



Note a margine alla società della sorveglianza # 1¹

di Chiara Fonio

Pubblicato: 20/02/2009



by Celine Shenton

La **Giornata Europea della Protezione dei dati Personali** è stata dedicata ai social network.

ITSTIME, presente all'incontro (<http://www.garanteprivacy.it/garante/doc.jsp?ID=1582491>) tenutosi in Università Cattolica il 28 gennaio scorso, coglie l'occasione per "fare il punto della situazione" riguardo i social network, la privacy e il controllo.

Il Presidente del Garante Francesco Pizzetti e Mauro Paissan hanno sottolineato la necessità di riflettere sul fenomeno dei social network a causa del notevole successo ottenuto anche in ambito nazionale. Facebook (<http://www.facebook.com>), per esempio, raccoglie 150.000 milioni di utenti in tutto il mondo tra i quali 6 milioni e mezzo di profili personali di cittadini di nazionalità italiana (dato raccolto il 23/01/09). Lungi dal demonizzare i siti in questione, gli esponenti dell'Autorità Garante hanno piuttosto cercato di enfatizzare l'esigenza di una maggiore consapevolezza dell'uso da parte degli utenti. In particolare, le dimensioni sociali della privacy, le potenziali conseguenze inattese e un uso dei dati diverso rispetto a quello auspicato.

I rischi sui quali si sono maggiormente soffermati sono:

- I furti di identità;
- l'impossibilità di eliminare definitivamente i dati immessi per costruire un profilo (cancellare un profilo non significa cancellare automaticamente i dati);
- le ricadute in ambito professionale (la nostra identità, ha affermato Paissan, è sempre più "mobile" ed ancorata a forme di rappresentazione online che possono avere un impatto negativo sulla nostra vita professionale);

¹ Inizia oggi il primo appuntamento a scadenza mensile dedicato ai temi della sorveglianza, del controllo e della privacy. Per segnalazioni e commenti si prega di contattare l'autrice a questo indirizzo: chiara.fonio@unicatt.it

- l'utilizzo di informazioni sensibili da parte di terzi senza il consenso dell'interessato.

La necessità di regolazione normativa deve essere accompagnata da pratiche di auto governo basate su una maggiore consapevolezza. E' stato ribadito più volte che il più potente anti-virus è costituito dagli utenti che dovrebbero battersi per la libertà e sicurezza nell'uso della rete più che per "*lasciare la rete più libera*". La globalizzazione senza regole si sta traducendo in una mancanza di sufficienti garanzie per gli habitués della rete. All'interno della network society il dato assume un peso notevole in quanto può essere facilmente associato all'identità off line costruendo una rappresentazione "altra" derivante dall'incrocio di più elementi che possono limitare le chances di vita degli attori sociali.

Cosa fare? Le buone pratiche proposte dall'Autorità sono semplici ma efficaci:

- scegliere *cosa* condividere;
- scegliere *consapevolmente* (per esempio, non dimenticarsi che alcune informazioni possono danneggiare la ricerca di lavoro);
- usare *pseudonimi*;
- astenersi dal postare informazioni relative ad altri *senza il loro consenso* (es. "taggare" le foto in facebook associando all'immagine di un amico il profilo personale);
- leggere le *privacy policies*.

Mentre gli studi dedicati ai social network e alle dimensioni sociali della privacy sono al centro dell'attenzione di studiosi e accademici (due esempi tra tutti: la tesi di dottorato di danah boyd http://www.zephor.org/thoughts/archives/2009/01/18/taken_out_of_co.html e il saggio di Grimmelmann http://works.bepress.com/cgi/viewcontent.cgi?article=1019&context=james_grimmelmann), in Italia manca uno studio sistematico in merito. Si segnala a questo proposito un progetto di ricerca al quale partecipiamo denominato **Social Network Sites Italia** (<http://larica-virtual.soc.uniurb.it/socialnetworkitalia/>).

Non va dimenticato, tuttavia, che la società della sorveglianza digitale ha ancora delle coordinate "materiali" ben precise che si manifestano nell'uso sempre più invasivo di tecnologie di sicurezza all'interno dello spazio urbano. Questi sistemi socio-tecnici hanno contribuito a ridefinire, non solo i rapporti tra i cittadini, ma anche quelli tra questi ultimi e lo stato. E' di recente pubblicazione il report del Parlamento britannico intitolato **Surveillance: Citizens and the State** (<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm>) che sarà commentato nel secondo appuntamento della nostra rubrica.

Un'altra notizia recente che riguarda la città di Milano, invece, è la messa in rete di tutti gli occhi elettronici della città (<http://milano.repubblica.it/dettaglio/Tredicimila-telecamere-per-spiare-Milano-De-Corato:-in-rete-anche-gli-impianti-privati/1590544>). E' bene ricordare che le telecamere di Milano sono già "in rete", ovvero le immagini arrivano alla centrale di Piazza Beccaria. La differenza risiederà probabilmente in una maggiore responsabilità da parte degli operatori alla videosorveglianza che si trovano alla centrale rispetto a quelli che lavorano nei posti di controllo locale (oltre a nuove potenzialità tecniche). Inoltre il "rischio Grande Fratello" paventato nell'articolo sopra menzionato è reale nella misura in cui il sistema integrato farà convergere anche le immagini delle telecamere private.

La videosorveglianza continua ad essere oggetto di analisi e di studio da parte di equipe di ricerca internazionali. Si ricorda a questo proposito il progetto canadese **SCAN** (<http://www.surveillanceproject.org/projects/scan>) al quale partecipa chi scrive. La prima parte del report ha ottenuto un'ampia risonanza sulle pagine dei media locali.

La sorveglianza è stata inoltre ampiamente utilizzata nel corso dei grandi eventi sportivi degli ultimi anni. Anche in questo caso, però, sembrano mancare degli studi sistematici in grado di mettere in luce le ricadute sociali delle tecnologie di sicurezza, la loro efficacia e l'eventuale mancato smantellamento a "giochi" conclusi. Il workshop **The Surveillance Games** (<http://www.surveillanceproject.org/node/288>) sembra voler colmare queste lacune.