

SICUREZZA INFORMATICA: ASPETTI GIURIDICI DELLA RESPONSABILITÀ

AVV. DANIELE MINOTTI
Studio Legale Minotti, Genova

L'argomento della sicurezza informatica è sicuramente alla moda, ma, allo stesso tempo, assai attuale e serio.

Malgrado i primi segnali di interesse, da parte del legislatore, siano giunti con la legge 547/93 (in ritardo rispetto al fenomeno dell'informatica, ma in anticipo se si guarda alla diffusione commerciale di Internet in Italia), l'attenzione di giuristi e tecnici si è concentrata, non del tutto a sproposito, sulla successiva l. 675/96 riguardante i dati personali (e, come si vedrà, non soltanto il più ristretto ambito della c.d. "privacy") che, sempre di più, sono gestiti da tecnologie informatiche.

La legge menzionata, completata dal Regolamento sulle misure di sicurezza minime (D.P.R. 318/99), ha, per la prima volta nel nostro Paese, disciplinato in maniera organica la materia imponendo precisi comportamenti attivi che, sino a quel momento, erano considerati, incidentalmente, soltanto in norme riguardanti alcuni reati informatici (es. art. 615-ter c.p. di cui si dirà).

Importanza fondamentale assumono, in tale prospettiva, le misure di sicurezza (non soltanto informatiche; cfr. art. 2 D.P.R. 318/99) menzionate nell'art. 15 l. 675/96 e più precisamente regolate dal decreto del 1999.

Scendendo nel particolare, non si può fare a meno di stigmatizzare la "confusione" in cui non pochi cadono e cioè quella riguardante, da un lato, le "misure di sicurezza" ex art. 615-ter c.p. e, dall'altro, le "misure di sicurezza minime" di cui fa menzione l'art. 15 l. 675/96 che possono coincidere tecnicamente, ma che dal punto di vista giuridico si pongono in ben differenti prospettive.

Nella prima norma il riferimento è alle misure di sicurezza che devono essere presenti affinché l'intrusione in un sistema, informatico o telematico, possa definirsi penalmente

illecita. Emerge, pertanto, la funzione "simbolica" delle misure, quella funzione che, secondo parte della dottrina giuridica, coincide con un ipotetico avviso "vietato l'accesso". Nulla di più, nulla di meno, soltanto, sotto questo profilo, un qualcosa che, quanto meno, renda edotto colui che si appresta ad accedere ad un sistema che quella è un'area riservata e non pubblica e che, secondo buona parte delle dottrine, coincida con un sistema "logico" e non "fisico".

Sebbene, in un certo senso, si possa parlare di "tutela imposta" (per la verità a beneficio dei terzi i cui dati sono trattati), ben diversa è la funzione delle misure di sicurezza (minime) regolate dalla l. 675/96 e dal successivo Regolamento. Come chiarisce l'art. 15 l. 675/96, le misure di sicurezza (obbligatorie in una data misura minima) hanno la funzione di scongiurare i "rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Ecco perché, come accennato, è consentito sostenere che la c.d. "legge sulla privacy" non è (soltanto) tale e che, per adottare la dizione più semplice, meno in voga ma sicuramente più corretta, occorrerebbe parlare di "legge sui dati personali" (peraltro, coerentemente con quanto fatto dal legislatore).

Ma quel che è più centrale nel nostro discorso è che, rispetto all'art. 615-ter c.p., le conseguenze previste dal legislatore sono esattamente ribaltate. Nella norma del codice, l'omessa predisposizione comporta il venir meno della tutela che, altrimenti, sarebbe accordata. Se non si predispongono misure di sicurezza non è possibile attivare le difese penali contro l'intruso (ecco perché, sovente, il titolare del sistema non denuncia le intrusioni. Soltanto per non appalesare il basso livello di sicurezza predisposto).

Nella legge sui dati personali, invece, l'omissione comporta, a determinate condizioni, il sorgere di una responsabilità penale in capo al titolare del sistema con cui viene effettuato il trattamento e di altri soggetti (art. 36 l. 675/96) e va precisato che la sanzione penale può scattare indipendentemente da qualsiasi intrusione.

L'esperienza dimostra che, malgrado di sicurezza informatica si parli quotidianamente e a tutti livelli (in particolare giuridico e informatico) l'argomento è ampiamente trascurato o, nei casi migliori, trattato con estrema superficialità verosimilmente a causa di quella confusione di cui si accennava. Ne è prova, tra l'altro, l'estrema diffusione di virus, worm e, in generale, *malicious codes* evidentemente non contrastati da efficaci e aggiornati sistemi antivirus e *firewall* pur richiesti dalla legge (cfr. art. 4, lett. c), d.P.R. 318/99).

Al di là di ciò, non va, però, esclusa una diversa forma di responsabilità, quella civile di cui all'art. 18 l. 675/96: "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile". Il richiamo all'art. 2050 c.p. (che disciplina il regime dalla responsabilità per fatto illecito relativo alle attività definite "pericolose") non è certo cosa da poco: "Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno".

In termini giuridici, si tratta di una chiara quanto gravosa inversione dell'onere della prova. In termini pratici, un inequivocabile segnale della necessità di predisporre misure di sicurezza "allo stato dell'arte".