La sicurezza dei dati e delle informazioni: diritti, doveri e responsabilità

ORDINE DEGLI INGEGNERI DI MILANO – 19 MARZO 2007

Sicurezza e protezione dei dati

- ISO 27001: sicurezza = disponibilità, integrità, confidenzialità delle informazioni
- Protezione delle infrastrutture critiche = protezione dei dati e delle informazioni
- Problematiche di carattere giuridico connesse alla creazione, alla conservazione e alla circolazione di dati e informazioni in reti aperte o aziendali:
  - il DIRITTO alla protezione dei dati
  - il DOVERE di riservatezza
  - le RESPONSABILITA' per l'impresa e i suoi collaboratori in relazione a comportamenti non conformi.
  - Gli STRUMENTI ritenuti idonei dalla normativa a tutelare il patrimonio informativo aziendale

NUOVE TECNOLOGIE

NUOVE RESPONSABILITA'

RISK ANALISYS LEGALE PREVENTIVA

INFORMAZIONI

Tesoro aziendale

- Piani strategici
- Documentazione riservata
- Know-how

Bene da proteggere

- Dati personali
- Dati sensibili e giudiziari

INFORMAZIONI

Tesoro aziendale

- Piani strategici
- Documentazione riservata
- Know-how

La tutela del patrimonio informativo

- La nostra normativa prevede ipotesi di responsabilità disciplinare, civile e penale, contenute sia nei nostri codici fondamentali, sia in normative speciali in materia di segreto industriale e concorrenza sleale, che tutelano il titolare dei diritti dall'ipotesi di fuoriuscita di informazioni riservate.

- Spesso non ci si rende conto che le misure di sicurezza a protezione della rete informatica sono fondamentali per proteggersi contro la diffusione del proprio know-how, ma sono altresì necessarie attente policies che impongono comportamenti corretti da parte dei dipendenti, dei collaboratori, dei consulenti.

Le responsabilità

- RESPONSABILITA' DISCIPLINARE

  → Sanzioni disciplinari!

- RESPONSABILITA' CIVILE

  → Risarcimento del danno!

- RESPONSABILITA' PENALE

  → Sanzioni penali!

Le basi civilistiche del dovere di riservatezza: diligenza e fedeltà

Art. 2104 c.c. - Diligenza del prestatore di lavoro

- Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.

Art. 2105 c.c. - Obbligo di fedeltà

- Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.

Art. 2106 c.c. - Sanzioni disciplinari

- L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

Le basi civilistiche del dovere di riservatezza: la concorrenza sleale

- L' **2598 n. 3 c.c.**, in combinato disposto con l'**art. 2600**, prevede che è obbligato al risarcimento del danno chiunque con dolo o colpa si avvalga direttamente o indirettamente di mezzi (al di là dell'uso sleale di marchi altrui) non conformi ai principi della correttezza professionale e idonei a danneggiare l'altrui azienda.
- La giurisprudenza ha ritenuto che, ad esempio, lo storno di dipendenti ai fini dell'acquisizione del know-how di un concorrente rientri in questa ipotesi di concorrenza sleale.
- Ai sensi dell'**art. 2125 c.c**. può essere sottoscritto un patto di non concorrenza tra datore e prestatore di lavoro per il tempo successivo alla cessazione del rapporto con:
  - Atto scritto
  - Corrispettivo
  - Limiti di oggetto, tempo e luogo.
  - Durata massima: 5 anni per i dirigenti, 3 anni per gli altri.

La responsabilità civile (artt. 2043 e ss. c.c.)

- La responsabilità civile, che porta al risarcimento del danno, è sicuramente propria di colui che, per dolo o colpa, cagiona ad altrui un "danno ingiusto" (art. 2043 c.c.)
- In un contesto aziendale, è propria del legale rappresentante dell'azienda il cui dipendente ha commesso il fatto, in quanto vige la responsabilità dell'imprenditore per il fatto commesso dai dipendenti nell'espletamento delle loro mansioni (art. 2049 c.c.)
- Nel caso in cui l'azienda si avvalga dell'opera di collaboratori e consulenti è bene che l'azienda si tuteli tramite specifiche clausole contrattuali di riservatezza in modo da potersi rivalere sul collaboratore/consulente nel momento in cui notizie destinate a rimanere segrete sfuggano al controllo dell'imprenditore.

La riservatezza e i comportamenti umani

- I comportamenti umani sono quelli più difficili da regolare per contratto, in quanto l'azione preventiva delle clausole contrattuali può funzionare solo se:
  - l'informazione è comunicata a tutti coloro che devono mantenere la riservatezza (il fornitore in primo luogo, ma altresì i dipendenti/collaboratori/consulenti esterni del fornitore, eventuali subfornitori, eventuali terzi che per qualsiasi motivo dovessero intervenire operativamente);
  - esistono delle precise responsabilità per coloro che non dovessero rispettare gli accordi di riservatezza previsti;
  - esistono delle sanzioni (civili oppure disciplinari) previste per l'inottemperanza degli obblighi ed esiste la percezione che le sanzioni saranno applicate.

La clausola sulla riservatezza

- La clausola di riservatezza disciplina in dettaglio tutti gli aspetti, molto delicati, relativi a:
  - quali informazioni siano da considerare riservate
  - quali limitazioni alla riservatezza esistono e i casi in cui le limitazioni alla riservatezza possono essere considerate non applicabili
  - periodo durante il quale tali informazioni devono mantenersi riservate
  - eventuale penale prevista in caso di mancato rispetto dell'obbligo di riservatezza.

I risvolti penalistici del dovere di riservatezza: la tutela del segreto

- **Art. 621 c.p.** : prevede che venga punito chiunque, essendo venuto a conoscenza abusivamente di documenti destinati a rimanere segreti, ne riveli il contenuto.
- **Art. 622 c.p.** : viene punito chiunque, venuto a conoscenza per ragione del suo stato o del suo ufficio, arte o professione, di notizie destinate a rimanere segrete le riveli o le impieghi a proprio od altrui profitto. La pena è aggravata se il fatto è commesso da amministratori, direttori generali, sindaci, liquidatori, revisori.
- **Art. 623 c.p.** : punisce chiunque, venuto a conoscenza per ragione del suo stato o del suo ufficio, arte o professione, di notizie destinate a rimanere segrete riguardanti scoperte, invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto.

Il codice della proprietà industriale: le informazioni segrete

- **Art. 98 comma 1**: costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni siano segrete, nel senso che
  - non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;
  - abbiano valore economico in quanto segrete;
  - siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.
- E' vietato rivelare a terzi oppure acquisire od utilizzare le informazioni e le esperienze aziendali di cui a questo articolo.

INFORMAZIONI

Bene da proteggere

- Dati personali
- Dati sensibili e giudiziari

Privacy = diritto

- Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
- Convenzione di Strasburgo n. 108/1981 del Consiglio d'Europa
- Carta dei diritti fondamentali dell'Unione Europea
- Direttiva 1995/46/CE; Direttiva 2002/58/CE
- D. Lgs. 196/2003

- … il **diritto di "essere lasciati soli"**
- … il **diritto di controllare le informazioni che ci riguardano** (Fidelity cards, TV digitale, sms,…)

- TRE DIRITTI FONDAMENTALI DELLA PERSONA:
  - **diritto alla privacy**
  - **libera trasmissione e circolazione delle informazioni**
  - **bisogno di sicurezza**

Il D. Lgs. 196/2003: I soggetti …

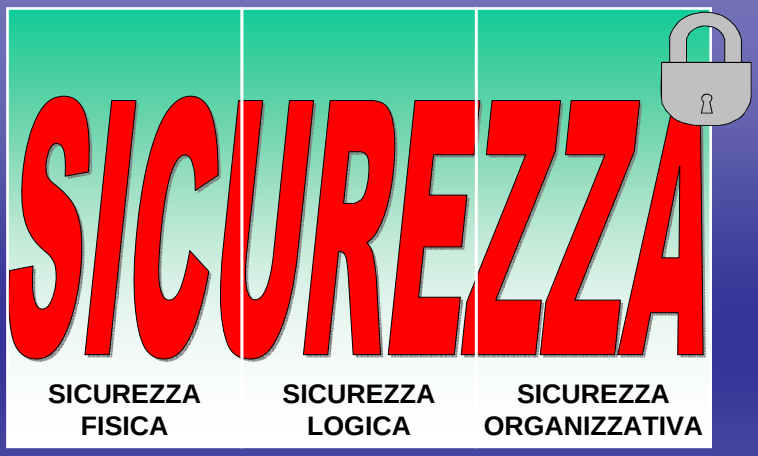
- INTERESSATO: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (clienti, fornitori, dipendenti!);
- TITOLARE: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- RESPONSABILE: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- INCARICATO: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

… e le responsabilità

TITOLARE
- RESPONSABILITA' CIVILE
- RESPONSABILITA' PENALE

RESPONSABILE
- RESPONSABILITA' DISCIPLINARE
- RESPONSABILITA' PENALE

INCARICATO
- RESPONSABILITA' DISCIPLINARE
- RESPONSABILITA' PENALE



SICUREZZA FISICA	SICUREZZA LOGICA	SICUREZZA ORGANIZZATIVA
PROTEZIONE DELLE AREE E DEI LOCALI	PROTEZIONE DELLA RETE	ISTRUZIONI
PROTEZIONE DELLA RETE		PROCEDURE

La sicurezza dei dati e dei sistemi (artt. 31-36 del D. Lgs. 196/2003)

- MISURE IDONEE …
  - I dati personali devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di **idonee e preventive misure di sicurezza**, i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- … E MISURE MINIME DI SICUREZZA:
  - **Il livello minimo di sicurezza è garantito mediante l'applicazione delle misure minime** elencate negli artt. 34 e 35 ed esplicitate nel disciplinare tecnico del Codice (Allegato B).

Le misure idonee (art. 31)

- Non esistono parametri minimi di valutazione dell'idoneità, se non il "progresso tecnico" e *l'importanza* dei dati trattati;
- Chiunque cagiona ad altri danno per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c. (esercizio di attività pericolose), "se non prova di aver adottate tutte le misure idonee ad evitare il danno" (art. 15).

INVERSIONE DELL'ONERE DELLA PROVA

Le misure minime (artt. 33-35)

ART. 34: mezzi elettronici

- procedure di autenticazione;
- sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati
- protezione degli strumenti elettronici e dei dati
- procedure di backup
- Documento Programmatico sulla Sicurezza
- tecniche di cifratura o codici identificativi per trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

ART. 35: senza mezzi elettronici

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
- procedure per idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il dettaglio per i trattamenti con strumenti elettronici (Allegato B)

- Sistema di autenticazione informatica
  - **Credenziali di autenticazione + procedura di autenticazione**
  - **Caratteristiche della parola chiave e del codice di identificazione**
  - **Obblighi per l'incaricato**
  - **Istruzioni scritte**
- Sistema di autorizzazione
  - **Profili di autorizzazione**
  - **Verifica periodica della sussistenza delle condizioni**
- Altre misure di sicurezza
  - **Antivirus**
  - **Aggiornamento dei programmi di protezione**
  - **Backup dei dati**
- Documento Programmatico sulla Sicurezza
- Ulteriori misure per dati sensibili o giudiziari
  - **Protezione contro accessi abusivi**
  - **Custodia, uso e protezione dei supporti rimovibili**
  - **Ripristino dell'accesso ai dati**
- Misure di tutela e garanzia
  - **Attenzione agli interventi esterni di installazione delle misure minime**
  - **Descrizione dello stato del DPS nella relazione accompagnatoria al bilancio d'esercizio**

Le sanzioni (artt.161-172)

Violazioni amministrative

Violazione	Riferimenti	Sanzione
Omessa o inidonea informativa all'interessato (art. 161)	Artt. 13, 17, 26, 27	Da 3.000 a 18.000 Euro se dati personali. Da 5.000 a 30.000 Euro se dati sensibili. Aumento fino al triplo se inefficacia in ragione delle condizioni economiche dell'interessato. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Cessione di dati (art. 162 comma 1)	Art. 16	Da 5.000 a 30.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Comunicazione dei dati all'interessato da parte di altri rispetto al medico designato dal titolare o dall'interessato (art. 162 comma 2)	Art. 84	Da 500 a 3000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Omessa o incompleta notificazione (art. 163)	Artt. 37, 38	Da 10.000 a 60.000 Euro e pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Omessa informazione o esibizione al Garante (art. 164)	Artt. 150, 157	Da 4.000 a 24.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.

Le sanzioni (artt. 161-172)

Violazioni penali

Violazione	Riferimenti	Sanzione
Trattamento illecito di dati (art. 167 comma 1) (tra gli altri, trattamento senza il consenso dell'interessato)	Artt. 18, 19, 23, 123, 126, 129, 130	Reclusione da 6 a 18 mesi. Se si tratta di comunicazione o diffusione di dati, da 6 a 24 mesi. Pubblicazione della sentenza.
Trattamento illecito di dati (art. 167 comma 2) (tra gli altri, violazione delle norme sui dati sensibili)	Artt. 17, 20, 21, 22, 25, 26, 27, 45	Reclusione da 1 a 3 anni. Pubblicazione della sentenza.
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)	Art. 37	Reclusione da 6 mesi a 3 anni. Pubblicazione della sentenza.
Misure minime di sicurezza (art. 169)	Art. 33	Arresto fino a 2 anni o ammenda da 10.000 a 50.000 Euro. Prescrizione da parte del Garante che fissa un termine per la regolarizzare (max 6 mesi). Se risulta l'adempimento della prescrizione del Garante, l'autore del reato è ammesso a pagare un quarto del massimo dell'ammenda stabilita. L'adempimento e il pagamento estinguono il reato.
Inosservanza di provvedimenti del Garante (art. 170)	Artt. 26, 90, 143, 150	Reclusione da 3 mesi a 2 anni. Pubblicazione della sentenza.
Violazione del divieto di indagine sulle opinioni dei lavoratori e del controllo a distanza (art. 171)	Art. 113, 114	Arresto da 15 giorni a 1 anno o ammenda da 51 a 516 Euro. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente e sentenza è pubblicata. Quando, per le condizioni economiche del reo l'ammenda può presumersi inefficace, il giudice ha facoltà di aumentarla fino al quintuplo.

DieRRe legal