Associazione Ticinese dell'Information and Communication Technology

Riservatezza dei dati finanziari: Quo vadis ?

Lugano, 27 gennaio 2010

AGENDA

Riservatezza dei dati finanziari: Quo Vadis ?

Equilibri e professionalità fra norme e buone pratiche di governance.

-Introduzione al sistema normativo – Avv. S.Codoni

- La riservatezza dei dati
- -Il segreto bancario
- -Il segreto professionale

-Governare la protezione dei dati – Avv. A. Frillici

- Il bene da proteggere, il valore da garantire.
- La "filiera" del trattamento
- Gestire il rischio
- I fornitori IT della filiera

I PARTE

Avv. Stefano Codoni

POLEDNA | BOSS | KURER

Obblighi di riservatezza

Elementi per l'analisi e la valutazione di un obbligo di riservatezza:

- Su cosa si fonda l'obbligo?
- Ampiezza dell'obbligo e in particolare in quali casi vi sono delle eccezioni
- Sanzioni in caso di violazioni

Sulla base di questa valutazione prevedere:

- Misure per adempiere gli obblighi legali e contrattuali di segretezza
- Eventualmente misure per garantire protezione più ampia ai propri clienti

Segreto professionale

Base: art. 321 CPS, rapporto contrattuale

Ampiezza e eccezioni:

- Avvocati, Medici, Ecclesiastici, Revisori / Non: fiduciari
- Ogni informazione relativa al cliente/paziente
- Funzione vs. titolo
- Diritto di rifiutare di testimoniare in procedure civili o penali
- Possibilità di svincolo da parte dell'autorità di sorveglianza

Sanzioni: penali, civili e disciplinari

Segreto Bancario e Segreto Professionale dei Commercianti di Titoli

Base: art. 47 LBCR / 43 LBVM, rapporto contrattuale

Ampiezza e eccezioni:

- Ogni informazione relativa al clienti della banca/commerciante di titoli
- Diritto di rifiutare di testimoniare:
  - Nelle procedure penali
  - Nelle procedure civili
  - Nelle procedure amministrative/fiscali
  - Nelle procedure esecutive
- Assistenza giudiziaria internazionale vs. segreto bancario

Sanzioni: penali, civili e disciplinari

Dati personali in genere

Base: Legge Federale sulla Protezione dei Dati

Ampiezza e eccezioni:

- Ogni informazione relativa a persone identificate o identificabili
- Comunicazione a terzi di dati sensibili di principio vietata, altri dati a dipendenza della situazione
- Sicurezza dei dati
- Diverse eccezioni (motivi giustificativi)
- Nessun diritto di rifiutare di testimoniare in procedure civili, penali e amministrative

Sanzioni: penali, civili e disciplinari

Impegni contrattuali (in particolare contratto di mandato)

Base: contratto di mandato – per es. consulenti fiduciari

Ampiezza e eccezioni:

- secondo quanto previsto contrattualmente
- di principio nessuna limitazione all'obbligo di testimoniare

Sanzioni: civili

Segreto commerciale e di fabbricazione:

Base: art. 162 CPS, art. 6 LCSl

Sanzioni: penali, civili

II PARTE

Avv. Alessandro Frillici CISM CGEIT

RBF & PARTNERS LV & PARTNERS CONSULTING SA

Proteggere

I dati personali in genere devono essere protetti al fine di rispettare:

- Leggi (nazionali ed internazionali)
- Obbligazioni di natura contrattuale (ad es. clausole di riservatezza)
- Obblighi di altra natura (usi e consuetudini, codici deontologici, codici etici, ecc…)

I dati personali

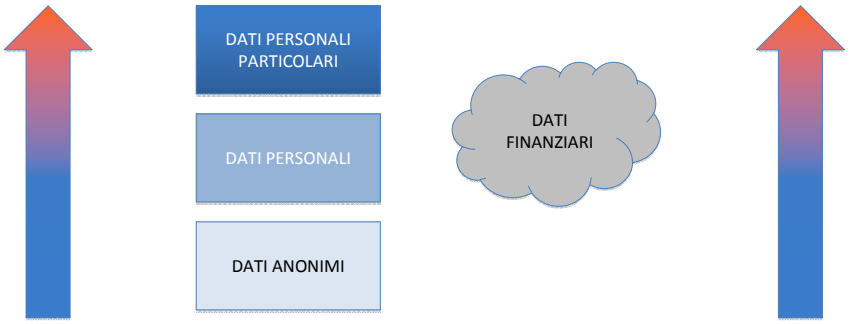
La Direttiva Europea n.46 del 1995 definisce i dati personali come "Qualsiasi informazione concernente una persona fisica identificata o identificabile".

Dello stesso tenore è l'art. 3 della Legge Federale sulla Protezione dei Dati (LPD).

In particolare, ai fini della presente esposizione, si intendono per dati personali finanziari "i dati personali relativi alla gestione delle risorse patrimoniali ed economiche di un individuo".

Curiosamente le diverse normative non inseriscono questa categoria di dati tra quelle particolari, meritevoli di tutela qualificata (Art. 3 Lett.c) LPD – Art. 8 Dir.UE 95/46 – Art. 4 comma 1 Lett. d) Cod.It. Priv.).

Le categorie di dati personali



Il pericolo

Eppure, se la logica dei legislatori è di ritenere i dati personali pericolosi per i diritti fondamentali e la dignità di coloro cui si riferiscono, questa categoria di dati avrebbe ben motivo di essere definita critica.

Normalmente, infatti, questo tipo di informazioni suscita alte motivazioni alla loro conoscenza:

- semplice curiosità,
- Ragioni criminali,
- Ragioni discriminatorie
- …

Ciò significa che la minaccia di perdita di riservatezza è alta.

Da obbligo a prodotto

Esaminiamo il problema secondo diverse prospettive

RISERVATEZZA DEI DATI PERSONALI FINANZIARI → **FIDUCIA**

Necessità di adempiere un obbligo

E' limitato al soggetto responsabile

Si limita a compiere solo ciò che è necessario

E' un costo

Perseguire un vantaggio strategico

Si estende a coloro che sono legati al responsabile (p.es. una categoria, una comunità)

Punta al miglioramento continuo

E' un investimento

PROTEZIONE DEI DATI PERSONALI FINANZIARI → **CREAZIONE E MANTENIMENTO DELLA FIDUCIA** → **MIGLIORAMENTO E STABILITA' DEL LAVORO**

↓

RISPETTO DELLE NORME

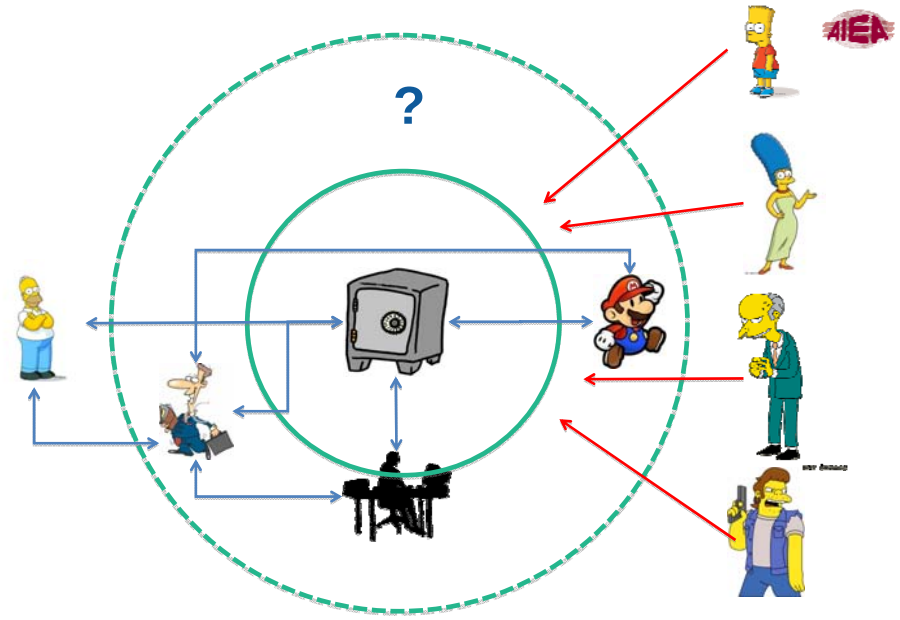
Dalla riservatezza alla fiducia

Una delle regole elementari di qualsiasi attività di sicurezza è che la misura della robustezza di un sistema è data dall'elemento più debole

Se questo principio è importante per la riservatezza lo è ancor più per la fiducia.

Qualsiasi azione deve considerare la "filiera".

Chi può conoscere questi dati ?



La filiera dei dati

Il principale attore nella scena è il sistema bancario, che è tradizionalmente sicuro.

Ma in un sistema aperto sono molteplici i soggetti che, anche incidentalmente, possono venire a conoscenza di tali dati.

E molti sono i soggetti che possono desiderare conoscere tali dati (e non sempre per giusti motivi).

Ed anche quando i motivi sono giusti occorre garantire il rispetto delle regole/leggi perché in queste risiede l'unica garanzia per l'interessato.

Soluzioni

Le Leggi da sole non bastano (l'esperienza quotidiana insegna).

La legge enuclea il principio od individua il fatto, ma, generalmente, non spiega il come.

Occorre individuare un sistema di governo di enti ed imprese che, secondo i principi fissati dalle norme, consideri anche la sicurezza dei dati e che tenga conto non solo degli attori primari, ma anche dell'intera "filiera" e degli interessi degli stakeholder.

A tutti coloro che partecipano alla "filiera" dei dati personali finanziari è richiesta un'alta "diligenza" nel gestire i dati.

Il peso dell'IT

Ad oggi, anche le più piccole realtà, trattano i dati mediante strumenti elettronici (in modo puro o misto).

L'IT è lo strumento più potente e più critico nel trattamento dei dati.

Ai professionisti dell'IT sono richieste specifiche competenze in materia di sicurezza da applicare innanzitutto a se stessi, quali "anelli" critici della "filiera".

Peraltro, tali competenze e la affidabilità, perché possano essere comunicate e trasmesse occorre che siano certificabili, ovvero che possano essere verificate, trasmesse e condivise.

Gli standard internazionali sono strumenti indispensabili.

Non è facile però orientarsi.

Il panorama visto dai professionisti

- ISACA (*Information Systems Audit and Control Association*)
  CISA – CISM - CGEIT
- $(ISC)^2$ (*International Information Systems Security Certifications Consortium Inc*)
  CISSP - SSCP
- SANS Institute
  certificazioni GIAC (GSEC – GCFW – GCIA – GSE …)
- CompTIA
- OSSTM (Open Source Security Testing Methodology)
- EUCIP (European Certification of Informatics Professionals)
- ISMS Lead Auditor
- EC-Council
- SCP (Security Certified Program)

Oltre alle c.d. certificazioni "vendor specific" (CISCO – MICROSOFT – SYMANTEC)

Il panorama visto dal lato servizi-enti

- COBIT – modello per la gestione ICT
- ISO/IEC 27001:2005 – standard per la gestione della sicurezza nelle teconologie dell'informazione
- ISO/IEC 20000:2005 – standard per la gestione dei servizi informatici
- ITIL – good practice per la gestione dei servizi IT

Prepararsi

In vista dell'aumentata sensibilità di coloro i cui dati sono trattati e conseguentemente delle future azioni regolamentatrici dei governi, è opportuno prepararsi da subito.

Le associazioni di categoria come ATED – ICT Ticino ricoprono un ruolo primario, è importante che siano promossi tavoli ove i rappresentanti dei diversi attori della "filiera" possano definire una precisa strategia ed individuare percorsi per vincere la sfida e garantire la massima sicurezza a tutta la "filiera".

Considerato che il cedimento di anche uno solo dei componenti, comprmette la stabilità dell'intero sistema minandone la credibilità, ovvero la fiducia.

Cosa fare

Mentre a livello collettivo si decidono ed attuano interventi, le imprese ed i professionisti IT è opportuno che abbiano:

- definito i propri obiettivi e le strategie.
- Individuato la propria posizione nella filiera.
- Individuato le competenze e le certificazioni appropriate alla propria posizione ed agli obiettivi.
- Effettuato una analisi dei rischi per individuare debolezze e punti di forza ed acquisire le necessarie informazioni per definire le azioni tattiche.
- Sviluppato a medio-lungo termine un programma per formare od acquisire le competenze strategiche.
- Sviluppato ed attuato a breve termine un programma di riduzione dei rischi critici.

Avv. Stefano Codoni
Poledna Boss Kurer
CP 5162
Via F.Pelli, 7 - 6901 Lugano Ti - CH
Email codoni@pbklaw.ch Tel +41 91 911 80 00

Avv. Alessandro Frillici CISM CGEIT
RBF & Partners Ltd
Via Trevano, 63 - 6900 Lugano Ti - CH
Email info@rbfpartners.com. Tel +41 91 971 83 00

ated – ICT Ticino
Casella Postale 1261
6502 Bellinzona, Svizzera
Tel: +41 91 857 58 80
email: info@ated.ch