



Sicurezza e nuove tecnologie: la videosorveglianza

Chiara Fonio

Università Cattolica – Dpt. di Sociologia

Aprile 2006

Negli ultimi decenni abbiamo assistito a un sempre più esteso utilizzo di nuove tecnologie di controllo sia all'interno dello spazio pubblico sia nell'ambito del settore privato. Il notevole incremento del numero di telecamere con fini di deterrenza e l'utilizzo di sofisticati dispositivi biometrici rappresentano la risposta più evidente al bisogno di sicurezza nel mondo post 11 settembre. Sarebbe tuttavia fuorviante considerare l'attacco terroristico del 2001 come l'evento scatenante che ha aperto la strada ai mezzi di sorveglianza. Va infatti ricordato che gli apparati tecnologici di controllo sono stati massicciamente utilizzati per scopi militari durante tutto l'arco del XX secolo. Piuttosto, la novità sembra risiedere nell'inserimento delle nuove tecnologie di sicurezza *all'interno della vita quotidiana*. Le minacce del terrorismo internazionale hanno da un parte amplificato la domanda di sicurezza dei cittadini, dall'altra spinto le istituzioni ad attuare una serie di politiche basate anche sulle potenzialità offerte dai dispositivi tecnologici. Come afferma David Lyon, "dopo l'11 settembre, non solo chiunque è un potenziale sospetto, ma chiunque è una potenziale spia" (2005:54). Lyon aggiunge inoltre che il miglioramento della sorveglianza elettronica è passato attraverso 4 metodi principali strettamente correlati tra loro:

1. la biometria,
2. le *smart cards*,
3. la videosorveglianza,
4. le intercettazioni

Il primo consiste nella misurazione di variabili fisiologiche, come l'impronta dell'iride o alcuni tratti del volto, con fini identificativi. Le tecniche biometriche di identificazione possono essere applicate sia al controllo dell'accesso a luoghi ed informazioni, sia all'autenticazione di informazioni e sono talvolta associate alle telecamere a circuito chiuso e alle *smart cards*. Queste ultime sono delle carte di credito dotate di un microchip interno la cui tecnologia è ora utilizzata anche per scopi non economici come le carte di identità e i passaporti digitali. Un esempio di *smart card* associata alla carta di identità è la nuova ID britannica proposta dal primo ministro inglese Tony Blair nel febbraio del 2006. L'idea consiste nell'inserire una copia dell'impronta digitale e della retina del possessore all'interno dell'ID. Se allo stato attuale le nuove carte di identità inglesi non esistono ancora, alcuni governi, come quello peruviano, hanno già provveduto a incorporare un chip per il riconoscimento facciale all'interno delle *cards* dei cittadini (Lyon, 2005: 74). Per quanto concerne invece le intercettazioni telefoniche e, più in generale, le forme di sorveglianza all'interno del World Wide Web basti pensare al cosiddetto "pacchetto sicurezza" approvato l'anno scorso in Italia che prevede, tra le altre misure, la non cancellazione dei dati relativi al traffico telefonico e telematico fino al 31 dicembre 2007. Le informazioni da conservare riguardano i dati anagrafici dei clienti e i *log files* dei server che contengono i dati del traffico.

Tra queste misure la più facilmente utilizzabile, sia per questioni economiche sia per relativa facilità con la quale è possibile gestire e migliorare l'apparato tecnologico implicati, è la videosorveglianza. Le telecamere si prestano più di altri mezzi a essere implementate attraverso i dispositivi biometrici e rappresentano una delle tecnologie di sicurezza maggiormente utilizzate. Come sostengono Norris, McCahill e Wood, la videosorveglianza è diventata una vera e propria tendenza a livello internazionale (2005). A questo proposito, sebbene la bene la Gran Bretagna detenga il primato europeo in quanto a estensione e

investimento pubblico, non va dimenticato che la videosorveglianza è oramai utilizzata ampiamente in quasi tutti i paesi del mondo. In America, per esempio, la diffusione delle telecamere ha seguito lo stesso trend europeo: dall'impiego nel settore privato i dispositivi di controllo sono gradualmente arrivati anche nello spazio pubblico, soprattutto dopo gli attacchi terroristici del 11 settembre 2001. Fino a quel momento, infatti, soltanto 25 città americane erano dotate di sistemi di videosorveglianza per monitorare le aree pubbliche (Nieto: 2002). Dopo l'11 settembre le telecamere diventano uno dei mezzi utilizzati per prevenire eventuali altri attacchi. Un esempio su tutti è la città di Chicago nella quale è stato da poco annunciato che saranno installati più di 2000 occhi elettronici in luoghi pubblici (Hunter: 2004). Anche altri paesi la videosorveglianza gode di un sempre più ampio seguito: Wilson e Sutton (2003) ci hanno messo al corrente di alcuni dati inerenti la situazione australiana e neozelandese. Mentre nel 1996 le telecamere erano utilizzate soltanto in 13 città australiane, nel 2002 il numero è salito a 33; in Nuova Zelanda, invece, già 9 città sono dotate di sistemi di questo tipo. Va inoltre aggiunto che paesi quali la Cina stanno investendo notevoli energie e risorse economiche per approntare "a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance" (Walton, 2001 cit. in Norris *et.al*, 2005: 116). In Iran la videosorveglianza è particolarmente utilizzata nella città di Teheran e anche in India, nonostante le telecamere non abbiano un posto di rilievo nei piani di sicurezza nazionale, il mezzo di controllo è diffuso all'entrata delle scuole e nei pressi di grandi magazzini (Times of India: 2002).

Anche in Italia il dispositivo in questione è molto diffuso. Come si legge nella Relazione del 2002 del Garante della Privacy, le finalità che si intendono raggiungere attraverso l'installazione della videosorveglianza sono molteplici: dalla prevenzione di reati, illeciti amministrativi e rilevazione di infrazioni del codice della strada, al monitoraggio del traffico; dal controllo degli accessi agli edifici pubblici e privati alla tutela del patrimonio artistico; dalla sicurezza pubblica al controllo delle zone utilizzate come discariche abusive. L'indagine recentemente condotta nella città di Milano ha evidenziato una generale accettazione degli occhi elettronici da parte dei cittadini ma ha anche sollevato alcuni dubbi riguardanti la tensione tra il bisogno di sicurezza e il diritto alla riservatezza. Se da una parte il binomio sicurezza - nuove tecnologie sembra essere un punto di forza delle politiche nazionali ed internazionali al quale non è possibile rinunciare, dall'altra occorre riflettere sulle potenziali ricadute sociali dei mezzi utilizzati. Nel caso della videosorveglianza, per esempio, viene di rado presa in considerazione la dimensione *sociale* consistente nel monitoraggio di flussi di persone da parte di operatori alla sicurezza i quali, soffermandosi su categorie generalmente associate a comportamenti devianti, favoriscono –anche se inconsciamente– processi di stigmatizzazione. Inoltre, la videosorveglianza va anche inserita nell'ambito di quei "networked systems" in grado di collegare mezzi differenti e di confrontare i dati provenienti da computer diversi. I dati raccolti, oltre ad essere trasferibili ad altri data base, sono anche di tipo visuale, e le immagini sono di per sé rivelatrici di tratti ascritti quali l'etnia o il genere. Non si tratta di profili senza volto, come quelli che si possono ottenere tracciando i navigatori della rete, al contrario le telecamere identificano in modo preciso associando una qualsiasi immagine al genere, alla razza, all'età e, potenzialmente (per esempio nei casi di criminali segnalati dalla polizia) a un nome.

E' indubbio che dati di questo tipo siano più "sensibili" di altri perché i soggetti *non* sono in grado, cosa invece possibile in altri ambiti, di nascondere il genere né tantomeno l'etnia. La videosorveglianza è dunque *qualitativamente* diversa dai mezzi dei quali si è discusso precedentemente perché permette un controllo più invasivo e penetrante di altri: l'identificazione e la localizzazione sono inequivocabilmente contenuti nell'immagine registrata.

Alla luce di quanto detto, occorre riflettere attentamente sui vantaggi e sui rischi connessi alle tecnologie di controllo in modo da evitare analisi semplicistiche che non tengono conto della complessità dell'ambito preso in esame in questa sede. Gli aspetti sociali, legali e criminologici saranno infatti oggetto di successivi approfondimenti.