Informatica e protezione dei dati

Lorenza Rusca
Area dei servizi
di consulenza

I dati sensibili e personali sono tutelati dalla Legge cantonale sulla protezione dei dati personali che, in linea con la direttiva europea sulla protezione dei dati, sancisce il diritto per il titolare di avere tutte le necessarie assicurazioni, affinché i propri dati personali siano trattati con la dovuta cautela al fine di garantirne l'integrità e la riservatezza. Promulgando questa legge, il Governo ticinese ha deciso che i dati personali dei cittadini devono essere protetti allo stesso modo, indipendentemente dal mezzo usato per il loro trattamento: quindi devono essere protetti anche quando facciamo uso dell'informatica.

Belli gli articoli di legge! Quando li vediamo citati da qualche parte, ci infondono un senso di sicurezza; ci sentiamo protetti, difesi contro possibili malfattori che attentano ai nostri beni e alla nostra persona. A maggior ragione se parliamo di dati personali che sentiamo ancora più «nostri». Ma se volessimo tradurre tutto quanto in un linguaggio comprensibile anche per i tecnici che si occupano di informatica? Allora gli articoli diventano definizioni, normative, modalità, regole, procedure e standard. Insomma un insieme di misure per garantire che i dati siano adeguatamente protetti. E per protezione intendiamo non solo la protezione del contenuto degli archivi e delle banche dati, ma anche dei dati in fase di trasmissione, delle copie storiche, dei salvataggi di dati, dei file di log, ecc. In poche parole si tratta di tutto quello che gira attorno ai dati, indifferentemente che si tratti di hardware, software, persone, documenti cartacei, supporti di memorizzazione o altro. Nel mondo informatico le minacce, che potrebbero impedirci di essere conformi alla legge, possono essere così suddivise:

- **Minaccia alla confidenzialità dei dati:** quando i dati sono visibili da processi o utilizzatori che non sono autorizzati ad accedervi. È possibile violare la confidenzialità mediante:
  - un sistema di autenticazione debole. Qui entra in gioco la password personale che deve essere il primo dato a dover essere protetto;
  - il mancato rispetto del segreto d'ufficio;
  - l'intercettazione del traffico di rete. Difficile ovviare a questo inconveniente, ma la soluzione sta nel rendere illeggibili i dati che transitano in rete tramite la crittografia o l'utilizzo di canali criptati;
  - la cattiva progettazione o implementazione dei controlli di accesso ai dati in ambito applicativo o banche dati. Da qui l'importanza che gli stessi siano progettati da specialisti e non da «fai da te»;
  - virus o meglio *spyware*: forme di virus che consentono di carpire informazioni all'insaputa dell'utilizzatore. Ecco l'importanza di aver attivo sul proprio desktop e sui server un buon prodotto Anti-Virus.

- **Minaccia all'integrità dei dati:** quando l'informazione può essere creata, modificata o cancellata da chi non ha le credenziali per farlo. L'integrità può essere messa a repentaglio da:
  - errori ed omissioni provocati dall'introduzione di dati errati nel sistema;
  - virus o codice maligno;
  - attacchi informatici, di solito fatti da interni che, cercando di rimuovere record legati ad azioni non corrette, aggiungono record.

- **Minaccia alla disponibilità di dati e servizi:** quando chi ha diritto di accedervi non può farlo. Sembra paradossale, ma questa indisponibilità, per analogia, può essere paragonata ad una perdita di dati, anche se solo momentanea. Importante, nei casi permanenti, poter disporre di un salvataggio che ci consenta il recupero. L'indisponibilità può essere ricondotta a:
  - guasti o malfunzionamenti dell'hardware;
  - virus;
  - attacchi informatici che distruggono i sistemi;
  - attacchi di tipo *Denial of Service* (DoS) che, per ora, non possono essere prevenuti, ma solo mitigati.

Tanto può essere fatto dall'utilizzatore finale rispettando valori etici come il segreto d'ufficio e la riservatezza dei dati nel proprio ambito lavorativo. Molto può essere fatto con la tecnologia laddove parliamo di disponibilità di dati e servizi o d'utilizzo di sistemi di trasmissione. Resta evidente che, ad infrangere la legge, non è mai una macchina, ma la volontà degli esseri umani che la governano. Noi tecnici, di fronte a questa volontà d'abuso, siamo disarmati, possiamo solo cercare di rendere il compito più difficile e fare in modo di preservare le prove che consentano alla Giustizia di identificare i colpevoli e di condannarli.

Basi legali:

- Legge federale sulla protezione dei dati (LPD) – Art. 7 Sicurezza dei dati
  [1] I dati personali devono essere protetti contro ogni trattamento non autorizzato, mediante provvedimenti tecnici ed organizzativi appropriati.
- Legge cantonale sulla protezione dei dati personali (LPDP), Art. 17 Sicurezza
  Chi elabora dati personali deve prendere misure appropriate di sicurezza contro la perdita, il furto, l'elaborazione e la consultazione illecita.
- Regolamento di applicazione della legge cantonale sulla protezione dei dati personali del 9 marzo 1987 (RLPDP) – Art. 14 Sicurezza (art. 17 LPDP)
  [1] L'organo responsabile prende tutte le misure idonee a garantire la sicurezza dei dati in funzione del tipo di dati elaborati (neutri o sensibili).