Informatica

Privacy e informatica, un difficile rapporto

di Nicola Bortolotti

Nel fervore normativo e legislativo in ambito informatico che contraddistingue il nostro paese da almeno due legislature, l'abitudine tutta italiana ai rinvii e proroghe - spesso esecrata - non sempre vien per nuocere, specie e soprattutto quando segue a serie riflessioni tecnico/normative e - nel contempo - ne impone di ulteriori. Resta censurabile il fatto che ci si ponga certi problemi - da subito evidenti - solo in prossimità delle scadenze; e rimane nodale il fatto che - sovente - le problematiche fondamentali rimangano irrisolte in attesa del pronunciamento dei giudici e costituiscano quindi una inquietante spada di Damocle per chiunque utilizzi anche solo un Personal Computer.

La proroga del DPS

Quanto avvenuto nel caso del posticipo a fine giugno del termine di presentazione del cosiddetto DPS (Documento Programmatico sulla Sicurezza) è, a suo modo, paradigmatico. Il DPS è un documento previsto (per una più ristretta categoria di utenti) sin dal DPR 318/99, il regolamento previsto dalla ben nota legge 675/96 "sulla privacy" ed ora interamente rimpiazzato dal nuovo Testo Unico in vigore da gennaio, ossia il Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (pubblicato nella sua forma originale sulla Gazzetta Ufficiale n. 174 dello scorso luglio e reperibile, tra le numerose fonti in rete, all'URL "ufficiale" del sito del garante della privacy:
http://www.garanteprivacy.it/garante/doc.jsp?ID=487961 con il testo completo all'indirizzo http://www.garanteprivacy.it/garante/doc.jsp?ID=722132).
A suo tempo questa rivista, nel numero 2/2000 ("Le misure di sicurezza minime per il trattamento dei dati personali"), non lesinò perplessità e critiche anche forti all'antesignano DPR 318/99, derivanti non solo da alcune ingenuità tecniche quanto dalla loro commistione con fondamentali aspetti organizzativi e pesantissime responsabilità civili e penali, al tempo mitigate solo dal ristretto ambito applicativo del DPR.
A distanza di pochi anni, e in modo quasi bipartisan dato il cambio di legislatura, lo stesso testo con alcune modifiche, integrazioni e armonizzazioni non sostanziali viene riproposto in veste unitaria, ma il suo ambito applicativo (come ricordato nel numero 4/2003 "Innovazione tecnologica: buoni propositi e discutibili realtà") viene enormemente ampliato e abbraccia ora una cospicua schiera di aziende e professionisti prima esenti da obblighi che non fossero realmente minimali. Nel caso del DPS, ad esempio, il Garante sintetizza al punto 2.2 del parere del 22 Marzo: "In base al nuovo Codice, la misura minima del DPS deve essere ora adottata dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici, attraverso l'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento aziendale o della pubblica amministrazione interessata (art. 34, comma 1, lett. g), del Codice; regola 19 dell'Allegato B). Come accennato, *il DPS deve essere redatto da alcuni soggetti che non vi erano precedentemente tenuti (ad esempio, da chi trattava dati sensibili o giudiziari, ma con elaboratori non accessibili mediante una rete di telecomunicazioni disponibili al pubblico)*. Inoltre, a differenza del passato, la categoria dei dati giudiziari è oggi rappresentata anche da altri dati personali, riferiti ad esempio a provvedimenti giudiziari non definitivi o alla semplice qualità di imputato o indagato (v. art. 4 del Codice)."

Timori non concretizzati

I timori manifestati al tempo del DPR 318/99 non si sono ancora concretizzati: non c'è stata dunque nessuna clamorosa sentenza (o anche solo indagine - essendo l'attività in ambito informatico della Polizia Postale prevalentemente orientata al contrasto alla pedopornografia) che sia finita sulle prime pagine dei giornali (dato l'ambito applicativo assai ristretto del DPR precedente) e questo è stato paradossalmente un male perché non ha messo in luce l'ambiguità, sotto il puro profilo del "diritto", di cui sono permeate le disposizioni di legge che *si rifanno a certezze tecniche che in ambito informatico non possono esistere*.

Per quanto concerne la riproposizione ampliata, il D.Lgs. 30 giugno 2003, n. 196, sorprendeva che una tale e onerosa messe di nuovi adempimenti - soprattutto burocratico-organizzativi più che strettamente informatici - potesse essere assorbito silentemente da aziende e professionisti. Al limite dello scadere del tempo massimo, ecco dunque arrivare in extremis richieste di chiarimenti (ad esempio quelle presentate dall'autorevole fondazione Luca Pacioli - si veda al proposito la circolare numero 10 all'indirizzo:
http://www.fondazionelucapacioli.it/approfondimenti/circolari/default.asp) e la proroga della presentazione del DPS (il comunicato stampa, in sintesi, all'indirizzo:
http://www.garanteprivacy.it/garante/doc.jsp?ID=772126; il parere esteso all'URL:
http://www.garanteprivacy.it/garante/doc.jsp?ID=771307). Ma i nodi principali - stranamente - non sono stati toccati da organizzazioni, associazioni e ordini di categoria; rimanendo irrisolti, è dunque opportuno ricordarli.

Misure minime (ma non così minime) e pene massime

Da un punto di vista strettamente tecnico l'allegato B (ossia il "Disciplinare tecnico in materia di misure minime di sicurezza" contenuto nel Testo Unico, al link:
http://www.garanteprivacy.it/garante/doc.jsp?ID=488497 e che contiene l'obbligo di redazione del Documento Programmatico sulla Sicurezza) non è che un compendio di alcune regole ben note - *e che comunque non sollevano da eventuali ulteriori responsabilità* - alle quali si deve attenere un qualsiasi amministratore di sistema (ma comunque assai pesanti in piccole realtà lavorative): backup periodico e sistematico dei dati, protezione mediante opportuni software - come antivirus e firewall - costantemente aggiornati, controllo degli accessi e così via.

Nel contempo si sofferma però su alcuni dettagli prescrittivi (alcuni dei quali discutibili) che possono creare non pochi grattacapi in sede di perizia e in un'aula di tribunale. Alcuni esempi: come può il titolare assicurare che sia soddisfatto il requisito evidenziato in corsivo? "5. (...) essa [la parola chiave, la password] *non contiene riferimenti agevolmente riconducibili all'incaricato* ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi (...)"; quali possono essere gli "idonei strumenti" di cui al punto 16 ("16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.") se è ben noto che vengono costantemente scoperti e non sempre corretti bug e vulnerabilità in antivirus e firewall tali da renderli di fatto inidonei? Aggiungendo il fatto che "cadenza almeno semestrale", con virus che si propagano nel giro di poche ore, è ormai puntualizzazione risibile e comunque fuorviante.

Un capoverso che sembra dedicato all'obbligo di attivare servizi invasivi del tipo "windowsupdate" è il seguente: "17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.".

In pratica c'è l'obbligo di dotarsi di un collegamento ad Internet veloce (visto che le patches di protezione possono essere di decine di megabyte), di scaricare aggiornamenti che a volte peggiorano la situazione o non sono affatto indispensabili a fini di sicurezza (come ad esempio certi service packs) per poi - alla prova dei fatti, in tribunale - *dover dimostrare l'indimostrabile*, perché le vulnerabilità sono tante e tali da rendere un dibattito tra Consulenti Tecnici d'Ufficio (del giudice) e di parte pressoché inestricabile e *sempre indecidibile*.

Se poi - come accade - il produttore di software decretasse "morto" il suo prodotto, non fornendo dunque più siffatti aggiornamenti, cosa succederebbe dal punto di vista legale? Ne sarebbe vietato l'utilizzo pur disponendo di una licenza illimitata nel tempo?

Il vero problema è la responsabilità

Con questo limitatissimo esempio non si vuole certo mettere in dubbio l'importanza di trattare gli strumenti informatici con meno pericolosa disinvoltura rispetto alle proprie abitudini.

Ma - parimenti - non si può sottacere la voragine di incertezza aperta da tali obblighi, laddove nessun tecnico competente potrà mai certificare in un'aula di tribunale che sia stato fatto *tutto* il possibile per prevenire abusi, semplicemente perché la complessità degli strumenti informatici li rende non testabili e, dunque, dal comportamento imprevedibile in una miriade di casi possibili. Anche il poter contare su strumenti software dal codice aperto (Open Source), ossia analizzabile da parte di chiunque, non risolve il problema dal punto di vista probatorio.
I più diffusi sistemi operativi, poi, sono sostanzialmente non conformi alle richieste dell'allegato B, in certi casi addirittura per scelta del produttore che apre appositamente (e all'insaputa dell'utente) notevoli varchi di sicurezza per fini non sempre chiari. E vale quindi la giusta domanda (alla quale non viene peraltro data risposta, proprio per quanto concerne questo punto nodale) posta da un anonimo lettore all'autorevole testata specializzata Interlex (http://www.interlex.it/675/mscontinua.htm) con riferimento alla licenza d'uso di alcuni prodotti Microsoft: "Mi chiedo: il mio avvocato, il mio medico, il mio commercialista, può nel suo computer con sistema operativo Windows XP (o con Windows 2000 con SP2 che ha la stessa licenza) tenere i dati che riguardano me ed altri suoi clienti e averlo nello stesso tempo collegato alla rete? Lo stesso vale per qualsiasi computer della PA, dove sono custoditi i miei dati. Da un lato deve essere protetto da password e dall'altro si lascia la porta aperta per Microsoft."

L'informatica andrebbe abolita!
Con un'interpretazione letterale del Decreto Legislativo (come già del DPR del '99 che lo precedeva), gli strumenti informatici *non* andrebbero utilizzati per gestire dati personali, soprattutto se sensibili e/o giudiziari.
L'affermazione è ovviamente provocatoria, paradossale e inattuabile, ma così è. Perché *nessun* esperto di sicurezza può onestamente ritenere di avere *blindato* un sistema. Perché nessun "soggetto esterno" (al quale - singolarmente - non è richiesto nessun requisito come un'abilitazione o un'iscrizione a un apposito albo, il che la dice lunga - e basta un semplice confronto con la vetusta 46/90 sugli impianti elettrici - sulla sensibilità solo epidermica all'informatica del legislatore...) potrà attestare la *totale* conformità richiesta al punto 25 dell'allegato B: "25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.".
E quale assicurazione (e in cambio di quale premio) coprirà una responsabilità civile come quella prevista dall'articolo 2050 del codice civile, con inversione dell'onere della prova? ("Art. 15. Danni cagionati per effetto del trattamento 1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.").

Il Garante rimarca
Le possibile e pesantissime conseguenze sono state ribadite e rimarcate anche nel citato parere del Garante del 22 Marzo, del quale è opportuno citare una significativa parte:
"In particolare è stato confermato il principio (evidenziato con maggiore chiarezza dalle nuove disposizioni) secondo cui *le 'misure minime', di importanza tale da indurre il legislatore a prevedere anche una sanzione penale, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza* (art. 33 del Codice). In materia, come già previsto dalla legge n. 675/1996, si distinguono due distinti obblighi:
a) l'obbligo più generale di ridurre al minimo determinati rischi.
Occorre custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.
Resta in vigore, *oltre alle cosiddette 'misure minime', l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze*, avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi (art. 31).
Come in passato, *l'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati*; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), *ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice)*;

b) *nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le 'misure minime'*.
Nel quadro degli accorgimenti più ampi da adottare per effetto dell'obbligo ora richiamato, occorre assicurare comunque un livello minimo di protezione dei dati personali.
Pertanto, in aggiunta alle conseguenze appena ricordate, *il Codice conferma l'impianto secondo il quale l'omessa adozione di alcune misure indispensabili ('minime'), le cui modalità sono specificate tassativamente nell'Allegato B) del Codice, costituisce anche reato (art. 169 del Codice, che prevede l'arresto sino a due anni o l'ammenda da 10 mila euro a 50 mila euro,* e l'eventuale 'ravvedimento operoso' di chi adempie puntualmente alle prescrizioni impartite dal Garante una volta accertato il reato ed effettua un pagamento in sede amministrativa, ottenendo così l'estinzione del reato)."

Nessuno può dirsi sollevato dagli obblighi

E per chi si sentisse a priori "al sicuro", non trattando dati sensibili e/o giudiziari, valga la sibillina nota conclusiva che conclude la ricordata circolare numero 10 della Fondazione Luca Pacioli: "Diverso il discorso per quanto riguarda le professioni economico-contabili. Non sembra infatti possa ravvisarsi in questa area il trattamento di dati sensibili o giudiziari. Per quanto attiene la compilazione delle dichiarazioni dei redditi, infatti, non sembra sia contemplato alcun trattamento di dati sensibili, neanche in relazione alle spese sanitarie per le quali è possibile risalire unicamente agli importi e non allo stato di salute del contribuente. Pertanto, a nostro avviso, i ragionieri e i dottori commercialisti non dovrebbero essere tenuti alla redazione del documento. *Nonostante questa indicazione di massima, consigliamo comunque la predisposizione di un documento costruito secondo lo schema del DPS a supporto della predisposizione delle altre misure di sicurezza che comunque dovranno essere adottate (si veda in merito la Circolare n. 9 del 19 marzo 2004)."*

Ma ci sono anche buone notizie

Mentre l'inquietante spada di Damocle chiamata "tutela della privacy" rimane appesa sul capo di chiunque utilizzi strumenti informatici, l'iperattività del ministro Stanca (http://www.innovazione.gov.it) continua a dare buoni frutti.
Nel numero 2/2003 ("Gioie e dolori della posta elettronica") si era dato risalto alla pubblicazione sul sito del CNIPA (l'organismo ufficiale che prosegue l'attività dell'AIPA) delle già mature "Linee guida del servizio di trasmissione di documenti informatici mediante Posta Elettronica Certificata" e relativo allegato tecnico.
A distanza di un anno, alla "e-mail raccomandata" - ossia alla PEC - è giunto l'imprimatur definitivo del Consiglio dei Ministri come si può leggere nella nota pubblicata sul sito http://www.cnipa.gov.it e che fornisce il quadro della situazione: "Il Consiglio dei Ministri nella seduta del 25.03.2004 ha approvato in via preliminare uno schema di decreto presidenziale, su proposta del Ministro per l'Innovazione e le Tecnologie di concerto con il Ministro per la Funzione Pubblica, che intende disciplinare le modalità di utilizzo della Posta Elettronica Certificata (PEC) non solo nei rapporti con la Pubblica Amministrazione, ma anche tra privati cittadini. Il provvedimento adottato pone in rilievo i due momenti fondamentali nella trasmissione dei documenti informatici: l'invio e la ricezione. 'Certificare' queste due fasi significa che il mittente riceve dal proprio gestore di posta una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Il decreto stabilisce inoltre che nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte venga conservata per 24 mesi in un apposito registro informatico custodito dai gestori, con lo stesso valore giuridico delle ricevute. Viene anche istituito un elenco ufficiale dei gestori di PEC presso il CNIPA, al quale sono assegnati compiti di vigilanza e controllo sull'attività degli iscritti."
Via libera definitivo, dunque, ad un servizio che ha ottime probabilità di diventare il più utilizzato nella rete negli anni a venire.
Un altro significativo passo avanti è stato fatto nell'archiviazione ottica con la deliberazione CNIPA n. 11 del 19 febbraio 2004 (sempre reperibile sul sito) pubblicata sulla Gazzetta Ufficiale n. 57 del 9/3/2004 e inerente "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali" in sostituzione della deliberazione AIPA n. 42/2001, argomento sul quale si ritornerà nei prossimi numeri.