Protezione dei dati e sicurezza

Michele Albertini
Responsabile cantonale
per la protezione
dei dati

La protezione e la sicurezza dei dati sono in un rapporto stretto e vicendevole, benché perseguano obiettivi sostanzialmente diversi. Mentre la protezione dei dati si prefigge di tutelare la personalità e i diritti fondamentali delle persone i cui dati sono elaborati, la sicurezza dei dati è volta a garantire la salvaguardia delle informazioni. Più che la diversità degli obiettivi, è importante invece la relazione tra i due concetti, che si riassume in un'affermazione tanto semplice quanto importante: senza sufficienti misure di sicurezza gli scopi perseguiti dalla protezione dei dati risulterebbero vani. A ben vedere, la sicurezza è una premessa essenziale, o meglio, uno strumento per garantire la tutela della personalità. Non a caso quindi i legislatori – federale e cantonali – hanno ritenuto indispensabile richiamare, nelle normative generali sulla protezione dei dati, il principio della sicurezza.

L'esigenza della sicurezza dei dati nella LPDP

La legge ticinese sulla protezione dei dati personali (LPDP) prescrive che «chi elabora dati personali deve prendere misure appropriate di sicurezza contro la perdita, il furto, l'elaborazione e la consultazione illecita» (art. 17 LPDP). Questa norma, al pari delle corrispondenti disposizioni del diritto federale e del diritto degli altri Cantoni, si limita a stabilire il *principio* della sicurezza dei dati. La finalità prima della massima è quella di rendere effettive le disposizioni sulla protezione dei dati: nel contesto della tutela della personalità, la sicurezza dei dati verte principalmente – e tradizionalmente – ad assicurare la *confidenzialità*, la *disponibilità* e l'*integrità* delle informazioni, allo scopo di documentare il rispetto dei principi guida della protezione dei dati (come la liceità, la buona fede, la conformità allo scopo, ecc.; art. 6 LPDP), di dimostrare l'esattezza dei dati (art. 7 e 8 cpv. 2 LPDP), di assicurare al cittadino un esercizio compiuto dei suoi diritti, come il diritto di accesso, di rettifica e di blocco dei dati (art. 23 segg. LPDP), nonché di favorire la corretta eliminazione o archiviazione dei dati (art. 21 e 26 LPDP). Va subito precisato che le disposizioni sulla sicurezza dei dati non si riferiscono a tutti i tipi di informazioni: tutelati sono solo i *dati personali*, ossia le indicazioni che direttamente o indirettamente permettono di identificare una persona, sia essa fisica o giuridica (art. 4 cpv. 1 LPDP). Occorre poi precisare che tutti i *metodi di elaborazione dei dati* devono essere oggetto di misure di sicurezza: l'art. 17 LPDP concerne – indistintamente – la raccolta, la conservazione, l'utilizzazione, la modifica, la trasmissione e anche la distruzione di dati personali (art. 4 cpv. 3 LPDP). Poco importa infine che l'elaborazione avvenga su supporto cartaceo o informatico: la legge è infatti applicabile ad ogni trattamento di dati, indipendentemente dagli scopi, dai modi e dalle procedure utilizzati (art. 2 cpv. 1 LPDP).

Titolari dell'obbligo

L'obbligo di garantire la sicurezza dei dati compete, in generale, a *tutti i soggetti sottoposti alla LPDP*, e cioè il Cantone, i Comuni, gli altri istituti e corporazioni di diritto pubblico e i loro organi, come pure le persone fisiche e giuridiche di diritto privato, cui siano demandati compiti pubblici (art. 2 cpv. 2 LPDP). Un obbligo corrispondente vige anche per i terzi incaricati di elaborare dati personali per conto di uno degli organi appena citati (art. 16 LPDP). Al di là di questi richiami generali, titolare dell'obbligo di garantire la sicurezza dei dati è in prima analisi l'*organo responsabile*, ossia l'autorità che elabora o fa elaborare dati personali per lo svolgimento dei suoi compiti legali e che, in questa veste, decide sul contenuto e sul tipo di utilizzazione dei dati, assicurandone il controllo come pure la gestione (art. 4 cpv. 5 e art. 8 LPDP). Questo dovere è esplicitato del resto nell'art. 14 cpv. 1 del regolamento di applicazione della LPDP (RLPDP), a norma del quale «l'organo responsabile prende tutte le misure idonee a garantire la sicurezza dei dati in funzione del tipo di dati elaborati (neutri o sensibili)». Da un profilo più generale, il dovere sancito dall'art. 17 LPDP riguarda anche i *singoli collaboratori o incaricati* che dovessero elaborare dati personali. Essi devono essere consapevoli dei rischi e delle conseguenze di un trattamento non conforme alla protezione dei dati. In questo senso, è importante rafforzare il concetto di autodisciplina o di autocontrollo dei singoli utenti, perché favoriscano individualmente l'adozione di misure tecniche e comportamentali di sicurezza, per far fronte in modo adeguato ai rischi dettati soprattutto – ma non solo – dall'utilizzazione dei moderni strumenti telematici, in particolare Internet e posta elettronica.

Categorie di misure

La LPDP non indica le tipologie di misure obbligatorie o auspicabili in materia di sicurezza dei dati. Nella prassi è tuttavia consolidato il principio secondo cui, dal profilo della protezione dei dati, occorre tener conto, già al momento dell'allestimento del sistema, non solo dell'aspetto *giuridico*, ma anche di quello *tecnico*, *organizzativo* e *logistico*, come del resto stabilito dall'art. 8 segg. dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD), i cui contenuti assurgono ad elementi di riferimento. In sostanza, l'organo responsabile è tenuto ad adottare provvedimenti tesi in particolare ad impedire a persone non autorizzate l'accesso fisico ai locali e alle banche dati, a garantire la possibilità di verificare a posteriori chi – e in quali tempi e modalità – possa accedere ai dati ed elaborarli nei sistemi informatici, a definire procedure d'autorizzazione personalizzate d'accesso (a dipendenza delle necessità imposte dall'adempimento dei compiti legali), come pure ad assicurare la possibilità di identificare i destinatari a cui vengono comunicati dati personali con l'ausilio di impianti di trasmissione. I sistemi devono in ogni caso essere concepiti in modo trasparente, tali da essere verificabili anche da parte delle istanze preposte al controllo.

Caratteristiche delle misure di sicurezza

I termini «misure appropriate» e «misure idonee», indicati negli art. 17 LPDP e 14 RLPDP, sono espressione del *principio della proporzionalità*. Questa massima, che regge tutto il concetto di protezione dei dati (art. 6 cpv. 2 LPDP), esige che in ogni fase d'elaborazione di dati la probabilità di

identificazione delle persone interessate deve essere minimizzata e commisurata in funzione delle specifiche caratteristiche, modalità e necessità del trattamento. Determinante anche nel contesto della sicurezza, il principio della proporzionalità esige in generale una *valutazione* della gravità delle conseguenze di un'eventuale violazione della protezione, della disponibilità in termini di risorse necessarie (anche finanziarie) a realizzare tali misure e delle probabilità che si verifichi una lesione. Le caratteristiche di ogni sistema di sicurezza possono essere molto diversificate a dipendenza del tipo di elaborazione, come pure dei contesti operativi ed organizzativi in cui si svolge. La massima va quindi concretizzata di caso in caso, tenendo conto peraltro, che l'entità necessaria delle singole misure può essere influenzata anche da precise disposizioni legali dell'ambito specifico (p. es. obblighi del segreto, obblighi di tenuta e conservazione di determinati registri ecc.). Per valutare la proporzionalità – e quindi l'idoneità e l'adeguatezza – di una misura di sicurezza, la prassi ha individuato una serie di *criteri essenziali*, che è opportuno sottolineare. Un elemento importante, come del resto traspare dall'art. 14 cpv. 1 RLPDP, è senza dubbio la *natura dei dati personali*. Più i dati elaborati sono sensibili (perché ad esempio concernono informazioni sulla sfera intima, sulla salute psichica o fisica, o su reati penali) più le esigenze di sicurezza sono accresciute. Per contro dati personali usuali accessibili a tutti non esigono, per questo solo motivo, l'adozione di un dispositivo particolare di sicurezza. Un altro criterio concerne *il modo e l'estensione dell'elaborazione dei dati*. Il tipo specifico di elaborazione (ad esempio manuale o informatico) può essere di rilievo per definire le esigenze in materia di sicurezza: così l'apposizione di un indirizzo su una busta, che costituisce un'elaborazione di dati personali, non dovrebbe esigere importanti cautele, al contrario invece del trattamento sistematico di dati concernenti molte persone, su supporto elettronico. Le esigenze devono essere massime nelle fasi in cui le informazioni hanno la più alta probabilità di identificazione personale, e progressivamente minori in fasi con probabilità ridotta. Particolare attenzione dev'essere prestata alla definizione degli standard di sicurezza delle modalità di trasmissione, per esempio riferiti alla posta elettronica. Occorre poi considerare anche lo *scopo dell'elaborazione di dati*. Le esigenze di sicurezza possono variare sensibilmente a dipendenza se gli interessi perseguiti siano di natura pubblica o privata, se le finalità dell'elaborazione siano l'adempimento di un compito legale, uno scopo commerciale o ideale, oppure se l'elaborazione sia limitata all'uso personale dei propri dati. Nella valutazione va poi prestata particolare attenzione ai *rischi dell'elaborazione* per le persone interessate e allo *sviluppo tecnico*. I rischi principali sono notoriamente: la distruzione accidentale o non autorizzata dei dati, gli errori tecnici, la falsificazione, il furto e l'uso illecito, ma anche la modificazione, la copia, l'accesso oppure un altro trattamento non autorizzato o altrimenti improprio (p. es. incompatibile con le finalità della raccolta). Un'analisi completa dei rischi e dei danni potenziali in funzione dei contenuti e delle modalità del trattamento riveste un'importanza certa, soprattutto nell'ambito dell'elaborazione telematica di dati. A questo proposito, occorre definire e rendere minimi i rischi di danni dipendenti da fattori interni (p. es. causati da dipendenti) o esterni alla singola amministrazione, oppure ambientali. L'adeguatezza e l'efficacia delle misure di sicurezza dev'essere costantemente vagliata alla luce dell'evoluzione dei bisogni, della comparsa di nuovi rischi, dei progressi tecnologici (riferiti ai sistemi e alle applicazioni) e delle procedure di sicurezza. Per quanto attiene alla sicurezza informatica si pensi per esempio ai metodi di autenticazione e certificazione elettronica (come la firma digitale) e alla codifica dei documenti elettronici (crittografia).

Conclusioni

La sicurezza nel contesto della protezione dei dati è un processo dinamico, che non esige però «sicurezza assoluta ad ogni costo», ma l'adozione di provvedimenti proporzionati allo scopo, in base alle conoscenze, alle disponibilità e alle risorse, premesso in ogni caso un costante aggiornamento delle misure per rapporto alle esigenze di tutela dei dati personali. In questo contesto appaiono imprescindibili la designazione, in seno all'unità amministrativa, di un responsabile della sicurezza e dei dati («security manager»), che possa fungere da persona di riferimento (anche per la formazione del personale) e l'elaborazione di un regolamento interno che descriva in particolare, oltre all'organizzazione, anche le procedure di accesso, di elaborazione e di controllo dei dati, e che includa i documenti attestanti la pianificazione, gli strumenti (informatici) come pure, più in generale, la gestione delle banche dati. Nel contesto globale della sicurezza dei dati si attesta inoltre lo sviluppo di procedure volte al rilascio di marchi di qualità (audit relativi alla protezione dei dati), con esame dei processi operativi (sistemi, procedure e organizzazione). Inserite ed esplicitate nella prossima revisione della legge federale sulla protezione dei dati, queste disposizioni si fondano anche sul concetto di autoresponsabilità del detentore della raccolta di dati. Ma il discorso dell'autodisciplina merita di essere esteso a tutti gli utenti e collaboratori, che dovessero elaborare dati personali propri e di terzi. È importante che tale esigenza sia rafforzata per prevenire, già alla base, rischi e violazioni delle normative sulla protezione dei dati.

Informazioni e approfondimenti

Per ragguagli più ampi, destinati in particolare alle persone private e agli organi federali, ma utili anche per gli organi sottoposti alla legge cantonale, l'Incaricato federale per la protezione dei dati ha pubblicato una «Guida ai provvedimenti tecnici e organizzativi concernenti la protezione dei dati», consultabile e scaricabile all'indirizzo **http://www.edsb.ch/i/doku/leitfaeden/tom/tom.pdf**.

In tema di sicurezza dei dati, l'Associazione svizzera dei delegati cantonali e l'Incaricato federale per la protezione dei dati (DSB2CPD.CH) hanno pubblicato un interessante opuscolo divulgativo (purtroppo attualmente disponibile solo in lingua tedesca e francese), che spiega in modo chiaro le misure minime di sicurezza che devono essere applicate da chi fa uso dei moderni strumenti telematici, in particolare Internet e posta elettronica.
Questo opuscolo può essere scaricato all'indirizzo **http://www.dsb-cpd.ch/f/publikationen/depliant_securit%E9_f.pdf** (francese), rispettivamente **http://www.dsb-cpd.ch/d/publikationen/broschuere_sicherheit_d.pdf** (in tedesco).
Per quanto riguarda specificamente la sicurezza in rete, è consigliabile anche la consultazione della sezione «consigli pratici per l'utilizzazione sicura del PC e dell'Internet», curata dall'Incaricato federale per la protezione dei dati **http://www.edsb.ch/i/themen/sicherheit/tipps/index.htm**

Fantasia.

LA MACCHINA DEL TEMPO PER IL BUSINESS. Questa è la sua opportunità. Ha trovato lo strumento per proiettare la sua azienda nel futuro. Un semplice giro di manopola e si troverà nel passato con l'opportunità di correggere gli errori commessi! Questa macchina cambierà il suo modo di fare business. Utopia? Ha ragione. Questa macchina non esiste.

Realtà.

E-BUSINESS ON DEMAND. Le visioni di business del futuro richiedono soluzioni reali. L'era on demand, impone nuovi pensieri e nuove tecnologie. Senza dimenticare le persone che conoscono e capiscono il suo business e le soluzioni tecnologiche necessarie. IBM ha quindi costituito un nuovo settore: IBM Business Consulting Services. Un team di esperti a sua disposizione per offrirle la loro esperienza e consulenza mirata. IBM offre anche nuove prospettive nell'ambito della nuova tecnologia. Esse sono ancora più semplici da integrare e si gestiscono quasi da sole, sia in caso di ottimizzazione delle prestazioni sia in caso di riparazione. Navigate un po' sul nostro sito **ibm.com**/e-business/ch/fr/ondemand per non perdere il prossimo passaggio tecnologico.

BENVENUTO NELL'ERA ON DEMAND.

e business on demand | IBM