di conseguenza, anche la pubblicazione della sentenza di condanna).
Non è possibile in questa sede procedere all'esame analitico dei menzionati delitti, ma una lettura sommaria è sufficiente per far comprendere che il legislatore (in conformità con la Decisione quadro dell'Unione Europea 2005/222/GAI contro gli attacchi informatici) ha dato completa attuazione alle previsioni della Convenzione di Budapest, prevedendo la responsabilità delle persone giuridiche in dipendenza della commissione di numerosi reati informatici (sia introdotti dalla vecchia legge 547/1993 che dalla più recente legge 48/2008)[2].
Naturalmente, posto che (secondo i meccanismi sopra illustrati) la responsabilità amministrativa dell'ente sussiste solo se il reato è stato commesso nel suo interesse o a suo vantaggio, il caso dell'accesso abusivo o del danneggiamento informatico commesso da un dipendente per proprio conto utilizzando il PC sul luogo di lavoro non comporta sanzioni a carico dell'ente. Rimane, tuttavia, aperta la possibilità di agire nei confronti del datore di lavoro ai soli fini civili, ossia **per il risarcimento del danno**.

4. Reati presupposto: diritto d'autore

Se l'inserimento nel d.lgs. 231/01 dei reati informatici sopra elencati era atteso da anni, maggiore sorpresa ha invece destato l'introduzione dei delitti in materia di violazione del diritto d'autore, avvenuto ad opera della legge 23 luglio 2009 n.99.
In virtù dell'art. 25 *novies*, viene punita con la sanzione pecuniaria **fino a cinquecento quote** (nonché con le sanzioni interdittive per una durata non superiore a un anno) la commissione di alcuni delitti previsti dalla legge 22 aprile 1941 n. 633 (vale a dire la Legge sul diritto d'autore) tra cui i casi che si elencano:

a. immissione in un sistema di reti telematiche mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o parte di essa, senza averne diritto, a qualsiasi scopo e in qualsiasi forma (si pensi al *filesharing* mediante *peer to peer*);

b. abusiva duplicazione al fine di profitto, detenzione a scopo commerciale o imprenditoriale, concessione in locazione, importazione, distribuzione, vendita di programmi per elaboratore (*software*) contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);

c. abusiva duplicazione, riproduzione, trasmissione o diffusione con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico,

[2] Si veda l'articolo "L'accesso abusivo ai sistemi informatici e telematici: Aspetti giuridici e informatici di un attacco hacker" sul numero 10 di giugno 2004, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

della vendita o del noleggio, dischi, nastri o supporti analoghi;
d. introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, commercio, concessione in noleggio o cessione a qualsiasi titolo delle duplicazioni o riproduzioni abusive di cui sopra;
e. fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicità per la vendita o il noleggio, o detenzione per scopi commerciali di attrezzature, prodotti o componenti ovvero prestazioni di servizi che abbiano la prevalente finalità o l'uso commerciale di eludere le misure tecnologiche di protezione[3] ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione delle predette misure;
f. abusiva rimozione o alterazione di informazioni elettroniche di protezione, ovvero distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, azioni volte a comunicare o mettere a disposizione dal pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse;
g. fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.
Anche in questi casi vale la pena ribadire che non vi è una responsabilità ai sensi del d.lgs. 231/01 in capo alla società datrice di lavoro per eventuali violazioni al diritto d'autore poste in essere dal dipendente nel proprio personale interesse (si pensi al caso di *upload* o di *filesharing* di opere protette utilizzando le risorse informatiche e telematiche aziendali).
Può, al contrario, sussistere una piena responsabilità amministrativa dell'ente qualora sui personal computer in uso ai dipendenti venisse installato software abusivo, oppure nel caso molto diffuso di *underlicensing*, consistente nell'installazione di un numero di copie del programma superiore a quello previsto dalla licenza d'uso.
Si tratta di fenomeni già pesantemente perseguiti sul piano penale (la cosiddetta "pirateria" del software è punita con la reclusione da sei mesi a tre anni e con la multa da 2.600 a 15.500 €), ma come ricordato la responsabilità penale è personale.
L'assoluta novità è, invece, la possibilità di applicare - in aggiunta a quanto sopra - anche le suddette sanzioni amministrative (sia pecuniarie secondo il sistema delle quote, sia interdittive con le intuibili conseguenze negative) direttamente all'ente nel cui interesse sia stato commesso il fatto illecito.

5. La prevenzione

Considerate tali responsabilità, in quale maniera un ente può porsi al riparo da eventuali sanzioni?
Come anticipato, nel caso di commissione di uno dei cosiddetti "reati presupposto" (come i *computer crimes* ovvero le menzionate violazioni al diritto d'autore), l'ente può essere esonerato dalla responsabilità prevista dal d.lgs. 231/01.
A tale fine deve, in primo luogo, aver adottato e attuato un **modello di organizzazione e gestione** e, possibilmente, un **codice etico**.
Questi documenti, ai fini della loro efficacia preventiva in azienda e della successiva valutazione da parte del giudice, devono essere il frutto di un iter procedimentale articolato in due fasi distinte:
a. l'analisi dei rischi-reato (*risk assessment*);
b. la gestione dei rischi-reato (*risk management*).
Durante questi processi di **valutazione** e **gestione**, i rischi vengono identificati prevedendo la possibilità che questi eventi accadano e soppesando il valore di ogni diverso modo di agire. Queste strategie hanno differenti effetti sui rischi, inclusi la riduzione, la rimozione e la ridefinizione degli stessi.
Si tenga conto che prevenire un reato informatico è un'attività di estrema difficoltà in quanto gli stessi strumenti impiegati per un normale uso lavorativo possono essere utilizzati per commettere reati.
Alla fine nel modello dovrebbero essere contenute chiare direttive indirizzate a:
1. definire e regolamentare l'affidamento e la custodia degli strumenti informatici;
2. definire e regolamentare i limiti di utilizzo degli strumenti informatici, contemplando di norma la

[3] Si veda l'articolo "*Diritto d'autore tra Digital Right Management* e *Creative Commons*" sul numero 21 di marzo 2007, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

sola possibilità di utilizzo per lo svolgimento delle attività lavorative e non per usi personali;
3. disporre regole sull'utilizzo di dispositivi e di credenziali di accesso e sulla loro utilizzazione, compreso l'uso delle aree dei *server* aziendali;
4. definire e regolamentare le modalità di produzione della documentazione, anche in forma cartacea, e della loro custodia;
5. definire e regolamentare l'impiego della rete *internet* e della posta elettronica.

In secondo luogo, ai fini dell'esenzione da responsabilità, l'ente deve aver affidato a un **organismo di vigilanza** il compito di verificare il funzionamento e l'osservanza del suddetto modello e di curarne l'aggiornamento.

Con riferimento alle imprese e ad Enti di piccole dimensioni è consentito che i compiti di vigilanza siano assolti dall'organo dirigente. Diversamente la scelta deve tenere conto delle finalità perseguite dalla legge e, quindi, deve assicurare il profilo di effettività dei controlli in relazione alla dimensione e alla complessità organizzativa dell'ente.

I principali requisiti dell'organismo di vigilanza sono l'autonomia e l'indipendenza, la professionalità e la continuità di azione.

A tal proposito la pianificazione e l'attuazione di verifiche ispettive o audit[4], come peraltro indicato dalle norme ISO9001[5], la documentazione delle stesse e l'attuazione del ciclo di Deming (*Plan-Do-Check-Act*) sono strumenti utili, ed in alcuni casi indispensabili, per la gestione dei processi riguardanti la sicurezza informatica.

Nel dettaglio, le attività che l'Organismo è chiamato ad assolvere, anche sulla base delle indicazioni contenute nel d. lgs. n.231/200, possono così schematizzarsi:

- vigilanza sull'**effettività** del modello, che si sostanzia nella verifica della coerenza tra i comportamenti concreti ed il modello istituito;
- disamina in merito all'**adeguatezza** del modello, ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;
- analisi circa il **mantenimento** nel tempo dei requisiti di solidità e funzionalità del modello;
- cura del necessario **aggiornamento** in senso dinamico del modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti.

L'organismo di vigilanza, per poter garantire l'effettività e la congruità dei controlli in ambito informatico, dovrà necessariamente far riferimento a tali competenze specifiche e, se del caso, avvalersi di consulenze eseguite da esperti del settore, in grado di giudicare la rispondenza dei controlli alle finalità per le quali sono eseguiti. Il ricorso a consulenti esterni potrà essere necessario, in quanto non potrà essere utilizzato a tale scopo l'amministratore di sistema la cui attività è per antonomasia da assoggettarsi a controllo.

6. Conclusioni

Il d.lgs. 231/01, in virtù delle novità introdotte prima dalla legge 48/08 e poi dalla legge 99/09, obbliga società, associazioni e persone giuridiche a una seria riflessione sull'utilizzo delle nuove tecnologie in ambito aziendale.

Sarà importante procedere, se non lo si fosse già fatto, alla piena attuazione di quanto dispone il d.lgs. 196/2003 in materia di trattamento dei dati personali e sicurezza informatica e, al tempo stesso, rivedere e implementare i modelli di organizzazione e gestione, nonché le modalità di funzionamento dell'organismo di vigilanza, con particolare riferimento alle consulenze esterne da parte di esperti informatici.

Ciò non per mero formalismo, peraltro inutile dinanzi al vaglio del giudice nel caso di commissione del reato, bensì nello spirito di efficacia protettiva tipico del suddetto decreto; solo con tale ottica l'ente potrà non solo evitare la responsabilità, ma soprattutto prevenire l'illecito.

David D'Agostini, avvocato, master in informatica giuridica e diritto delle nuove tecnologie, docente all'Università degli studi di Udine. Presiede la Commissione informatica dell'Ordine degli avvocati di Udine, è responsabile dell'area "/Diritto& informatica/" della rivista "/Il foro friulano/". Presiede l'Organismo di vigilanza di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

[4] Interni o esterni.

[5] Si vedano gli articoli "LA SICUREZZA DELLE INFORMAZIONI E LE NORME ISO 27000" sul numero 27 di settembre 2008, "ISO/IEC 20000: LA NORMA PER LA QUALITÀ DELL'EROGAZIONE DEI SERVIZI IT" sul numero 29 di marzo 2009, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.