

La comunicazione elettronica delle informazioni, la loro utilizzazione commerciale e le esigenze di tutela della privacy e sicurezza dei dati

Andrea Stazi

(estratto da F. Graziadei, G. Rizzo, A. Stazi, "Reti e contenuti nella prospettiva della convergenza: scenari ed opzioni aperte dallo sviluppo del digitale", pubblicato in "Il diritto dell'informazione e dell'informatica", n. 3/2005")

1. Premessa. La comunicazione elettronica ed i rischi per i dati personali.

L'utilizzazione "ampliata" e "multicanale" delle informazioni, che da un lato può senz'altro produrre il beneficio di un allargamento dei mercati e delle offerte di comunicazione, sotto un diverso profilo può dar luogo ad un aumento delle minacce alla privacy e alla sicurezza dei dati personali immessi in tale "Rete telematica integrata".

Di qui, una possibile conseguente riduzione della propensione soggettiva all'utilizzo stesso dei mezzi di comunicazione elettronica: si pensi in particolare, al riguardo, da un lato, al fenomeno dello spamming ed ai disagi che il medesimo comporta per i titolari di caselle di posta elettronica; dall'altro, alle difficoltà ed incertezze operative che accompagnano, quanto meno nel nostro Paese, lo sviluppo del cosiddetto e-commerce.

2. Le misure di sicurezza richieste per il trattamento di dati con strumenti elettronici dal nuovo Codice per la tutela della privacy.

Un contributo fondamentale, in argomento, appare quello proveniente dal nuovo Codice in materia di protezione dei dati personali, che ha recepito la precedente disciplina in materia al fine di completarla con adattamenti rispondenti alla continua ed inesorabile evoluzione dei sistemi informatici.

Nel nuovo corpus normativo, infatti, oltre a prevedersi in generale il divieto di utilizzare una rete di comunicazione elettronica per accedere ad informazioni archiviate nell'apparecchio terminale di un abbonato o utente, per archiviare informazioni o per monitorare le operazioni dell'utente - salvo peraltro il caso di determinati scopi legittimi relativi alla memorizzazione tecnica (per il tempo strettamente necessario alla trasmissione della comunicazione) o alla fornitura di uno specifico servizio richiesto dall'abbonato o utente (che abbia espresso il proprio consenso al trattamento) - vengono disciplinati in modo specifico gli aspetti tecnici delle misure di sicurezza da applicare, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, alle diverse operazioni che contemplano l'impiego di dati di natura personale, con particolare riguardo proprio alla trasmissione dei dati per via telematica.

I soggetti fornitori di servizi di comunicazione elettronica sono tenuti ad adottare tutte quelle misure tecniche ed organizzative idonee rispetto al caso concreto, e comunque

adeguate al rischio esistente per salvaguardare da ogni forma di utilizzazione o cognizione non consentita sia la sicurezza dei servizi offerti, sia l'integrità dei dati relativi al traffico e all'ubicazione dell'apparecchiatura terminale dell'utente. Inoltre, quando per aversi un'effettiva sicurezza del servizio o dei dati è richiesta anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica deve adottare tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni.

Il fornitore di servizi, ancora, è tenuto a fornire una specifica informativa nei confronti degli abbonati ed, ove possibile, degli utenti, tutte le volte in cui sussista un particolare rischio di violazione della sicurezza della rete, dovendo altresì indicare, quando il rischio è al di fuori dell'ambito di applicazione delle misure che egli stesso è tenuto ad adottare, tutti i possibili rimedi e i relativi costi presumibili. Attraverso quest'insieme di disposizioni, dunque, il Codice in sostanza recepisce integralmente le prescrizioni dettate in tema di sicurezza dalla direttiva 2002/58/CE.

Il Codice demanda, poi, al Disciplinare Tecnico di cui al suo "Allegato B" la determinazione degli aspetti organizzativi e delle modalità di applicazione delle misure di sicurezza dei dati personali.

In base ad esso, i sistemi informatici utilizzati per il trattamento dei dati debbono, affinché il trattamento venga eseguito lecitamente, rispettare una serie di "misure minime di sicurezza".

Innanzitutto, in tal senso, essi dovranno essere dotati di un sistema di "autenticazione", ovvero di identificazione certa dell'utente mediante un apposito processo di riconoscimento (password, smart card, impronta digitale, etc.), e di adeguate procedure di gestione delle relative credenziali di autenticazione ; nonché di un successivo sistema di "autorizzazione" - ovvero quel meccanismo attraverso cui il sistema concede o meno, all'utente già autenticato, l'accesso a determinati dati o programmi (quali ad esempio un database o una risorsa di Rete).

Il titolare dovrà, inoltre, curare l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici - e ciò in particolare attraverso l'aggiornamento dei software antivirus "con cadenza almeno semestrale" e dei software volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti "almeno annualmente" (salvo per il caso di trattamento di dati sensibili, per cui l'aggiornamento deve essere almeno semestrale) - nonché, ancora, l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati sensibili.

Per quei casi residuali, poi, nei quali la limitatezza tecnologica degli strumenti in uso o la loro obsolescenza non consentano di attuare completamente il dettato normativo, è prevista una dilazione dei termini per mettersi a norma , con l'obbligo per il titolare di

descrivere in un documento avente data certa, da custodire presso la propria struttura, gli impedimenti tecnici che hanno reso impossibile o parziale l'immediata applicazione delle misure minime di sicurezza.

Il Codice prescrive, inoltre, la redazione e l'aggiornamento annuale di un Documento Programmatico sulla Sicurezza (DPS), qualificandone specificamente finalità e contenuti. In particolare, riguardo alle misure di protezione da adottare, il Codice si propone l'obiettivo di tutelare l'integrità e la riservatezza dei dati in tutte le fasi del trattamento (raccolta, registrazione, correzione, trasmissione, distruzione), con misure: a) fisiche (quali, ad esempio, limitazione degli accessi ai locali, protezione delle aree, presenza di armadi con chiave); b) logiche (antivirus, firewall); c) organizzative (nomine, sensibilizzazione del personale e dei collaboratori).

Riguardo al contenuto del suddetto DPS, è espressamente previsto, per quanto di rilievo in questa sede, che esso contenga: - l'elenco dei trattamenti di dati personali ai quali si procede e l'analisi dei rischi incombenti sui medesimi; - la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati; - le misure da adottare per garantire l'integrità e la disponibilità dei dati stessi, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità.

Quanto fatto per la tutela dei dati, infine, dovrà in ogni caso essere documentato in un atto avente data certa.

3. Le "misure minime di sicurezza" del Codice privacy sono sufficienti ed effettivamente praticabili nel contesto delle comunicazioni elettroniche?

E' opportuno domandarsi, riguardo alle suddette previsioni - ed al di là della tempistica che sarà effettivamente necessaria per la loro attuazione, come accennato in precedenza già più volte prorogata ed in generale certamente non priva di difficoltà ed incertezze per gli operatori - se esse siano o meno sufficienti, di per sé, a fornire soluzione al possibile incremento delle minacce alla privacy e alla sicurezza dei dati immessi nella nuova rete integrata delle comunicazioni. Già ad una prima analisi, la risposta a tale quesito appare negativa.

E' vero, come si è detto, che tali disposizioni apportano un notevole contributo al sistema normativo della materia ed alla sicurezza dei dati trattati. E' però altrettanto vero, nel contempo, che da un lato per proprie carenze intrinseche, e dall'altro per la loro natura congenitamente connessa al carattere "personale" dei dati immessi nella rete, le disposizioni in tema di tutela "tecnologica" del trattamento di dati personali con strumenti elettronici non risultano certamente esaustive delle esigenze di sicurezza inerenti alla circolazione delle informazioni on line.

Ancor prima, non soltanto si mette frequentemente in dubbio la effettiva utilità, o meglio "praticabilità", di misure di sicurezza in un orizzonte, quello delle comunicazioni elettroniche, che appare sempre più incessantemente dematerializzato, naturalmente avulso dai controlli, ed in cui in ogni caso il progresso delle tecnologie risulta sempre più rapido dei provvedimenti normativi, eternamente costretti a "rincorrerlo". Ma ci si interroga anche, allo stesso tempo e proprio in virtù di tali fattori, su quale sia la strada migliore da percorrere per contrastare i suddetti fenomeni, se quella degli strumenti giuridico-regolatori o quella degli strumenti tecnici (con tutti i dubbi sopra citati che questi ultimi suscitano).

In argomento, innanzitutto, abbandonare il mondo delle comunicazioni elettroniche alla legge della giungla, non sembra un'opzione da prendere in considerazione, anche per la sua sempre maggiore incidenza su primari interessi "extra-elettronici" (informazione, proprietà intellettuale, concorrenza, etc.).

D'altronde, sembra opportuno segnalare come l'esperienza degli ultimi anni evidenzi la diffusione, tra gli operatori del settore, dell'erronea convinzione secondo cui la sicurezza dei dati personali possa essere garantita da rimedi puramente tecnici (quali l'installazione di un firewall o di un antivirus).

E' partendo dal polo opposto a tale visione, viceversa, che il citato Disciplinare Tecnico del Codice privacy si occupa dell'opportunità che i meccanismi predisposti per la sicurezza siano formalizzati e verificabili, collegando inoltre l'effettività delle misure alle adeguate informazione e consapevolezza dei rischi da parte degli utenti delle banche dati.

Proprio l'esempio di tale Codice, sia pure con le sue suddette carenze e la sua natura inevitabilmente "settoriale", appare porsi quale adeguato strumento per una soluzione dei dubbi da ultimo riportati, indicando in sostanza quale via auspicabile, anche a livello di disciplina generale degli aspetti in esame nel settore delle comunicazioni elettroniche, quella di una normazione attenta e costantemente vigile rispetto alle evoluzioni del settore medesimo, che indichi dettagliatamente e specificamente le misure di sicurezza da adottarsi da parte dei soggetti coinvolti ad ogni livello nella circolazione delle informazioni.

Ciò naturalmente, si badi bene, senza trascurare nello stesso tempo l'importanza, ai fini della tutela della sicurezza e della privacy nelle comunicazioni elettroniche, dell'impiego di strumenti più strettamente e direttamente "pratici" - quali ad esempio carte prepagate o accordi e-traders - distributori off line, e così via - che con sempre maggior frequenza gli operatori del settore stanno tentando di promuovere tra il pubblico (in particolare riguardo a strumenti ritenuti particolarmente "a rischio" come ad esempio l'e-commerce), per incrementare in misura sempre maggiore la propensione soggettiva degli utenti all'utilizzo dei mezzi di comunicazione elettronica.