PARTE TERZA TECNOLOGIE

5. A CASA E AL LAVORO

5.1 Home networking

Le nostre case si stanno sempre maggiormente configurando come ambienti connessi al mondo esterno. Negli ultimi tempi, soprattutto nel settore dei mass-media, stanno nascendo una serie di dispositivi che stravolgono il ruolo passivo del telespettatore e ne esaltano la sua attività. Si sviluppano decoder digitali per far si che l'utente possa scegliere cosa vedere e in quale momento e connettersi alla Reti o dialogare con altre agenzie, consolle multimediali che svolgono molteplici funzioni, come quella di leggere i DvD ad esempio, che permettono ai giocatori di sfidare altri utenti in qualsiasi parte del pianeta, pc che svolgono anche la funzione di televisori e così via (Bolter, Grusin, 2001).

In parole povere si stanno creando le basi per un sistema di trasmissione dei messaggi televisivi e di altre forme di intrattenimento che ponga al centro l'utente esaltando la sua interattività. Per fare questo è necessario però creare un canale di ritorno che permetta all'utente di dialogare. Generalmente come canale viene usata la normale linea telefonica a cui questi dispositivi vengono connessi. Risulta evidente come lo stesso canale venga usato dalle aziende anche per raccogliere una serie di informazioni personali su di noi.

I dati che abbiamo raccolto sono pochi, in quanto queste tecnologie sono in fase d'implementazione, non riguardano tutta la maggioranza della popolazione, anche se in due o tre anni, calcolando la velocità di sviluppo, la riguarderanno, e infine neanche le aziende interessate hanno ben chiare le potenzialità[19] che le nuove tecnologie offrono. Inoltre bisogna dire che gli sviluppi tecnologici non riguardano solo le tecnologie che ci offrono intrattenimento, ma anche tutta la serie di elettrodomestici che circondano le nostre esistenze che verranno solo accennati in quanto saranno tecnologie con le quali avremo a che fare fra cinque o sei anni.

Per quello che riguarda il decoder e le consolle noi non possiamo decidere di far rientrare nessuno dei due in una categoria ben definita, *tecnologie d'identificazione* o *di sorveglianza*, in quanto il confine appare essere troppo sfumato e le informazioni riguardo al funzionamento di questi dispositivi troppo carenti. A nostro avviso, come vedremo avanti per i Player, si configurano come ibridi fra queste due categorie.

5.1.1. Decoder

Il decoder, sia esso basato sul digitale terrestre o sul più conosciuto sistema satellitare, è uno strumento che permette di ricevere un segnale criptato, decodificarlo e di visualizzare un determinato programma. La ricezione del segnale nei sistemi satellitari è affidata ad un'antenna parabolica, mentre nei sistemi digitali terrestri avviene utilizzando l'antenna con cui normalmente riceviamo le trasmissioni.

Per il sistema satellitare all'utente viene concessa una smart card, il cui funzionamento verrà spiegato nel capitolo seguente, che permette allo stesso di

accedere ai servizi, e all'azienda di riconoscere in maniera chiara ed univoca il decoder. Ad ogni smart card è in pratica abbinato un decoder e solo questo è abilitato a ricevere le trasmissioni. In questo modo le aziende riescono a tutelarsi contro eventuali usi impropri.
All'utente viene concesso anche di acquistare determinati prodotti soltanto nel momento in cui desideri guardarli (Pay per View). Le aziende in questa maniera riescono a raccogliere una serie di informazioni personali su ciò che il telespettatore ha visto, è abituato a vedere, o sta vedendo. Le informazioni che vengono fornite alle aziende riguardano, come leggiamo dall'informativa della privacy di *Sky*,[20]:

> 2) a) nome, cognome, sesso, data e luogo di nascita, indirizzo e/o altro recapito per esigenze di fatturazione se diverso da quello di attivazione del servizio, ragione sociale, numero di telefono dell'abitazione o di altro recapito;b) codice fiscale e/o partita IVA;c) tipo, numero e data di scadenza della carta di credito, se si sceglie tale modalità di pagamento;

E inoltre :

> 3) il CPI (Codice Personale di Identificazione), il codice segreto ed i dati relativi all'utilizzo dei servizi Pay per View e Pay TV sono generati automaticamente dal sistema di gestione degli abbonati di Sky.

In pratica tutto ciò che noi vediamo è inserito, in maniera automatica, all'interno dei database dell'azienda. Gli scopi per la raccolta dati vengono chiaramente esplicitati sempre dall'azienda nell'informativa[21]:

> 1) i propri dati personali forniti in questa Richiesta di Abbonamento sono raccolti per essere trattati, direttamente o anche attraverso terzi, mediante comunicazione a questi ultimi, ai fini ed in esecuzione del contratto di abbonamento;
> 12) i dati di cui al precedente punto 2), oltre che per ottemperare agli obblighi previsti dalla legge, da un regolamento o dalla normativa comunitaria, potranno essere trattati direttamente da Sky, indipendentemente dalla conclusione ed esecuzione del contratto di abbonamento, anche per:a) elaborare studi e ricerche statistiche e di mercato; b) inviare materiale pubblicitario ed informativo; c) compiere attività dirette di vendita o di collocamento; d) inviare informazioni commerciali.

Infine

> *6) per le finalità di cui ai punti 1) e 12) della presente informativa, Sky si avvale di società specializzate nell'area dei servizi editoriali, customer service, smistamento e recapito postale, istituti bancari e finanziari, società di recupero crediti, alle quali consegnerà con cadenza periodica i dati di cui ai punti 2), 3)* (corsivi nostri).

Il sistema satellitare permette quindi alle aziende di migliorare significativamente il profilo che hanno su di noi, e offre l'opportunità di indirizzare campagne pubblicitarie mirate.
Per quello che invece riguarda il sistema basato sul decoder digitale terrestre esso si avvale della linea telefonica per far si che l'utente possa comunicare con diversi soggetti. Infatti il *DTT* permette all'utente non solo di accedere a particolari servizi interattivi sviluppati dalle reti, come giochi e simili, ma offre ad esso l'opportunità di dialogare con un'altra serie di agenzie, come le P.A., ed accedere ai servizi che esse

garantiscono. Il funzionamento è basato su un set top box, che è il decoder, che permette tutto questo.
Come per il sistema satellitare è chiaro che tutto ciò che viene visto dall'utente, le transazioni che vengono effettuate tramite il set top box, ed i servizi a cui esso ha accesso saranno registrati dalle diverse agenzie. Non sappiamo gli utilizzi che vengono effettuati dei dati generati ne tantomeno quali dati sono raccolti perché le aziende interessate non hanno un'informativa sulla privacy.
Per quello che invece riguarda le nuove possibilità offerte dai pc che si stanno configurando come strumenti multimediali, permettendo l'accesso a determinati servizi d'intrattenimento forniti dai provider Internet, come nel caso di *Rosso Alice*, vale lo stesso discorso che effettueremo nel prossimo paragrafo parlando del pc in genere.

5.1.2. Consolle

La convergenza di più media in uno può essere notata a pieno nello sviluppo delle consolle. La loro funzione primaria è quella di essere strumenti di gioco, ma si stanno evolvendo fino ad includere al proprio interno lettori DvD, e sistemi di connessione alla Rete.
Prendendo ad esempio l'*XBox* della Microsoft possiamo vedere come essa includa al suo interno molteplici funzioni e si presti ad essere l'emblema della futura convergenza. Attraverso questa consolle l'utente può giocare in rete con altri utenti, può far parte di una community, può guardare film attraverso il lettore. Inoltre la Microsoft ha sviluppato il servizio *XBox Live* che è una carta prepagata, sviluppata in collaborazione con *Poste Italiane*, che offre all'utente la possibilità di acquistare una serie di prodotti on-line. Le consolle in pratica rivoluzionano la televisione facendola diventare un elettrodomestico con molteplici funzioni.
Se andiamo sul sito della Microsoft possiamo vedere come lo sviluppo di tali sistemi ampli notevolmente le capacità di raccogliere i nostri dati personali.

> L'utilizzo di Xbox *Live* presuppone che voi apriate un conto di fatturazione. Al momento dell'apertura del conto vi sarà richiesto di fornire nome, indirizzo, numero della carta di credito, numero di telefono, data di nascita e indirizzo email. Queste informazioni possono essere unite ad informazioni ottenute da altri servizi Microsoft e altri fonti. Quando aprite un conto, siete esortati a creare un Gamertag. Potreste anche essere autorizzati a scegliere soprannomi separati da usare nel gioco. Questi Gamertag e soprannomi saranno mostrati ad altri giocatori quando sarete iscritti a Xbox *Live* e possono essere mostrati unitamente alle vostre statistiche di gioco e allo stato di presenza come indicati nel gioco e/o sul Web.

E inoltre

> Ci sono inoltre informazioni dirette riguardo al vostro utilizzo di Xbox *Live* raccolte automaticamente da Microsoft. Queste informazioni possono comprendere attività come: i momenti di entrata o uscita da Xbox *Live*; i giochi che avete giocato su Xbox *Live*; contenuti che acquistate su Xbox *Live*; e le statistiche del punteggio giochi. Queste informazioni sono utilizzate da Microsoft per la gestione di Xbox *Live*, per migliorare e mantenere la qualità del servizio e fornire statistiche generali riguardo l'utilizzo di Xbox Live, come determinare quali giochi ed aree di Xbox *Live* sono i più popolari. *Questi dati possono anche essere utilizzati per fornire contenuti e pubblicità personalizzati ai clienti il cui comportamento indica che sono*

interessati ad un particolare soggetto. Informazioni globali sul gioco, sul titolo e sull'utilizzazione possono essere condivise con editori di giochi, rivenditori e fornitori di servizi a banda larga così che essi possono valutare le opportunità di marketing relative a Xbox Live *e assistere Microsoft nel migliorare Xbox Live*[22] (corsivi nostri).

Come nel caso del decoder possiamo vedere che le consolle riescono a fornire alle aziende una serie di informazioni personali al nostro riguardo. Più del decoder però esse offrono l'opportunità di monitorare costantemente l'attività dell'utente.
Grazie a questi strumenti la distinzione fra sfera pubblica e sfera privata, centrale nella considerazione della privacy individuale, viene costantemente erosa e anche l'ambiente domestico si configura essere uno spazio di sorveglianza.

5.1.3 Infodomestici

Gli infodomestici non sono altro che elettrodomestici intelligenti che riescono a semplificare e migliorare le funzioni svolte. Possiamo così avere lavatrici che leggono le informazioni di lavaggio direttamente dal capo, forni che si accendono con un messaggio dell'utente, frigoriferi che ordinano la spesa, e così via (Bolter,Grusin,2001).
Nella maggior parte dei casi il loro funzionamento è basato sulle *tags*, di cui parleremo nel prossimo capitolo, o su un sistema di comunicazione con l'utente o altri soggetti. Quello che infatti si cerca di sviluppare è di far si che gli elettrodomestici siano connessi in un network, sia esso la Rete oppure uno locale, attraverso il quale l'utente possa "dialogare" con gli infodomestici in maniera tale da semplificare la propria quotidianità. Questo sistema in pratica permetterebbe a noi di far accendere a distanza i nostri elettrodomestici, o far si che si accendano quando siamo vicini alle nostre case, far ordinare direttamente a loro la nostra spesa, sorvegliare la nostra casa a distanza, attuare un risparmio energetico facendoli accendere solo lo stretto necessario (Bolter, Grusin,2001).
Quello che deve essere evidenziato per il nostro settore d'interesse è che questo network permetterebbe sicuramente anche ad altri soggetti di raccogliere informazioni su di noi. I modi, la quantità, e il tipo dei dati raccolti non possono da noi essere conosciuti in quanto i progetti in questione sono in fase di sperimentazione. Quello che però è certo è che nel momento in cui le nostre case saranno sviluppate come ambienti intelligenti il monitoraggio delle nostre esistenze potrebbe trovare nuovi spazi in cui esercitarsi e far cadere ogni distinzione fra sfera privata e pubblica.

5.2 Pc in Rete

Come abbiamo potuto osservare in precedenza la rete offre alle aziende un notevole aumento della loro capacità di sorveglianza sul consumatore. Di seguito effettueremo un'escursione sulle tecnologie maggiormente utilizzate, prima però è bene effettuare una contestualizzazione del problema.
Le tecnologie che vengono utilizzate sono globali, agiscono nell'identica maniera in ogni parte del pianeta e su tutti i pc. In quest'ottica appare centrale evidenziare il fatto che i dati che vengono raccolti dalle aziende non possono tener conto delle

legislazioni nazionali in maniera di privacy: i dati vengono raccolti da un pc e poi vengono trasferiti in un server che può essere situato dall'altra parte del mondo. Il problema, come nota Cammarata, è stato evidenziato anche in sede europea dai vari Garanti della Privacy e si è arrivati all'emanazione di un documento di lavoro[23] che concerne la Direttiva sulla Privacy (n. 95/46/CE), che prevede per tutti gli Stati non appartenenti all'Unione, di sottostare alla legislazione che viene applicata nella stessa nel momento in cui il computer su cui vengono raccolti i dati si trovi situato in un paese membro. Il documento, proprio per far fronte alle continue violazioni della privacy effettuate da spyware e simili, invitava tutte le aziende di software a specificare in maniera chiara in quale misura i dati venivano raccolti, le modalità attraverso cui farlo, i fini del trattamento ed infine richiedevano l'esplicito assenso alla trattazione degli stessi. Al tempo stesso proponeva lo sviluppo di particolari applicativi tecnologici per far fronte al problema (Cammarata, 2002).
A tutt'oggi noi possiamo vedere come le indicazioni fornite e la stessa Direttiva vengano costantemente ignorate o abilmente aggirate dalle aziende produttrici di software. Appare pertanto evidente come le legislazioni nazionali siano impotenti a fronteggiare il problema, e come le aziende stesse accrescano il loro potere di conoscenza sugli individui in maniera esponenziale all'utilizzo delle nuove tecnologie.
Fra quelle che di seguito vengono presentate possiamo vedere come l'indirizzo IP, *i GUID*, i *cookie* e gli *adware*, si configurino come *tecnologie d'identificazione* in quanto permettono l'autenticazione dell'utente. Gli s*pyware* come *tecnologie di sorveglianza* in quanto monitorano costantemente l'attività dell'utente, mentre i *player* e i sistemi di messaggistica istantanea vadano a con-fondersi fra i due tipi di tecnologia. Infatti esse permettono da un lato l'identificazione univoca di un utente permettendogli di avere accesso a determinati servizi e dall'altro, mantenendo le informazioni relative all'attività dell'utente, sorvegliano costantemente la sua attività. È da sottolineare come tutte queste tecnologie possano poi essere utilizzate dalle *tecnologie d'indagine*, in quanto ogni informazione generata viene racchiusa in appositi database.

5.2.1 Indirizzo IP

L'indirizzo IP non è altro che una combinazione numerica univoca, composta di 4 cifre separate da un punto (Es. 95.216.45.2), che ci viene assegnato automaticamente dal provider per distinguerci ogni volta che ci colleghiamo a Internet, e a cui per facilitare le cose viene associato un proprio nome alfabetico detto *domain name* o nome di dominio. Sarà poi compito di un server apposito detto *Domain name system*, provvedere a tradurre l'indirizzo IP alfabetico nel relativo indirizzo IP numerico.
In pratica ogni volta che ci colleghiamo ad una rete attraverso il pc l'indirizzo permette ai server di identificarci in maniera chiara ed univoca. È il nostro segno di riconoscimento nella rete. È attraverso questo che è possibile risalire all'identità di un individuo ed è esso che consente alle aziende di tracciare i nostri movimenti.

5.2.2 GUID,Globally Unique Identifier

Il *GUID* è un ID univoco globale, un codice a 16 byte, formato attraverso un complesso algoritmo, che identifica un'interfaccia di un oggetto su tutti i computer e le reti. Viene utilizzato per contraddistinguere una determinata installazione di un prodotto ed è presente in molti software comuni, i browser web e i lettori multimediali.
La funzione dei *GUID* è quella di permettere alle aziende di poter riconoscere il loro prodotto una volta che si è connessi alla rete. Se per caso vogliamo accedere attraverso un *player* multimediale ad un contenuto protetto, i " *GUID* del *player* vengono attivati per motivi di gestione del contenuto, autenticazione e invio di relazioni sull'accesso ai contenuti e sui dati sull'utilizzo ai content provider e ai detentori legittimi del copyright"[24].
I *GUID* però vengono anche comunemente usati per identificare ogni documento generato da un particolare software. Ogni volta noi utilizziamo programmi, quali gli applicativi *Office*, ad ogni nostro documento viene assegnato un codice che contiene la data e l'ora della creazione del documento e il codice identificativo del pc che lo ha generato. Per vedere questo basta andare in una cartella dove teniamo i nostri documenti e visualizzare i file "nascosti" e potremmo notare come ad ogni nostro documento salvato ne corrisponda un altro contenente le informazioni di cui sopra. Le aziende, utilizzano questa procedura per ottenere particolari informazioni sull'utilizzo che un utente fa dei loro prodotti. Basta andare sul sito della Microsoft, di Real Network o della Logitech dedicato alla privacy e possiamo leggere che i dati raccolti servono per: "valutare le prestazioni di un prodotto, migliorare la comprensione dei contenuti preferiti dagli utenti e le modalità di utilizzo dei prodotti, nonché per eseguire sondaggi tra i clienti. L'azienda può combinare i dati contrassegnati da GUID con altre informazioni personali fornite dagli utenti"[25].
In pratica le aziende di software utilizzano i GUID per monitorare l'uso che facciamo del nostro pc in generale. Tendono tutte a sottolineare come i dati che vengono forniti a terze parti non contengono le nostre informazioni personali in quanto vengono aggregati e combinati in statistiche. In parole povere le aziende in questione creano dei profili su di noi, riguardo all'utilizzo del pc, ma non cedono questi profili ad altri.
I problemi relativi alla privacy si fanno presenti in quanto di questo processo l'utente sa praticamente niente e avviene del tutto in maniera routinizzata. La preoccupazione su questi sistemi viene maggiormente avvertita se la compariamo con lo sviluppo di marcatori funzionanti con i metadati. Il pericolo è che i *GUID* migliorino significativamente la loro capacità di monitorare l'attività dell'utente fino a comprendere nel loro codice anche informazioni sui contenuti dei nostri documenti.

5.2.3 Spyware

Lo *spyware* è un programma che viene inserito in un computer con l'intento esplicito di raccogliere informazioni personali riguardo l'utilizzo del computer da parte di un utente. I programmi in questione vengono definiti come "spie" perché vengono inseriti all'interno del computer dell'utente a sua insaputa, o senza che ad esso ne sia stata data una particolare informazione al riguardo. In alcuni casi i programmi in

questione vengono inseriti in software più grandi, quasi sempre versioni *free*, e l'utente li installa insieme alla normale procedura d'installazione del programma stesso. Programmi come *Divx Pro* alla loro installazione inseriscono *spyware* come il famigerato *gain trickler*. A differenza dei GUID che servono ad identificare un documento o un programma, e permettono alla azienda di "riconoscerci", gli *spyware* vanno alla ricerca d'informazioni dell'utente e una volta che ci si collega alla Rete, in maniera automatica utilizzando la loro porta d'accesso, inviano le informazioni sull'utente al loro server di riferimento. Questo tipo d'applicazione è molto sviluppata per tutti quei programmi che vengono forniti gratuitamente nella rete. Sistemi di scambio peer-to-peer come *Godzilla* o *Kazaa* inseriscono al loro interno gli spyware in maniera tale da riuscire a sapere quali sono i file che l'utente ha scaricato o condiviso con altri utenti.
In pratica le aziende che forniscono gratuitamente i programmi nella rete tendono a sviluppare questi applicativi in maniera tale da rivendere i dati in questione ad altre aziende e così riuscire a guadagnare anch'esse. Bisogna però ricordare che i programmi che vengono forniti con licenze OpenSource non sviluppano applicativi *spyware*.

5.2.4 Adware

Gli *adware* come gli *spyware* sono anch'essi dei software, ma una differenza fondamentale con quest'ultimi sta nella funzione. Come per gli *spyware* anch'essi vengono forniti con programmi freeware o shareware, tuttavia, almeno a detta dei produttori, essi non raccolgono informazioni sull'utilizzo che un utente fa del proprio computer.
I programmi in questione si collegano in maniera diretta ad un server di riferimento e permettono a quest'ultimo di inviare banner pubblicitari sul nostro computer nel momento in cui utilizziamo un programma. In parole povere il software viene fornito gratuitamente purchè l'utente accetti di ricevere della pubblicità in cambio. È una tecnologia invasiva, ma appare essere totalmente innocua e, soprattutto, richiede un consenso esplicito dell'utente in quanto esso accetta le condizioni d'utilizzo del software in questione.

5.2.5 Cookie

Un *cookie*, in inglese "biscotto", è una stringa di testo inclusa nelle richieste e risposte del protocollo *HTTP* (*Hypertext Transfer Protocol*). I *cookie* vengono utilizzati per mantenere informazioni relative allo stato di un utente durante il passaggio tra le diverse pagine di un sito Web o quando si torna a visitare un sito Web in un secondo tempo. Vengono sviluppati essenzialmente per far risparmiare tempo all'utente in quanto le informazioni necessarie al caricamento di una pagina vengono inserite al loro interno. Possono essere presenti informazioni come l'*User ID* di un utente e la sua password d'accesso per far si che lo stesso non debba di volta in volta ridigitarle.
I *cookie* vengono inseriti nel nostro computer dai siti in cui andiamo a navigare, ogni sito ne inserisce uno sul nostro pc in maniera tale da riuscire a riconoscerci ogni

volta che navighiamo al suo interno. La possibilità offerta dal *cookie* per le aziende è notevole, infatti riconoscendoci attraverso il nostro *indirizzo IP* i *cookie* permettono alle aziende di mandarci informazioni pubblicitarie mirate. Aziende come *DoubleClick* non fanno altro che inserire milioni di *cookie* nei computer degli utenti avvalendosi delle centinaia di siti a cui è consociata. In questa maniera può analizzare tutti i siti che sono stati visualizzati da un singolo utente, fare un profilo delle sue preferenze, e poi permettere alle aziende di mandare una pubblicità mirata grazie al profilo ottenuto (Castells,2001).

5.2.6 Instant messenger e VoIP

Gli *instant messenger* sono tutti quei programmi che permettono la comunicazione diretta, in tempo reale, fra due o più utenti connessi nello stesso momento alla rete. Il funzionamento è lo stesso che avviene in una chat soltanto che la comunicazione non avviene sfruttando un sito terzo, ma una connessione diretta con l'altro utente. Stesso discorso per i *VoIP* (*Voice Over IP*) che però non solo permettono lo scambio di messaggistica in tempo reale, come gli instant messenger, ma sono in grado di far scambiare la voce. I programmi quali *Skipe* permettono in pratica telefonate gratuite da pc a pc e a pagamento fra il pc ed un telefono normale.

Le aziende che sviluppano tali applicativi mantengono in database tutte le comunicazioni che avvengono fra gli utenti, in maniera tale da potersi tutelare contro possibili usi impropri della rete. Come abbiamo precedentemente notato, è proprio grazie a questa raccolta di informazioni che *Aol* è stata in grado di far arrestare i due pirati informatici che avevano violato i propri database. Le aziende in questione garantiscono la privacy degli utenti non cedendo a terze parti i dati raccolti.

Tuttavia nel momento in cui scriviamo la libertà offerta dal servizio sembra venir minacciata in quanto il Ministro della Giustizia americano John Ashcroft ha recentemente inviato una lettera a Michael Powell, Presidente della *FCC* (*Federal Communication Commission*) che invita la Federazione ad emanare un provvedimento per permettere all'FBI di avere una porta d'accesso remota a tutti i server delle aziende che forniscono questi servizi, in maniera tale da riuscire a monitorare il traffico in rete generato da questi software[26]. La convergenza nel settore della sicurezza fra aziende e Stato potrebbe avere conseguenze veramente inaspettate per la privacy dei navigatori.

5.2.7 Player

I *player* sono tutti quei programmi che ci permettono di leggere una serie di file audio e video. Uno degli aspetti da rilevare è che in moltissimi casi essi vanno a configurarsi come dei veri e propri *spyware* (Cammarata, 2004). Meritano una trattazione a parte in quanto tendono ad usare una serie di tecnologie di cui abbiamo parlato sopra.

Basta collegarsi al sito della *Microsoft* che tratta del lettore multimediale[27] per sapere che una volta collegati ad Internet nel nostro pc vengono inseriti dei *cookie* per sapere a quali contenuti abbiamo accesso. Ogni lettore è contrassegnato da un *GUID* che permette all'azienda di riconoscerlo. È la stessa Microsoft a dirci che:

> Quando si riproduce o si copia un CD audio, Windows Media Player tenta di individuare le informazioni associate al CD, quali il nome dell'artista, il titolo e i titoli dei brani. Queste informazioni vengono aggiunte all'elenco generale delle informazioni memorizzato nel Catalogo multimediale. Per ottenere queste informazioni, viene inviato a WindowsMedia.com un ID univoco del CD. Durante questa transazione non vengono ottenute né memorizzate informazioni di carattere personale. Il Catalogo multimediale contiene una raccolta di file audio e video e i relativi collegamenti. A queste informazioni possono accedere altre applicazioni software disponibili nel computer o su Internet.

E inoltre:

> Microsoft ha collaborato con alcuni partner commerciali, quali case discografiche, produttori di PC palmari, case di produzione video e molti altri, per sviluppare un servizio che consenta, per soli fini leciti, operazioni di spostamento e ripristino di licenze multimediali tra i computer dell'utente, ma non tra computer di utenti diversi. Questo servizio consente un numero limitato di transazioni di licenze. Quando vengono ripristinate le licenze, vengono inviate a Microsoft le informazioni necessarie per identificare in modo univoco il computer per scopi di verifica interna. Le informazioni relative all'identificativo univoco dell'utente vengono memorizzate in un database e viene tenuta traccia del numero di tentativi effettuati per ripristinare le licenze. Microsoft non condivide tali informazioni con terze parti, interne o esterne a Microsoft.

Il discorso effettuato dalla *Microsoft* in un punto sembra entrare in contraddizione con se stesso. Ci dicono che vengono inviate informazioni relative ai nostri file, ma che esse non sono di carattere personale, quando appare evidente che trattandosi della musica o dei video da noi visti lo sono eccome.
Quello che comunque questa lettura ci palesa è che *Microsoft*, ma il discorso vale anche per tutte le altre grandi aziende, mantiene i dati relativi al nostro lettore in un proprio database. Il nostro lettore è identificato in maniera univoca e pertanto essi possono sapere l'identità della persona che lo possiede. In questo modo la *Miscrosoft* può creare dei profili riguardo all'utente che contengano tutte le preferenze musicali dello stesso. In pratica i *player* musicali consentono una sistematica raccolta dati individuali e la creazioni di profili sempre più accurati dal punto di vista culturale.

5.3 Tu lavori io guardo

Per le aziende monitorare l'attività lavorativa dei dipendenti diventa fondamentale perché un utilizzo errato della Rete può comportare danni economici rilevanti (Strano, 2000). Inoltre l'accento posto sulla delocalizzazione delle fabbriche porta all'accrescimento della creazione di sistemi informatici che permettano un controllo a distanza dell'attività produttiva (Ball, 2003; Castells, 2001; Lyon, 1994; 2001). Lo sviluppo di applicazioni che permettano di svolgere queste attività pertanto deve essere inserito nelle normali pratiche gestionali di un'azienda.
In questo settore più che in altri può essere notata la flessibilità delle tecnologie, infatti la maggior parte di essa viene da principio installata per uno scopo e successivamente permette anche di monitorare l'attività lavorativa dei dipendenti (Lyon, 2001). Gli strumenti di pianificazione vengono installati per gestire la produzione e naturalmente si prestano anche al controllo dell'attività lavorativa del dipendente. Stesso discorso per gli strumenti per la gestione degli accessi.

In campo informatico strumenti quali *Gatekeepe*r, letteralmente guardiano di porte, vengono installati inizialmente per preservare le reti informatiche aziendali da attacchi provenienti dall'esterno come virus o hacker, e poi vengono applicati per controllare un utilizzo improprio della rete da parte dei dipendenti. In questo settore è da notare come però l'accento venga sempre maggiormente spostato verso il puro e semplice monitoraggio dei dipendenti per prevenire il "furto di tempo macchina".
In un recente studio[28] commissionato dalla *Hitachi Data Systems* alla *Storage Index* per verificare l'ampiezza del fenomeno viene mostrato come la pratica di monitorare i dipendenti sia quasi sistematica. Dallo studio salta fuori come le aziende interpellate, dislocate in Europa, Africa e Medio Oriente, nel 56 per cento dei casi controllino la posta elettronica dei dipendenti; nel 61 per cento la archivino centralmente; nel 36 per cento monitorino le comunicazioni che avvengono attraverso i sistemi di messaggistica istantanea; nel 68 per cento dei casi i dipendenti sono sottoposti ad una *policy* rigida di utilizzo delle reti informatiche.
Il fenomeno è in rapida ascesa e soltanto adesso i governi stanno attuando interventi legislativi adeguati. Molte sono le aziende che comunicano ai dipendenti di controllare la loro attività, ma altrettanto tante sono quelle che non usano criteri di trasparenza.
A questo va aggiunto che moltissime aziende possono giustificare l'adozione di sistemi di videosorveglianza in funzione della loro attività: banche ed esercizi commerciali essendo attività a rischio possono adottare tali dispositivi per tutelarsi rispetto al crimine. Per altri luoghi di lavoro quali fabbriche la legislazione italiana vieta il loro utilizzo, ma in altre aree del mondo mancano legislazioni adeguate al riguardo. Il funzionamento di tali sistemi verrà spiegato nel capitolo successivo.
Per quello che riguarda le tecnologie che di seguito descriviamo possiamo vedere come i *gatekeeper* e i controlli gestionali si configurino come *tecnologie di sorveglianza*, i sistemi per il controllo accessi come *tecnologie d'identificazione*, che poi in seguito diventano di sorveglianza.

5.3.1 Guardiani di porte

I gatekeeper forniscono alle aziende sia una prevenzione contro attacchi esterni sia la possibilità di monitorare il traffico Internet del dipendente, la sua posta elettronica o anche solo l'utilizzo di giochi sul computer. Le possibilità offerte variano da software a software.
Gatekeeper riesce a mostrare tutto il traffico Internet che passa nella rete, stabilendo con precisione chi sta utilizzando Internet e quali siti sta visitando. Con *F-Secure Internet Gatekeeper*, l'amministratore può controllare il contenuto che è scaricato dal web oppure inviato o ricevuto via e-mail, bloccare filmati, file audio o altri file dal contenuto estraneo all'attività lavorativa per tipo di file o dimensione e proibire agli impiegati di accedere a siti web non appropriati. *Netreplay* è un applicativo "cattura contenuti". Lanciato dall'inglese *Chronicle Solutions*, *Netreplay* monitora, allerta, registra, ricerca, archivia e ripropone tutto quello che viene visto o ascoltato su pc. E' un *Grande Fratello* in versione aziendale, in grado di registrare email, messaggi, file trasferiti, fino a replicare esattamente tutte le pagine web visitate dal lavoratore. Il

sistema è addirittura in grado di lanciare allarmi in real time di fronte a potenziali abusi.
I software permettono sia soltanto il controllo del traffico sia un vero e proprio "spionaggio" dei contenuti delle mail. Infatti molti applicativi vengono sviluppati solo per controllare gli indirizzi a cui le mail sono spedite, mentre altri come *Netreplay* o *xVMail,* basandosi su parole chiave riescono a fare una vera e propria scansione del testo.
Molti software inoltre sono sviluppati per controllare la quantità del lavoro svolto dal dipendente. *SuperScout,*della *SurfControl*, ad esempio, può generare classifiche delle 10 persone che spediscono più mail, di quelli che ne ricevono di più, il loro peso in Kb e il loro titolo.
L'utilizzo di quelli che vengono comunemente denominati come "programmi spia" permette alle aziende sia di controllare che i dipendenti non effettuino operazioni improprie attraverso la rete, come guardare siti pornografici, scaricare musica illegalmente o mandare mail personali, sia quantificare il carico di lavoro svolto da ciascun dipendente.

5.3.2 Rilevazione e gestione delle presenze e controllo del personale
La maggioranza delle aziende per controllare le entrate e le uscite che avvengono all'interno delle proprie sedi si avvale di strumenti per gestire gli accessi. In questo modo si può evitare che personale non addetto possa entrare all'interno delle proprie strutture, e si può suddividere l'accesso dei dipendenti in determinate aree in base alla loro competenza. Sono essenzialmente tecnologie che permettono l'esclusione da determinate aree e l'inclusione in altre. Nella stragrande maggioranza i sistemi vengono utilizzati attraverso *badge* d'accesso, anche se in molti casi, nelle aziende dove la sicurezza è maggiormente importante, gli accessi sono sviluppati con tecnologia biometrica come le impronte digitali o la scansione dell'iride.
I sistemi utilizzati possono essere diversi, ma la base di funzionamento è la stessa per tutti, di solito sono suddivisi in due parti[29]: rilevazione e gestione presenze del personale e controllo e gestione accessi.
Il primo modulo serve per gestire tutte quelle informazioni legate al personale che opera nell'azienda inclusi i collaboratori esterni o saltuari (imprese di pulizie, autisti, fattorini,ecc.). "Svolge in maniera semplice e concreta quelle attività spesso lunghe e non sempre precise dell'ufficio personale legate alla determinazione degli orari giornalieri del personale, alle loro autorizzazioni, al loro saldo ferie e permessi, alle compensazioni automatiche, alla gestione del cartellino dipendente, ecc."[30] In pratica attraverso il *badge* d'accesso il sistema è in grado di mostrare l'anagrafica di ciascun dipendente; calcolare i suoi orari di entrata, d'uscita, e la quantità delle pause effettuate; calcolare l'insieme delle presenze/assenze di ciascun dipendente e del totale dei dipendenti; calcolare automaticamente i compensi di ciascun dipendente in base ai dati raccolti; stilare statistiche giornaliere, settimanali e mensili sull'attività lavorativa di ciascun dipendente, di ciascuna categoria lavorativa e dell'insieme dei dipendenti.

Il secondo modulo che si occupa del controllo e della gestione degli accessi permette ai terminali di controllare e verificare le autorizzazioni. Rappresenta, in sintesi, un semaforo "intelligente", che in relazione alla configurazione che riceve dal Personal Computer a cui è collegato, permette di abilitare al passaggio di determinate soglie (porte, tornelli, cancelli, sbarre, ecc.). Le funzioni di controllo accessi vengono svolte compiutamente dal sistema che permette, inoltre, di centralizzare, raccogliere, monitorare, impostare e configurare liberamente una serie di parametri e dati legati al transito del personale. In questa maniera il sistema attraverso l'associazione del codice matricola del dipendente al terminale di controllo permette l'accesso a determinate aree solo ai dipendenti autorizzati e calcola il tempo di permanenza di ciascun dipendente per ciascuna area di transito.
I sistemi di gestione delle presenze e degli accessi riescono a rendere la gestione del personale completamente automatizzata e si prestano ad essere degli ottimi strumenti per monitorare l'attività lavorativa dei dipendenti.

5.3.3 Pianificazione della produzione e controllo di qualità

Come si è osservato precedentemente, la produzione aziendale è sempre maggiormente automatizzata lasciando all'operaio poco o nullo margine per controllarla. Al tempo stesso nelle attuali pratiche aziendali diviene centrale il controllo di qualità del prodotto, dato il maggior peso che ha il cliente. Le aziende pertanto, anche in funzione del controllo a distanza, si avvalgono di sistemi informatici che garantiscano un monitoraggio costante e continuo della produzione, in maniera tale da poter reagire tempestivamente ad ogni imprevisto e per snellire significativamente la produzione stessa.
I sistemi utilizzati sono di due tipi[31]: uno per pianificare la produzione ed uno per controllarne la qualità.
Nel primo caso i sistemi di pianificazione permettono alle aziende di gestire in maniera automatizzata tutta la filiera produttiva. Vengono di solito anch'essi suddivisi in due moduli.
Il primo pianifica e suddivide la produzione in tanti frammenti: calcola gli ordini ricevuti, l'approviggionamento dei materiali, le consegne più urgenti, la potenzialità del reparto, i costi di produzione, i tempi improduttivi, e suddivide il carico delle macchine e degli operai. In pratica il software attraverso un algoritmo complesso valuta tutte le combinazioni possibili e sceglie quella più adatta in quel momento per l'azienda.
Il secondo modulo invece permette il controllo, il monitoraggio e la gestione della produzione. È formato da una serie di terminali dislocati nella fabbrica, connessi in rete fra loro, e collegati ad uno o più pc di supervisione. In questo modo i dati sulla produzione vengono trasmessi in tempo reale al pc di controllo che può rilevare i tempi di produzione, l'avanzamento dei lotti, le quantità prodotte, gli scarti, le inefficienze, i fermi di produzione, ed evidenziare eventuali anomalie. Attraverso questi sistemi le aziende sono in grado di gestire in maniera automatica tutta la catena di produzione, le commissioni ricevute, e le spedizioni. In questo contesto i sistemi riescono a supervisionare il lavoro dell'operaio perché permettono di

effettuare analisi precise riguardo il carico di lavoro svolto da ciascuno e forniscono tempestivamente informazioni riguardo eventuali inefficienze o mancanze degli stessi.
Il sistema di gestione e del controllo della qualità invece viene utilizzato dalle aziende per constatare la qualità delle materie utilizzate, gestire la taratura e l'efficienza delle macchine, garantire la conformità e la rintracciabilità dei prodotti. Anche in questo caso il sistema è sviluppato attraverso il posizionamento in fabbrica di diversi terminali collegati in rete come il sistema di cui sopra. Grazie alle potenzialità offerte le aziende sono in grado di poter risalire all'origine di ogni falla o anomalia dei prodotti, sapere se la stessa è dovuta ad un difetto del materiale di produzione, ad una negligenza o sbaglio di un operaio, ad una inadempienza di un fornitore o di un trasportatore.
L'automatizzazione della produzione comporta pertanto un controllo minimo dell'operaio sulla stessa, ma, è bene evidenziare, questo non implica una minore responsabilità per il dipendente. Infatti, come sottolinea Lyon, i controlli di qualità tendono a far diventare l'operaio stesso come responsabile della parte di produzione a lui assegnata. In questa maniera i sistemi automatizzati comportano un assoggettamento maggiore dell'operaio alla disciplina di fabbrica in quanto sa di essere costantemente monitorato in ogni sua attività allo stesso modo in cui è monitorata ogni attività di produzione (Lyon,1994).

6. LA SORVEGLIANZA UBIQUA

Ci siamo accorti che le nuove tecnologie rendono possibile un controllo dentro le nostre case, e queste hanno sempre rappresentano la soglia che delimitava il pubblico dal privato. E proprio nei luoghi pubblici possiamo assistere all'impiego massiccio di tecnologie per monitorare quotidianamente le nostre esistenze.
Le città sembrano diventare spazi di classificazione, come li definisce Lyon, ed è proprio in esse che vengono maggiormente esercitate forme di sorveglianza continua. Non che questa non sia presente nelle piccole comunità, ma semplicemente in esse ancora viene svolta attraverso quel controllo di tipo informale che abbiamo incontrato nel primo capitolo. Nelle città invece sono i diversi centri di potere, statali ed aziendali, ad utilizzare dispositivi tecnologici per perseguire i propri obiettivi. Il controllo della popolazione ha bisogno per esercitarsi di spazi di visibilità, di zone d'esclusione e zone d'inclusione, di varchi d'accesso e di separazione. In una città i luoghi da controllare sono molteplici.
Bisogna poter analizzare i flussi di traffico, sapere quante macchine passano in una determinata via in ogni ora della giornata in maniera tale da poter gestire la loro affluenza e smistarle nelle diverse direzioni. Il semaforo non è altro che una tecnologia che permette, attraverso la gestione dell'accesso, di controllare l'afflusso del traffico. Bisogna sapere quante persone prendono il servizio pubblico e le ore di punta per poter pianificare la quantità di veicoli da utilizzare ad ogni orario. Il concetto di prevenzione va ad applicarsi in ogni angolo delle città perché è necessario prevedere gli incidenti. Garantire ordine. Sapere con precisione dove potrebbero verificarsi disordini, che possono spaziare dall'essere un semplice

incidente stradale o dall'essere una sommossa popolare, e pianificare tattiche di reazione adeguate. Dividere i compiti e le aree di competenza fra le varie agenzie e per ognuna di esse fornire una serie di strumenti per reagire all'evento.
Fra gli strumenti in questione ci sono una serie di dispositivi tecnologici che permettono a queste agenzie di prestare al meglio, massimizzare, i propri compiti.
L'apparato poliziesco ha la necessità di sapere in una città in quali aree si possano verificare determinati incidenti. Deve poter vedere ovunque. La pianificazione urbana include anche questi obiettivi. Nell'esempio di Brasilia abbiamo potuto notare come l'afflusso della popolazione potesse essere smistato, attraverso l'architettura, verso una area comune che permetteva la piena visibilità. Le zone invisibili, quelle dove non è possibile vedere, devono essere interdette, sbarrate. Si possono utilizzare sistemi di videosorveglianza in determinate aree, o impedire l'accesso in altre, come nel caso della City londinese, oppure utilizzare il pattugliamento in altre ancora.
Le aziende di trasporti suddividono la città in tante aree in funzione della diversa affluenza delle persone a queste, così come fanno le imprese commerciali in funzione dei loro interessi. Esse infatti in base alla raccolta dei dati effettuati possono sapere in ogni zona quali classi socioeconomiche vi fanno spesa e posizionare così le loro sedi. Le imprese immobiliari possono sapere quale tipo di lavoratori possano abitare in determinate aree e strutturare così la costruzione delle palazzine. Stesso discorso per le varie amministrazioni in sede di approvazione dei piani regolatori.
In qualsiasi ottica noi la vogliamo vedere, sotto qualsiasi aspetto, dobbiamo prima constatare che tutti gli spazi urbani sono classificati. Divisi in aree. Le nuove tecnologie sono al servizio delle diverse agenzie nel processo di classificazione, andando a rafforzarlo significativamente. E permettendo un monitoraggio continuo ed ininterrotto delle nostre esistenze.

6.1 Videosorveglianza

Negli ultimi anni abbiamo assistito ad un incremento spaventoso dei sistemi a circuito chiuso (*CCTV*). Basta camminare un po' nelle nostre strade e li possiamo vedere agli angoli delle strade, sotto i portoni, nelle stazioni della metro e dei treni, negli aeroporti, nelle università e nelle scuole, agli incroci dei semafori, lungo i varchi elettronici, sulle autostrade. Come spiega un'indagine effettuata per conto del Garante per la protezione dei dati personali[32], i sistemi CCTV vengono classificati in base ai loro utilizzi in:

- sistemi di rilevazione e controllo dei flussi di traffico;
- sistemi di rilevazione delle infrazioni al codice della strada;
- sistemi di vigilanza nel pubblico trasporto;
- sistemi di controllo dei perimetri e degli spazi di stabilimenti ed edifici pubblici da sottoporre a particolare tutela;
- aree a grande presenza di pubblico quali le stazioni, le aree aeroportuali e portuali, i grandi magazzini e centri commerciali, centri direzionali;
- filiali bancarie, sportelli automatici, farmacie e rivendite di merci di valore;
- stazioni di rifornimento;
- parcheggi e aree pubbliche ove si sono riscontrati frequenti episodi malavitosi.

Da qualunque agenzia vengano utilizzate, pubblica o privata, il loro scopo è monitorare una particolare area. Così gli organi di polizia utilizzeranno tali sistemi con lo scopo di prevenire il crimine, come abbiamo già osservato, e così le banche e i centri commerciali. In quest'ultime la flessibilità tecnologica permessa da questi sistemi li fa anche diventare però strumenti in grado di monitorare l'attività dei dipendenti (Lyon, 1994, 2001). Nelle imprese possono essere impiegati per controllare a distanza la produzione, e naturalmente l'operaio, andando fino ad essere inserite dentro i bagni[33] per fare in modo che i dipendenti non facciano uso di sostanze stupefacenti (Ball,2003; Lyon,2001). Le aziende di trasporti possono utilizzare sistemi di videosorveglianza a distanza per prevenire incidenti o prestare soccorsi tempestivi lungo le arterie di comunicazione.
Il funzionamento di tali sistemi, qualunque ne sia l'applicazione, è però sempre lo stesso. L'area da sorvegliare viene suddivisa in tante parti in base al raggio d'azione delle telecamere, al loro grado di fuoco, ed in ogni parte viene inserita una o più telecamere in maniera tale da evitare i "coni d'ombra", ossia delle zone di non visibilità dove le telecamere, anche muovendosi, non riescono ad arrivare. Le immagini che le diverse telecamere catturano confluiscono in un centro di controllo che ha a disposizione uno o più monitor per visualizzarle tutte. La trasmissione delle stesse avviene utilizzando sistemi via cavo o via radio. Attraverso questo sistema l'area viene costantemente monitorata. Le telecamere infatti sono così tecnologicamente avanzate da essere in grado di vedere anche in condizioni di scarsa visibilità.
Sempre dal Dossier del Garante riportiamo gli scopi per cui vengono vendute le telecamere e la loro capacità tecnologica:

> "Tipi di sorveglianza: perimetrale o ambientale con telecamere; consenso per l'accesso tramite riconoscimento biometrico-facciale; esclusivamente con telecamere senza tessere magnetiche o codici personali" (ciò vuol dire che le telecamere contengono rilevatori a tecnologia digitale e possono quindi operare operazioni di confronto con immagini di volti preregistrati in un archivio centrale, i volti delle persone abilitate ad accedere all'area protetta); "controllo permessi per parcheggi con riconoscimento targhe;" e ancora: "telesorveglianza del traffico veicolare; di punti del territorio comunale quali piazze, monumenti, palazzi; di sovrappassi stradali, contro atti vandalici all'arredo urbano e per la prevenzione degli stessi; per accessi alle zone a traffico limitato o parcheggi con riconoscimento targhe;" e ancora (e più invasivo perché non in postazione fissa e quindi individuabile): "novità - é inoltre disponibile un sistema portatile leggero e compatto racchiuso in un contenitore facilmente trasportabile e a tenuta stagna, in cui sono racchiusi una telecamera con sistema di intercettazione di movimenti (Motion detector), sistema di registrazione immagini, batterie per una lunga autonomia e illuminatore notturno ad infrarossi (per vedere ma non essere visti)". (*I virgolettati sono presenti nel testo in quanto parti di un annuncio di una azienda che vende tali sistemi*)

Gli impieghi e le capacità come si può vedere sono molteplici e variano a seconda della loro applicazione e, soprattutto, in base al collegamento o meno con altri strumenti. In molti casi infatti le telecamere sono associate a particolari software che permettono di effettuare determinati tipi di analisi.
Anche in questo caso infatti il concetto basilare è quello di prevenire particolari incidenti, e i sistemi a circuito chiuso, integrati agli strumenti informatici,

permettono a questi ultimi di effettuare simulazioni, calcolare probabilità, o semplicemente segnalare anomalie: le immagini vengono catturate, comparate con altri dati, e portano alla predizione dell'evento (classificazione, comparazione, predizione) (Graham, Wood, 2003).
Nelle stazioni metropolitane inglesi viene utilizzato un sistema di rilevazione e controllo dei flussi denominato *Cromatica* (Froomklin, 2000; Lyon, 2001), in via di sperimentazione anche in Italia (Mazoyer, 2001). Il sistema permette di monitorare il grado di affollamento della metropolitana, e allerta in caso di anomalie, come un sovraffollamento od un comportamento non idoneo. Sono i colori dello schermo a cambiare d'intensità, da qui il nome, quando avviene una anomalia, come quando qualcuno si trattiene troppo a lungo sui binari o va in luoghi dove l'accesso non è consentito. Il sistema dovrebbe essere in grado anche di prevenire i potenziali suicidi, calcolando che questi tendono a perdere una o più metro prima di compiere l'estremo gesto (Lyon,2001).
Sistemi quali il *PNC* britannico o l'*N-System* giapponese servono alle polizie per monitorare il flusso del traffico, vedere chi commette infrazioni, ma, soprattutto, per individuare possibili veicoli rubati. Entrambi i sistemi sono stati installati secondo la *strategia dell'emergenza:* in Inghilterra in seguito agli attentati dell'IRA (Lyon,2001), mentre in Giappone per combattere contro l'organizzazione criminale Aum Shinrikyo (Abe, 2004). Il loro funzionamento avviene comparando le targhe dei veicoli, catturate dalle telecamere, che transitano lungo le strade, con quelle dei veicoli che risultano essere rubati che sono inseriti nei loro database (Abe, 2004; Lyon, 2001).
Per rispondere a particolari esigenze si sono anche creati i sistemi di riconoscimento facciale. Essi permettono in pratica di riconoscere un individuo in base alle caratteristiche biometriche del suo volto. Vengono utilizzati da particolari imprese come banche o aziende ad elevata sicurezza come *badge* d'accesso a determinate aree (una delle tecnologie che utilizza il corpo come password). Mentre dagli apparati di polizia questi sistemi vengono utilizzati per identificare le persone che transitano, o che sono transitate, in determinati luoghi. Negli aeroporti o nelle stazioni per verificare che non vi siano possibili terroristi, negli stadi per individuare i colpevoli di atti vandalistici e così via. Per spiegare il loro funzionamento prendiamo parte di un'intervista[34] che Punto Informatico ha effettuato a Davide Lombardi direttore del gruppo Sisge che è leader in Italia nello sviluppo delle tecnologie biometriche.

> *Punto Informatico: Sul piano tecnico, come funziona un apparato di riconoscimento facciale, quali sono i suoi componenti?*
> Davide Lombradi: I parametri biometrici, acquisiti attraverso una videocamera o altri device di riconoscimento, vengono estratti secondo un modello matematico e conservati in una stringa di dati (repository) da raffrontare con quelli del soggetto presente al momento dell'autenticazione. Il procedimento, nel dettaglio, si compone di due fasi: nella prima il volto della persona viene isolato all'interno dell'immagine e reso leggibile, nella seconda viene estratta un'impronta contenente i tratti distintivi di quel volto come distanza tra gli occhi e il naso, tipologia delle labbra, taglio degli occhi ecc. Dall'analisi di questi pattern si ottiene il faceprint, cioè un modello matematico (Local Feature Analisys) che compone una sagoma univoca del soggetto

riproducendo i processi di riconoscimento delle persone realizzati dal cervello umano. Basandosi sull'analisi di ben 40 elementi caratteristici del volto, detti anche punti nodali, il sistema può conservare un'elevata accuratezza anche in situazioni critiche, come scarsa illuminazione, differenti espressioni del viso, sfondi dinamici o complessi. Infine avviene il confronto tra i due insiemi di dati (Biometric Identifier Record). Il primo proveniente dalla device di riconoscimento, mentre il secondo è quello precedentemente codificato che viene prelevato dal database. Se viene rilevata una corrispondenza, un allarme lo segnala all'operatore.

P.I: E sul fronte dell'hardware?

DL: La scelta dell'hardware da impiegare dipende solo dalla mole di dati che si intende gestire. In una tipologia di identificazione uno a molti (partendo da un soggetto la cui identità originale è nota o ignota, si confronta il volto acquisito da telecamera o fotografia con un archivio preesistente) o sorveglianza molti a molti (partendo da un database di soggetti sospetti, il sistema effettua la sorveglianza automatica e continua di un ambiente attraverso telecamere, in cerca di un volto noto. Ciascuna sessione di ricerca prevede analisi dinamica del fotogramma, selezione di più volti, acquisizione e normalizzazione delle immagini grafiche, codifica dei volti) è preferibile impiegare hardware dedicato proprio per la mole di dati che dovranno essere gestiti.

P.I:Come viene costituito il database di "volti" che il sistema confronta poi con il "faceprint" che viene rilevato di volta in volta?

DL: Il popolamento del database di confronto può avvenire in vari modi, si va dalla scansione di una fotografia (foto segnaletica, oppure pubblicata su un giornale ecc.) o di un identikit, all'impiego di un fotogramma tratto da una videocamera, fino all'acquisizione diretta da parte del sistema attraverso un processo di enrolment (il sistema cattura il volto, ne estrae l'ID biometria e chiede all'operatore di confermarne l'identità).

Anche nell'adozione di tali sistemi possiamo vedere l'applicazione della *strategia dell'emergenza* in quanto sono stati implementati massicciamente dopo potenziali minacce. Il fenomeno hooligans per citare un esempio o la paura degli attentati dopo l'undici settembre che ha incrementato l'utilizzo dei sistemi di riconoscimento facciale nei principali aeroporti mondiali (Lyon, 2001b). Grazie all'utilizzo di tali sistemi le polizie possono individuare i colpevoli di alcuni reati, se le telecamere erano presenti, e altresì esse possono monitorare gran parte della popolazione urbana scovando fra esse possibili "sospetti". Quello che infatti deve essere evidenziato è che nel momento in cui ognuno di noi si trova in un luogo in cui vengono adottati sistemi basati sul riconoscimento facciale, la sua immagine verrà sottoposta a scansione e incrociata con tutte quelle contenute all'interno dei database.

L'incremento dell'utilizzo di sistemi di videosorveglianza non è comunque dovuto solo ad applicazioni di polizia, ma è dovuto in particolar modo alle imprese commerciali o a semplici privati che cercano di tutelarsi. Così nei supermercati vengono inserite le telecamere per prevenire ed individuare i furti, ma al tempo stesso esse monitorano sia il lavoratore e sia il consumatore abituale. In molti casi l'applicazione dei sistemi di videosorveglianza viene utilizzato per individuare particolari tipologie di individui che risultano essere non graditi ad un determinato luogo. Nei centri commerciali ad esempio il sistema serve per allontanare le bande giovanili da quell'area e spostare così in un altro luogo la possibile criminalità (Lyon, 1994), mentre nelle metropolitane è utilizzato per allontanare i barboni o coloro che chiedono l'elemosina (Mazoyer, 2001).

Uno degli aspetti da rilevare infatti è il fattore discriminate che i sistemi di videosorveglianza possono comportare. L'attuale costituzione delle città sembra basarsi sulla creazioni di aree d'accesso che includano i consumatori, ma fungano da deterrente ai "vagabondi", e di comunità isolate dal contesto sociale situate in fortezze iperprotette (Bauman, 1998, 2000). A Lione in Francia vengono utilizzati per fare in modo che gli homeless non entrino nel centro cittadino (Mazoyer, 2001), così come a Victoria negli U.S.A. (Lyon, 2001). Le tecnologie di videosorveglianza possono essere utilizzate per escludere da queste aree proprio quella frangia di popolazione più emarginata e così riversarla in altre zone, magari meno visibili come le periferie, e sottoporla poi ad un controllo di tipo diverso più rigido (Davis, 2004; Lyon, 2001).
I sistemi di videosorveglianza comportano un'erosione sistematica della privacy individuale e possono essere utilizzate per escludere o includere determinate tipologie di individui in alcune aree. Verificare sempre che chi si trovi in un luogo abbia le caratteristiche per restarci.

6.2 Dispositivi mobili

Per dispositivi mobili intendiamo tutti quegli strumenti tecnologici che quotidianamente portiamo con noi e che per il loro funzionamento non necessitano di una postazione fissa come il pc di casa. Proprio in essi viene evidenziata la flessibilità tecnologica dei sistemi di sorveglianza in quanto i diversi strumenti nati per uno scopo possono essere tranquillamente utilizzati per monitorare e raccogliere informazioni sul cittadino, sul consumatore e sul dipendente. Grazie anche ad essi noi possiamo vedere come la tecnologia non sia un male in sé, assolutamente, ma come l'utilizzo che viene fatto di essa, gli scopi per cui viene implementata, possono essere lesivi per la privacy individuale.

6.2.1 GPS

Il *GPS* (*Global Positioning System)* è un sistema che permette di sapere la posizione occupata nello spazio da un qualsiasi dispositivo ad esso collegato. È composto da 24 satelliti che orbitano attorno al pianeta, da sei centri di controllo situati nel globo e da una serie di antenne posizionate a terra. Le antenne a terra captano i segnali trasmessi dai diversi dispositivi mobili e li trasmettono ai satelliti, questi li ritrasmettono alle stazioni di monitoraggio che a loro volta li mandano ad una centrale situata a Falcon nel Colorado. Attraverso questo scambio di dati il sistema riesce a calcolare la longitudine, la latitudine e l'altezza in cui si trova uno dei dispositivi.
Le applicazioni di quest'ultimi sono molteplici. Le imprese marittime li utilizzano a bordo delle loro navi per sapere con precisione dove si trovano, le banche li utilizzano per trasportare i valori da una parte all'altra e così via. In tutti quei casi dove è necessario sapere con esattezza dove si trova un oggetto nello spazio vengono utilizzati sistemi *GPS*. Grande incremento agli stessi è stato fortemente dato dall'utilizzo civile di diverse applicazioni. Le case automobilistiche forniscono i *GPS* come strumenti per rintracciare la macchina in caso di furto, e come strumenti di

navigazione. Infatti caratteristica del *GPS* è quella di poter fornire all'utente l'esatta posizione in cui si trova. Aggiungendo a questo una mappa, l'automobilista può decidere quale percorsi effettuare, avere indicazioni, e così via. Essenzialmente possono essere inseriti in qualunque cosa, si pensi che l'*Applied Digital Solutions* ha recentemente sviluppato un sistema *GPS*[35] completo grande quanto uno stimolatore cardiaco da inserire a livello sottocutaneo. Potrebbe sembrare assurdo solo se consideriamo un determinato tipo di utilizzo del sistema. Infatti lo stesso sistema che serve per individuare navi, o camion, o fornirci indicazioni, cambiando categoria di indirizzo diventa un ottimo strumento di controllo.
Questo può essere utilizzato dai governi per superare il problema del sovraffollamento delle carceri. Molti stati stanno sviluppando infatti quella che Lyon definisce la soluzione "Uomo ragno": braccialetti elettronici messi ai detenuti agli arresti domiciliari (Lyon, 1994). In questo modo il reo potrebbe essere costantemente monitorato senza gravare come onere occupando un posto in cella. Questo esempio ci mostra benissimo la flessibilità tecnologica dei sistemi di sorveglianza e il fatto che gli stessi possano comportare un diverso tipo di controllo per diversi tipi di persone.
La stragrande maggioranza delle persone che possiedono questa tecnologia non viene monitorata come la popolazione carceraria perché gli scopi sono diversi. I sistemi *GPS* permettono alle aziende di controllare la posizione di un utente in un determinato luogo e, in base alla creazione dei profili di cui abbiamo abbondantemente parlato, offre loro di indirizzare le spese dello stesso quando si trova in una determinata zona. Per la stragrande maggioranza quindi i sistemi *GPS* sono strumenti che rendono possibile l'incremento della raccolta dei dati personali.

6.2.2 Telefonini

Il dispositivo mobile più utilizzato in assoluto è proprio il cellulare che sembra accompagnare in ogni dove la nostra persona. Funzionano tramite onde radio collegandosi alla cella più vicina che smista la nostra comunicazione ad un'antenna a terra che successivamente la rinvia ad un'altra cella dove si trova l'utente con il quale vogliamo entrare in contatto. I sistemi *GSM* (*Global System for Mobile Communications*) a differenza dei sistemi *GPS* permettono una localizzazione soltanto della cella in cui il cellulare si trova. E la grandezza delle celle varia a seconda del traffico di dati e degli ostacoli fisici che incontrano, per cui ne possiamo avere di decine di metri come di chilometri.
Lo standard UMTS (Universal Mobile Communications System) che invece si sta implementando in questo periodo, permette una localizzazione precisa come nei sistemi *GPS*, basando lo scambio dati anche su collegamenti satellitari. Inoltre questi nuovi cellulari rappresentano la convergenza di più strumenti in uno perché permettono al telefono il collegamento alla rete e la possibilità di accedere a determinati servizi, come vedere la televisione[36].
Questi nuovi sistemi si prestano ad essere però degli ottimi strumenti di sorveglianza. Già stanno nascendo particolari applicazioni che sono in grado di mettere in collegamento il nostro cellulare con le telecamere posizionate all'interno delle nostre

case per poterle costantemente controllare[37], ma questo rappresenta certamente un vantaggio.
Le evoluzioni preoccupanti riguardano gli utilizzi che le aziende possono effettuare di queste tecnologie. In molti casi le imprese forniscono ai propri dipendenti cellulari con strumenti di localizzazione per poter controllare la loro posizione una volta fuori dall'azienda. La *Nextel Communications* ha recentemente sviluppato un software chiamato *Mobile Locator* che consente di individuare i propri dipendenti che hanno un cellulare dotato di dispositivi di localizzazione: attraverso una tecnologia chiamata *geofence* (*geographical defence*) il software è in grado di far scattare un allarme in azienda ogni volta che i dipendenti si trovano in un luogo a loro vietato come i bar o i parchi[38].
Le applicazioni su cui però le aziende puntano maggiormente sono quelle che riguardano il settore commerciale. Come abbiamo già potuto osservare infatti questi sistemi vengono sviluppati per permettere alle aziende di inviare pubblicità sul cellulare di un utente nel momento in cui esso passa in una determinata zona. Così al passaggio vicino ad un cinema potremmo essere informati che si stanno svendendo dei biglietti e lo spettacolo può interessarci, dato che hanno già il nostro profilo. Il sistema inglese *Zagme* informa gli utenti delle offerte promozionali che sono presenti nell'area in cui stanno transitando in base alle loro preferenze (Mazoyer, 2001). In più questi sistemi configurandosi come strumenti multimediali permettono alle aziende che forniscono i servizi di telefonia mobile di implementare i nostri profili di riferimenti culturali che riguardano le nostre preferenze.

6.2.3 Wi-Fi e palmari
Discorso breve per il *Wi-Fi* (*Wireless Fidelity*) e per i palmari. In entrambi i casi ci troviamo di fronte a strumenti che permettono alle aziende di monitorare l'attività dell'utente come abbiamo potuto osservare con il pc una volta che ci si è connessi alla rete. L'unica differenza di questi strumenti sta nel contesto di fruizione della connessione stessa, in quanto non avviene a casa, ma può avvenire in diversi contesti. Per i palmari la connessione può avvenire sfruttando un telefono esterno oppure, e sono gli ultimi modelli, esso stesso svolge anche la funzione di cellulare. Mentre per il Wi-Fi ci troviamo di fronte ad una connessione che avviene in determinate aree che costituiscono un network.
Queste aree possono essere delle *LAN* (*Local Area Network*) aziendali, oppure possono essere determinate zone, come ce ne sono negli aeroporti o nelle stazioni dei treni, che permettono ad un utente l'accesso temporaneo alla Rete. In questo contesto l'aspetto da evidenziare è che queste tecnologie permettono alle aziende, come per i cellulari, di localizzare l'area in cui ci troviamo e pertanto alle informazioni raccolte tramite Internet dobbiamo aggiungere anche questo aspetto.

6.3 Carte ed etichette
Le carte non le abbiamo fatte rientrare nella categoria dei dispositivi mobili, anche se la possibilità di portarle sempre con noi le farebbe rientrare a pieno in questa, in quanto sono strumenti che necessitano di altri dispositivi per poter funzionare.

Le applicazioni per cui vengono comunemente usate sono molteplici. Abbiamo le carte di credito che permettono i pagamenti o quelle premio che permettono di ottenere sconti o finanziamenti. Così come abbiamo carte d'identità o passaporti elettronici che permettono la nostra identificazione, o *smart card* che ci permettono di accedere a determinati servizi.
Possono funzionare attraverso la lettura di una banda magnetica o di un chip ma il funzionamento è per tutte lo stesso: vengono inserite in un apposito strumento e permettono ad esso di leggere le informazioni che sono contenute al loro interno. Nella stragrande maggioranza dei casi vengono a rientrare nella categoria delle *tecnologie d'identificazione* che ci permettono di accedere a determinati servizi riconoscendoci, anche se poi il loro utilizzo e le informazioni raccolte vanno comunque ad ingrandire tutte le *tecnologie d'indagine*.

6.3.1 Smart card

Le *smart card* contengono un microprocessore incorporato e una memoria. Dispongono inoltre di un sistema di archiviazione protetta per i dati, incluse le chiavi private e i certificati con chiave pubblica. Anche le carte di credito come le carte di fedeltà possono rientrare in questa categoria, ma preferiamo trattarle a parte perché vengono utilizzate soltanto nel settore commerciale, mentre le *smart card* hanno un utilizzo molto più ampio.
La loro caratteristica è infatti quella di poter contenere nel proprio chip una serie di informazioni che possono essere costantemente aggiornate. La quantità delle informazioni varia dalla capacità di memoria della scheda. Questa caratteristica permette alle *smart card* di essere utilizzate in maniera diversa da varie agenzie con funzioni diverse a seconda dei loro scopi.
In Canada vengono utilizzate dal Ministero della sanità come tessera d'identificazione sanitaria inserendo al loro interno la cartella clinica del soggetto in maniera tale da fornire ai diversi enti coinvolti con il paziente, ospedali o anche farmacie, con precisione ogni sua informazione e somministrare le giuste terapie (Lyon, 1994). Possono essere utilizzate dalle amministrazioni per permettere ai cittadini di accedere a determinati servizi, come il pagamento delle imposte o la richiesta di certificati, inserendo al loro interno le informazioni ad essi relative. Vengono utilizzate nei cellulari di terza generazione per permettere di verificare che il telefono utilizzato funzioni solo con quel tipo di scheda, in maniera tale da impedirne utilizzi impropri. Le *smart card* vengono utilizzate nei decoder per permettere ad un abbonato di rivedere un servizio e fare in modo, associando in maniera univoca una scheda ad un decoder, che il sistema non venga utilizzato in maniera impropria.
Essenzialmente sono delle *tecnologie d'identificazione* che permettono di accedere ai servizi riconoscendoci. Per questo in moltissimi casi vengono comunemente chiamate "firma digitale", quando questa è una delle possibilità offerte. La necessità infatti di poter autenticare documenti digitali o di poter far accedere a distanza a determinati servizi ha comportato lo sviluppo delle *smart card* come firma che va a sostituire il timbro o la carta d'identità. La firma digitale è un segno di

riconoscimento che permette al cittadino di comunicare con le P.A. o permette alle aziende di scambiare documenti fra loro. È una certificazione dell'autenticità di un documento o di un soggetto[39].
Le *smart card* possono anche essere utilizzate come documenti d'identità elettronici nel momento in cui vengono inseriti all'interno dei passaporti, nelle patenti o nelle carte d'identità. In Italia[40] sono 83 i comuni in cui è stata avviata la sperimentazione e sono state emesse circa 100.000 carte d'identità elettroniche ibride (con banda magnetica e microchip). Al tempo stesso possono essere utilizzate come carte di trasporti come nel caso della *Metrebus card* per identificare i possessori di un abbonamento[41].
L'evoluzione tecnologica attuale permetterà di utilizzare un'unica smart card per le più svariate transazioni. Infatti si cerca di sviluppare carte uniche che possano essere utilizzate sia come documenti sia come carte di credito (Lyon, 2001).
Per l'individuo questo sarà una grande comodità in quanto permetterà di utilizzare un unico strumento per essere identificato dalle varie agenzie, pubbliche e private, con cui entrerà in contatto. Tuttavia la possibilità che i dati raccolti all'interno possano essere scambiati, visualizzati, e utilizzati dalle aziende o dagli stati in maniera non corretta può sollevare serie preoccupazioni relative alla privacy. Anche perchè all'interno delle stesse possono essere inseriti anche dati sensibili come quelli sanitari. Nel momento in cui i dati fluiscono nelle varie parti del mondo, dove non esistono le stesse tutele giuridiche al trattamento degli stessi, le preoccupazioni possono risultare maggiormente evidenti.
Inoltre il timore è che in alcuni casi le smart card possano essere aggiornate di informazioni che riguardano le preferenze politiche degli individui, andando ad essere utilizzate come strumenti di discriminazione per particolari gruppi. Situazione che con le normali carte d'identità avviene in diversi paesi (Lyon, 1994), e che abbiamo potuto notare è avvenuta in Europa quando alcuni contestatori sono stati bloccati alle frontiere (Mathesien, 2000).
E dove erano state prelevate le informazioni? In che modo? Forse lo sapremo fra qualche anno.

6.3.2 Carte di credito e fedeltà

Le carte di credito ed il bancomat negli ultimi anni hanno visto incrementare notevolmente il loro utilizzo. Per il cliente sono una comodità impensabile fino a pochi anni fa perché permettono di avere una disponibilità economica in qualsiasi angolo del pianeta che sia dotato della giusta apparecchiatura. L'architettura attraverso cui funzionano è la stessa dell'EFT (Electronic Funds Transfer), il sistema di bonifico bancario : la carta viene inserita in un apposito strumento, che può essere il lettore del supermercato o lo sportello bancomat, che si collega alla nostra banca e riceve da questa informazioni sulla nostra solvibilità (Lyon, 1994). La velocità della trasmissione dei messaggi, grazie all'incremento ricevuto negli ultimi anni, avviene in tempo reale. Le informazioni che ci riguardano sono contenute all'interno della banda magnetica oppure del chip e grazie a questo sistema le banche ed i negozi

riescono ad identificarci come consumatori affidabili e per cui possono concederci il credito.
Questi strumenti però hanno la possibilità di far ottenere informazioni dettagliate riguardo le nostre transazioni. Le banche attraverso gli sportelli bancomat riescono a sapere dove siamo soliti prelevare o per quali scopi utilizziamo la carta, quando paghiamo con il bancomat. Ma le informazioni ottenute sono alquanto generiche e i profili su di noi possono incrementarsi in maniera ridotta.
Discorso diverso se pensiamo alle carte di credito o alle carte fedeltà. Quest'ultime negli ultimi tempi vengono utilizzate da tutte le grandi catene di distribuzione, che spaziano dai grandi magazzini ai distributori di benzina, con due precisi scopi. Il primo è quello di "fidelizzare" il cliente promettendo a lui sconti o premi in funzione di un maggior utilizzo della carta, in maniera tale da battere la concorrenza. Il secondo è quello di raccogliere i dati personali dei clienti stessi.
Infatti le carte premio e le carte di credito permettono alle aziende di sapere con precisione cosa e dove abbiamo comprato, ed in questo modo esse possono effettuare un *profiling* geografico delle aree, come abbiamo già osservato, possono combinare i dati raccolti e formulare statistiche, e possono migliorare il *profiling* individuale (Clarke, 1987; Lyon, 1994, 2001; Marx G.T., 2002).
Attraverso questa raccolta dati le aziende possono rivendere gli stessi, per cui i dati diventano un altro settore in cui ottenere profitti, e attuare strategie di vendita che possono essere personalizzate. (Lyon, 1994, 2001).

6.3.3 Tag

Il *tag* non è altro che un'etichetta che viene inserita su un determinato oggetto. Quelle con cui maggiormente abbiamo contatto sono i codici a barre inseriti nelle confezioni dei prodotti che acquistiamo giornalmente. Come abbiamo detto in precedenza esse riescono a permettere alle aziende di rintracciare il prodotto e così riscontrare la causa di qualche anomalia o falla. Negli ultimi anni però si stanno studiando e immettendo sul mercato le *tags RFID* (*Radio Frequency Identification*) che sono delle etichette in radiofrequenza[42].
Scopo primario di queste etichette è quello di fornire l'identificazione di un prodotto attuando una connessione con un sistema wireless (senza fili). I componenti fondamentali di questi sistemi sono un'antenna ricetrasmittente, uno schermo di visualizzazione delle informazioni ricevute, e un transponder (quest'ultimo costituito a sua volta da un'antenna ricetrasmittente, una batteria e un microchip) inserito all'interno dell'oggetto. Questo sistema in pratica permette di scambiare informazioni in tempo reale fra l'etichetta e il sistema wireless ad esso connesso. Le applicazioni di questa tecnologia sono molteplici.
Il telepass ha al suo interno una *tag* che in vicinanza del casello si collega, attraverso le onde radio, a questo ed effettua il pagamento. Nelle fabbriche le *tags RFID* vengono adottate per far comunicare i vari rami della produzione. In campo sanitario si cerca di svilupparle per inserirle sulle sacche di emoderivati in maniera tale da permettere agli operatori sanitari di conoscere con precisione la quantità di sangue disponibile nei magazzini e il loro tipo. Così come si cerca di svilupparle per fare in

modo che al malato non vengano somministrate terapie sbagliate. Ma le applicazioni che possono entrare maggiormente in contatto con le nostre esistenze sono quelle che riguardano i prodotti commerciali.
In questo settore infatti si cerca di fare in modo che diversi dispositivi possano comunicare tutte le informazioni di cui ha bisogno un'impresa. L'inserimento di *tags RFID* nei prodotti sugli scaffali, permette ai grandi magazzini di sapere quando un prodotto viene preso in maniera tale da poterlo rimettere sugli scaffali stessi, diventando uno strumento fondamentale per gestire il magazzino. Inoltre esse permetterebbero una comunicazione fra il prodotto e tutta la serie di elettrodomestici intelligenti che si stanno sviluppando. *Le tags RFID* permetterebbero alle lavatrici di sapere come devono essere lavati i capi d'abbigliamento o permetterebbero al frigorifero di indicarci con un messaggio sul cellulare quando un prodotto è finito, o, ancora meglio, potrebbero ordinarlo direttamente se l'elettrodomestico fosse collegato alla Rete. Può sembrare fantascienza invece è proprio quello che si sta sviluppando (Bolter, Grusin, 2001). Al consumatore le *tags RFID* permetterebbero di avere informazioni precise sui prodotti, tant'è vero che la *Nokia* ha sviluppato il *Nokia Mobile RFID Kit*[43] che permette di collegare il cellulare a tutti gli oggetti intelligenti dotati di questa tecnologia e far ricevere informazioni, o far partire direttamente applicazioni, sull'oggetto al cellulare.
Per quello che riguarda il nostro settore possiamo vedere come queste *tags* possano comunicare in maniera diretta con una serie di dispositivi. La distanza di comunicazione delle *tags* varia da pochi centimetri a decine di metri. In questa maniera potremmo fare una serie di acquisti e una volta usciti da un supermercato anche altri soggetti, oltre naturalmente al negozio dove abbiamo acquistato, potrebbero essere in grado di identificare le nostre spese. Oltretutto, come nota Patierno nello speciale che *Punto Informatico* ha dedicato all'argomento[44], questi dispositivi potrebbero fornire indicazioni alla concorrenza riguardo le politiche di vendita adottate da un negozio e pertanto riuscire a riconfigurare le proprie in funzione dei dati raccolti.
Il fenomeno in questione è in rapida ascesa tant'è vero che un'indagine[45] condotta dalla società di ricerche *Vanson Bourne* ha evidenziato come in Italia circa il 38 per cento dei rivenditori intervistati ha dichiarato che circa la metà dei prodotti venduti è dotata di *tags RFID*. Il problema ha interessato anche i Garanti della Privacy che dopo la conferenza tenuta a Sidney hanno adottato la *Risoluzione sull'identificazione attraverso radiofrequenze (RFID)* del 20 novembre 2003[46] in cui si evidenzia che

> pur esistendo situazioni in cui tale tecnologia può avere effetti positivi e benefici, vi sono anche implicazioni potenziali in termini di privacy. Sinora le etichette RFID vengono utilizzate soprattutto per l'identificazione e la gestione di oggetti (prodotti), per il controllo della catena distributiva, o per tutelare l'autenticità di singoli marchi; tuttavia, esse potrebbero essere messe in relazione con dati personali come quelli ricavabili dalle carte di credito, e potrebbero essere utilizzate persino per raccogliere tali dati, oppure per localizzare o profilare individui in possesso di oggetti che rechino tali etichette. La tecnologia in questione potrebbe consentire di ricostruire le attività di singoli individui e istituire collegamenti fra le informazioni raccolte e banche dati preesistenti.

Lo sviluppo sistematico di queste etichette potrebbe comportare un'erosione massiccia della privacy individuale[47] permettendo a molteplici soggetti di ottenere informazioni sulle nostre preferenze d'acquisto senza che noi abbiamo deciso di fornirgliele, come invece avviene per le carte di credito e quelle fedeltà.

7. TUTTO IL MONDO È PAESE

In questo capitolo cercheremmo di identificare tutte le *tecnologie d'indagine* che fanno riferimento ai dati raccolti dai sistemi di sorveglianza o semplicemente per routine (Castells, 2001). Sono praticamente tutte quelle tecnologie che fondano sul database la loro esistenza.
Inoltre cercheremo di spiegare il funzionamento di quei sistemi che riescono ad incrementare in maniera significativa lo scambio dati fra le varie parti del globo, o che fanno dell'intero pianeta il fulcro del loro monitoraggio. Pertanto ci occuperemo di tutte quelle tecnologie che vengono utilizzate dalle polizie del pianeta per prevenire crimini o identificare criminali.

7.1 Il database

Il database non è altro che un contenitore. Un sistema di archiviazione in cui confluiscono i dati raccolti. Nel momento in cui i primi studiosi si accingevano ad analizzare il problema la grandezza del database appariva come uno degli aspetti maggiormente preoccupanti. La creazione di grandi database dove sarebbero andati a confluire l'insieme dei dati raccolti, magari su scala nazionale come si cercò di fare negli U.S.A. o in Inghilterra (Lyon, 1994) o si cerca di attuare in Canada (Cockfield,2004), sembrava comportare la nascita di quel *Grande Fratello* da tutti temuto (Lyon, 1994).
Tuttavia con il passare del tempo si è visto che la grandezza del database può essere irrilevante se l'insieme degli stessi sono connessi in una rete che permette lo scambio dei dati. In questo contesto è la velocità dello scambio dati ad essere centrale e il sistema d'identificazione dei dati raccolti. Cercheremo di analizzare quindi il funzionamento attuale.

7.1.1 UPI

L'*UPI* (*Universal Personal Identifier*) è lo strumento che serve per identificare un soggetto. Lo potremmo definire come un codice a cui corrisponde l'identità di una persona reale, quasi una carta d'identità elettronica in pratica.
Ogni database per poter inserire un soggetto al proprio interno e per aggiornare di volta in volta i dati relativi allo stesso deve poterlo identificare in maniera univoca, l'*UPI* permette proprio questo. Come ha sottolineato Poster i database funzionano in maniera rigida classificando ed inserendo i dati nelle proprie tassonomie (Poster,1990), un sistema perfettamente integrato non può pertanto essere basato su uno strumento di classificazione come il nome o la data di nascita di un soggetto, ma c'è bisogno di qualcosa che non possa lasciare margine di discrezione o di errore. Un numero, ad esempio, che identifichi chiaramente un individuo è certamente meglio. Per questo gli *UPI* vengono basati su dati che cercano il più possibile di essere unici.

Negli U.S.A. l'apparato burocratico usa il numero di previdenza sociale degli individui per identificarli nei propri database, utilizza le impronte digitali, come in Inghilterra, per schedare i criminali, (Lyon,1994) o può utilizzare il DNA per identificare i criminali che hanno compiuto reati sessuali[48]. Il sistema Enfopol utilizza i numeri di carte di credito come *UPI* (Chiesa,2000), e così via. Si può vedere come siano vari i sistemi d'identificazione sia in base ai paesi e sia all'interno degli stessi in base alle agenzie.
Tutto questo come abbiamo notato nel secondo capitolo genera confusione fra i vari database e non permette una comunicazione idonea fra gli stessi. Per questo motivo si cerca di creare un *UPI* unico che sia utilizzato da tutte le agenzie che raccolgono i dati in maniera tale da poter visualizzare tutte le informazioni su un individuo.
Le attuali tendenze in atto, in ascesa dopo gli attentati terroristici recenti, cercano di sviluppare sistemi basati su dati biometrici come l'impronta dell'iride, il DNA o le impronte digitali come *UPI* (Clarke, 1987, Lyon, 2001b) in questo modo tutti i database del mondo potrebbero scambiarsi i dati in tempo reale senza equivoci.

7.1.2 Computer matching

La computer matching è una pratica. È il controllo incrociato dei dati contenuti all'interno dei database. Il sistema si basa sul *front end verification*: dato un soggetto si cerca di raccogliere, nell'insieme dei database disponibili, tutte le informazioni sullo stesso e verificare così la sua posizione (Clarke, 1987). Tutto questo è naturalmente reso possibile dalla creazione di reti a cui sono connessi i database: maggiori ce ne sono e maggiori informazioni si potranno avere a disposizione. È proprio grazie a questa pratica che può avvenire il *profiling* di un individuo.
Come si è visto nel corso dei capitoli a fare uso di questa pratica sono tutte le agenzie, pubbliche e private, che hanno le esigenza di verificare l'identità di un soggetto o la sua attendibilità. Basta digitare l'*UPI* e i computer incroceranno i dati dei database fino a raccogliere tutte quelle di nostre interesse. Il funzionamento del sistema è lo stesso descritto nel capitolo precedente per le tecniche di riconoscimento facciale.
Quello che come abbiamo potuto notare nel corso dei capitoli è la sistematicità di questa pratica che va ad inserirsi in ogni angolo delle nostre esistenze, influenzandole direttamente, senza che il soggetto preso in esame ne possa venir a conoscenza.
Maggiore preoccupazione può essere evidenziata nel momento in cui i dati fra pubblico e privato possono essere tranquillamente scambiati rendendo i database statali disponibili al controllo incrociato da parte delle aziende, e viceversa quelli aziendali disponibili allo Stato. I sistemi di sorveglianza globale che ci accingiamo a descrivere infatti possono controllare tutti i database grazie a questa pratica.

7.2 Sorveglianza totale o quasi

Come descritto nel terzo capitolo ci sono una serie di agenzie che operano a livello globale o transnazionale che riescono a raccogliere quasi tutte le informazioni

riguardo agli individui. Di seguito descriveremo in dettaglio il funzionamento dei sistemi da essi utilizzati.

7.2.1 Echelon

Echelon è il sistema computerizzato per lo spionaggio utilizzato dall'NSA per sorvegliare tutte le comunicazioni mondiali. Al suo controllo non sfuggono né le comunicazioni che vengono criptate né tantomeno quelle che passano attraverso i cavi a fibra ottica (Bamford, 2001).

Per catturare le comunicazioni, come abbiamo visto nel terzo capitolo, vengono create delle postazioni vicino ai satelliti Intelsat in maniera tale da captare tutti i segnali che vengono trasmessi. Tutte le comunicazioni vengono sottoposte ad analisi in base alle parole chiave, queste vengono cambiate giornalmente in base a ciò che i governi vogliono cercare.

Quando l'NSA riceve le liste di controllo con le parole chiave, i nomi o i numeri di telefono da ricercare, gli analisti assegnano a questi dati dei numeri a quattro cifre, denominati codici di ricerca, e poi li trasmettono a tutte le postazioni dell'UKUSA sparse nel pianeta.

In questo modo può essere attivato un computer chiamato *Dictionary* che va alla ricerca di queste parole all'interno dei messaggi che transitano nel pianeta, catturati dalle postazioni d'ascolto. In pratica il funzionamento è simile a quello che viene utilizzato nei motori di ricerca (Bamford, 2001). Differenza è che l'NSA usa programmi appositi che vengono denominati *bots* che in automatico, una volta ricevuta la parola, partono al setaccio delle comunicazioni (Lyon, 2001). Quando le parole sono state trovate scatta una segnalazione e la comunicazione viene classificata ed archiviata per essere sottoposta ad analisi.

Le parole chiave però devono essere trovate anche all'interno di tutti i documenti che vengono scambiati nel mondo, come i fax, le e-mail o i testi che si trovano in rete. Per trovare le parole l'NSA ricorre ad un software chiamato *Semantic Forests* (foreste semantiche). Questo software si basa sui contenuti delle conversazioni ed è sviluppato per rispondere a domande di senso compiuto: si formulerà una domanda al computer e questo scoverà tutti i documenti che al proprio interno contengono i significati cercati. Il funzionamento è lo stesso che si svilupperà per il web semantico (Bamford, 2001).

Per tradurre la mole di tesi che ogni giorno vengono trovati, che possono spaziare dall'essere in azerbaigiano (dialetto turco) fino al chorti (variazione della lingua utilizzata dai Maya) vengono utilizzati programmi quali il *Systran* che riescono a tradurre automaticamente circa 750 pagine all'ora, quando un traduttore umano impiega circa quarantacinque minuti per tradurre una singola pagina (Bamford, 2001).

Molto più complessa è invece la traduzione delle comunicazioni vocali e la loro trascrizione una volta che esse vengono selezionate. Per risolvere il problema, l'NSA in collaborazione con l'University of South California hanno sviluppato un sistema computerizzato in grado di riconoscere gli interlocutori di una conversazione umana. Questo sistema viene chiamato *Speaker ID* e riesce ad emulare la maniera in cui il

cervello elabora le informazioni. In questo modo si può trascrivere un'intera comunicazione distinguendo con esattezza da chi vengono pronunciate le singole parole, e possono essere anche eliminati in automatico tutti i rumori di fondo (Bamford,2001).
Infine per analizzare i file che vengono scambiati in rete si utilizzano programmi *sniffer software*, normalmente utilizzati dagli hacker, che riescono a intercettare tutti i pacchetti TCP/IP che viaggiano nella rete (Lyon, 2001).
Qualunque sia il mezzo di comunicazione utilizzato, se qualcuno di noi dirà determinate parole può stare certo che la sua conversazione finirà in "Crypto City"[49].

7.2.2 Carnivore

Tutti coloro che sostengono che fra l'NSA e le altre agenzie governative non scorre buon sangue, probabilmente sostengono il vero. *Carnivore* è la risposta dell'FBI al sistema Echelon, anche se dobbiamo sottolineare come il compito di questa agenzia dovrebbe essere svolto a livello nazionale, mentre all'NSA è proibito sottoporre ad intercettazione i cittadini americani (Bamford, 2001).
Carnivore, il cui nome esatto è DCS1000, come si può leggere dal sito dell'FBI[50] è un sistema passivo capace di filtrare i pacchetti di dati che transitano tra l'utente ed il provider e di ricostruire i messaggi scambiati: posta elettronica, pagine Web visitate, e conversazioni in diretta. Essenzialmente è un filtro che viene montato nei server degli Internet Provider per monitorare le comunicazioni. Le giustificazioni che vengono adottate per l'implementazione del sistema fornite al Congresso ricalcano a pieno la *strategia dell'emergenza*: lotta al terrorismo, al traffico di droga, alla prevenzione della pedofilia, alla lotta contro gli hacker. Dopo l'undici settembre il sistema è stato sviluppato significativamente fino ad obbligare gli Internet Provider americani all'installazione sui propri server del filtro (Cockfield, 2004; Lyon, 2001b).
Il sistema è essenzialmente composto da un computer collegato presso un provider, che copia tutti i dati che passano. Questo viene inserito nella rete nel segmento di interesse della persona che si vuole indagare non interagendo con il flusso dei dati, ma limitandosi a copiarlo solo. Una volta copiati i pacchetti, questi vengono analizzati automaticamente da un filtro che cerca i termini richiesti. Tutto il materiale ininfluente viene eliminato liberando memoria, mentre i dati interessanti vengono salvati su un disco Jaz che un incaricato dell'FBI scarica quotidianamente[51].
La legislazione degli U.S.A. infatti sancisce che le intercettazioni delle comunicazioni delle persone prese in esame debbano essere prima approvate da un magistrato. Tuttavia dopo il Patrioct Act si è visto che le agenzie governative sono state dotate di una certa flessibilità e pertanto si può supporre che tutte le comunicazioni vengano prese in esame. Infatti gli Internet Provider avevano proposto all'FBI un loro filtro che di volta in volta avrebbe permesso di registrare solo le conversazioni delle persone indagate, questa in un primo tempo aveva accettato, ma successivamente si è tirata indietro ribadendo l'utilizzo del *Carnivore*[52].

La preoccupazione che tutte le comunicazioni che passino all'interno di tutti i server americani vengano costantemente monitorate riguarda tutti i cittadini del mondo dato che, come nota Castells, la maggioranza delle comunicazioni in rete, anche quando non sono dirette negli Stati Uniti, passa attraverso nodi della rete stessa situati negli U.S.A. (Castells,2001).
Inoltre la polizia federale americana pare abbia sviluppato un software, chiamato *Magic Lantern*, che è stato pensato per entrare nei computer dei sospetti e fornire non solo testi e documenti, ma soprattutto chiavi di accesso, password e modalità di decifrazione dei documenti criptati. *Magic Lantern* sembra poter installare sul computer del sospetto un software capace di registrare tutti i tasti che vengono premuti sul computer. Grazie al monitoraggio dei tasti si possono ottenere tutte le informazioni desiderate sulle attività del soggetto sottoposto a controllo[53]. Per sviluppare il progetto L'FBI ha chiesto alle case di software per la sicurezza quali *Symantec* di fornirlo nei loro prodotti, ma queste si sono rifiutate.
Il pensiero che il progetto della "Lanterna Magica" venga implementato a tal punto da essere inserito in tutti gli antivirus rende nessuno dei navigatori al sicuro dalle maglie del controllo americano. Fin troppo sviluppato.

7.2.3 Enfopol
Secondo l'Unione Europea, Enfopol sarebbe solo un acronimo usato per classificare i documenti relativi alla cooperazione delle polizie e al rafforzamento delle leggi che vengono distribuiti nell'ambito del Consiglio dei ministri. Secondo Raoul Chiesa, considerato uno dei più importanti hacker italiani, Enfopol è invece il nome con cui viene denominato un sistema di intercettazione, sviluppato in collaborazione con l'FBI, di tutte le comunicazioni che avvengono nell'Unione Europea (Chiesa, 2000).
Le origini del sistema, scoperto dall'organizzazione non governativa per le libertà civili *StateWatch*, risalirebbero al 1993 da un incontro fra servizi segreti australiani, polizie europee ed FBI. Nel 1994 queste arrivarono alla compilazione di un documento denominato *Iur (International user requirements for communications interception)* che conteneva gli standard ai quali le aziende di telecomunicazioni dovevano attenersi per consentire la più completa libertà di investigazione e di intercettazione alle forze di polizia internazionali[54]. Le aziende avrebbero dovuto fornire delle vie d'accesso, delle porte, per permettere alle polizie di intercettare le comunicazioni (più o meno come avviene per *Carnivore*). Negli U.S.A. il codice *Iur* fu approvato e divenne legge nel 1995, in Europa il Consiglio dei Ministri approvò la risoluzione *Enfopol 95*, nella quale chiedeva alle aziende di telecomunicazioni europee di adottare i requisiti tecnici che erano stati decisi. Successivamente partì il progetto denominato *Enfopol 98* che forniva una serie di proposte per far si che le forze dell'ordine europee e l'FBI potessero intercettare anche le comunicazioni passanti su Internet, sui satelliti, e sul telefono. Il documento venne approvato dal Parlamento Europeo nel maggio del 1999, ma fu in seguito ritirato per ragioni di cui non si ha conoscenza.
A tutt'oggi il funzionamento del sistema, i compiti ad esso relegati, e le agenzie coinvolte sono avvolti da un fitto mistero. Se come sostiene Chiesa il sistema

permette l'intercettazione di tutte le comunicazioni dei cittadini europei, ed è stato implementato senza l'autorizzazione del Parlamento Europeo, le preoccupazioni relative alla privacy dei cittadini europei si fanno maggiormente rilevanti (Chiesa, 2000).

7.3 SIS

Il 14 giugno 1985 a Schengen venne firmato un accordo che, grazie alla relativa convenzione d'applicazione avvenuta il 19 giugno 1990, istituiva uno spazio di libera circolazione delle persone, tramite la soppressione dei controlli alle frontiere interne degli Stati membri. Grazie a ciò si instaurò il principio di un controllo unico all'entrata nel territorio Schengen. Per garantire la sicurezza degli Stati appartenenti alla Comunità Europea si rafforzò la collaborazione e la cooperazione fra le polizie europee e si omogeneizzarono le procedure per le politiche riguardanti i visti e l'asilo. Inoltre venne creato il SIS, Sistema d'informazione Schengen, che permetteva lo scambio delle informazioni fra i vari paesi dell'Unione.
Il SIS è un archivio comune che contiene al suo interno due categorie d'informazioni che sono quelle che riguardano i veicoli rubati e le persone ricercate o poste sotto sorveglianza o a cui è vietato entrare nel territorio Schengen. Pertanto il SIS si configura come un'enorme database che, attraverso il controllo incrociato dei dati, permette alle polizie europee lo scambio delle varie informazioni[55].
L'aspetto preoccupante di questo sistema si configura nel momento in cui lo mettiamo in correlazione con le politiche adottate in seguito alla "lotta al terrorismo" e per fermare l'escalation dell'immigrazione.
Come abbiamo notato nel terzo capitolo, la creazione del sistema Eurodac ha comportato una schedatura di massa, utilizzando le impronte digitali, di tutti i soggetti che richiedevano asilo in Europa (Mathesien, 2000). Il rischio di questa struttura, come lì evidenziavamo, risiede nella possibilità di andare ad applicare un controllo di tipo rigido, istituendo i centri di prima accoglienza, soltanto verso una frangia di popolazione estremamente debole, dal punto di vista dei diritti, con il pericolo di andare ad "etnicizzare" la sorveglianza, considerando come pericolosi o indesiderati tutti i soggetti appartenenti a determinate etnie o provenienti da determinate aree (Lyon, 2001), senza calcolare le singole differenze individuali. La schedatura basata su dati biometrici, quali il DNA, inoltre permette alla *strategia dell'esclusione/inclusione* di attuare pratiche discriminatorie basate sulle caratteristiche genetiche.
Le attuali tendenze portate avanti dai biologi molecolari prefigurano un ritorno all'arcaica concezione lombrosiana di una correlazione fra tratti genetici e criminalità e alla predisposizione di alcuni soggetti a particolari forme di malattie (Rifkin, 1998), che se utilizzate nelle politiche di prevenzione dei flussi migratori, possono portare alla totale esclusione di visti o degli accessi all'Unione verso tutti quei soggetti che hanno dei particolari geni. Il sistema di sorveglianza della Comunità Europea potrebbe pertanto configurarsi come un sistema di discriminazione basato su genotipi, non più individuali, ma di determinate collettività.

Ma i pericoli maggiori riguardano l'implementazione del sistema attraverso la creazione del SIS II, e lo sviluppo del *SIRENE* (*Supplement d'Information Requis a l'Entree Nationale*). Quest'ultimo non è altro che un miglioramento del sistema di scambio d'informazioni che permette ad ogni singolo agente di polizia, non più quindi soltanto a quelli ubicati alle frontiere del territorio Schengen, di ricevere informazioni su un singolo individuo, in tempo reale grazie all'istituzioni di reti telematiche, su di un telefono cellulare o un altro terminale (Mathesien, 2000). In questa maniera le polizie europee vengono dotate di un efficace strumento di controllo e verifica della popolazione, basato sulle informazioni sugli individui racchiuse nei vari database nazionali. Il database, abbiamo sottolineato più volte, è una tecnologia fortemente discriminante e possono essere molteplici le distorsioni che può creare. Fortunatamente i cittadini europei possono avere accesso a questi dati e sapere quali informazioni sono raccolte su di loro[56].
Il SIS II invece, come dimostra l'organizzazione per le libertà civili *Statewatch*, prevede la creazione di carte d'identità nazionali basate sulle fotografie, sulle impronte digitali, e possibilmente sul DNA[57], in maniera tale da rendere certa ed univoca l'identificazione delle persone. I rischi di questa pratica sono già stati ampliamenti discussi precedentemente. Quello che deve essere sottolineato è la grande discriminazione che il sistema in generale comporterebbe.
Come infatti viene da più parti evidenziato[58] questo sistema non solo andrebbe a far rientrare una più ampia categoria di persone fra gli "indesiderabili", ma dovrebbe far figurare al proprio interno anche tutti quei criminali recidivi e sopratutto i militanti antiglobalizzazione. La collaborazione non solo delle polizie europee, ma anche dei servizi segreti, infatti permetterebbe un maggior numero d'informazioni all'interno del database.
In questa maniera il sistema si afferma come uno strumento di controllo politico per impedire l'accesso a particolari raduni, manifestazioni, o semplicemente per sorvegliare, una determinata fascia di popolazione che non accetta le politiche europee.

CONCLUSIONI

Siamo giunti al termine del viaggio. Abbiamo scavato e scoperto, visto e sentito, analizzato e cercato di capire i fenomeni. Ora ci troviamo di fronte ad un foglio bianco con l'intento di tracciare linee definitive e fornire soluzioni ai problemi delineati. Guardiamo indietro al nostro lavoro e ci sembra di essere incapaci di trovare uno sviluppo positivo dei fenomeni che fino a qui abbiamo delineato.
Vorremmo essere ottimisti, riuscire a tenere conto di tutte le necessità dei diversi attori, ponderarle, e indicare le linee di tendenza con cui tracciare il futuro. Purtroppo, però, sappiamo che i settori coinvolti e le implicazioni sono così tante, che per, scacciare da noi tutte le distopie che hanno accompagnato il nostro percorso, è necessario attuare un ripensamento dell'intero sistema. Cambiare le sue logiche di sviluppo.
Siamo partiti con Morin che ci mostrava come il modello che si è affermato fin dai primordi è stato quello della dominazione dell'uomo sull'uomo. Del più forte sul più

debole e dei pochi che governano i molti. Ogni fase storica, ogni società su cui abbiamo posato lo sguardo ci ha continuato a mostrare il perpetuamento di questo modello. Ci ha reso evidente che il Potere nelle fasi storiche è passato di mano in mano, prima nei sacerdoti, poi nei signori, poi nello Stato infine nelle mani dei capitalisti e delle grandi aziende, senza mai essere veramente nelle mani del popolo.
Siamo partiti nella ricerca convinti di vivere in uno Stato democratico, in cui il popolo è re e signore e a lui e solo a lui spetta il compito di governare se stesso. E ci siamo trovati increduli nel momento in cui abbiamo sentito parlare di classi politiche che tendono a perpetuare se stesse perseguendo come fine primario e ultimo il Potere. Avremmo voluto gridare che noi, popolo, governiamo decidendo ogni volta chi eleggere e che i nostri rappresentanti abbiano il nostro benessere come fine primario e ultimo. Ma anche se avessimo urlato non avremmo trovato argomenti con cui controbattere alle critiche. Ci siamo resi conto che noi, decidiamo veramente poco del processo politico in atto. Sono passate di fronte a noi tutte le scene di politiche e programmi che noi mai avremmo sognato di sostenere. E ci siamo rattristati quando siamo stati d'accordo con il professor Mongardini quando sosteneva che chi ci governa è una classe di plutocrati. Una serie di oligarchi diversi che rappresentano tanti diversi gruppi d'interesse. Che Destra e Sinistra, Reazionario e Rivoluzionario, Democratico e Repubblicano, non sono altro che facce della stessa medaglia in cui al centro c'è il Potere.
Ci siamo rattristati ancora di più quando abbiamo capito che anche il migliore dei nostri rappresentanti, quello che più ha a cuore il nostro benessere, non può nulla in quanto inserito in un particolare sistema. Che anche il migliore degli Stati inserito nei processi di globalizzazione non può far altro che piegarsi alle decisioni che altri organismi prendono per lui.
Abbiamo visto la nascita dell'impresa capitalistica, la sua espansione, il suo divenire modello unico, e siamo approdati al punto in cui essa permea e oltrepassa ogni sfera della nostra esistenza. In cui le grandi corporazioni agiscono a livello internazionale come se fossero Stati, e a livello individuale come se noi non fossimo nient'altro che consumatori. Siamo rimasti increduli nel vedere che esse cercano di monitorare costantemente le nostre esistenze, raccogliendo tutti i dati possibili su ciò che mangiamo, su quello guardiamo in tv, sulla musica che ascoltiamo, su quello che ci piace fare. E ci siamo indignati quando abbiamo scoperto di essere solo dei numeri, inseriti in tante tabelle che hanno lo scopo di definirci. Di sapere chi Siamo. Il nostro Essere. Ma, soprattutto, siamo rimasti stupefatti nel vedere che questi pseudo-noi vengono comunemente usati per influenzare le nostre esistenze. *Noi oggetti e soggetti di discorsi altrui.*
E allora abbiamo di nuovo confidato nel Potere dello Stato. Certi che in esso avremmo trovato risposta. Ma esso ci è apparso incapace. Piegato dai processi esterni lo abbiamo visto riversare su noi la sua perdita di Potere. Abbiamo assistito increduli al varo di misure eccezionali giustificate da lotte al terrorismo che non hanno comportato una maggiore sicurezza per noi, ma semplicemente una limitazione delle nostre libertà. Ci è sembrato assurdo vedere unirsi insieme, fino quasi a con-fondersi, lo Stato-nazione e l'impresa capitalistica. Vedere che essi lavorano insieme, uno

fornendo stabilità e l'altro tecnologia, per continuare a far stare noi soggiogati a loro. E ci è sembrato ancora più assurdo che le tecnologie che avrebbero dovuto garantire la nostra sicurezza vengano comunemente usate per sopprimere il dissenso. Eravamo certi di ciò pensando a Stati quali la Cina o la Birmania, ma quando ci siamo trovati di fronte all'evidenza che la nostra amata Europa utilizza questi metodi, abbiamo chiuso gli occhi. Riaprendoli abbiamo visto persone fermate alle frontiere perché i loro dati li classificavano come dissidenti politici. E ci siamo resi conto che anche la libera manifestazione del pensiero può diventare un problema. Che questo SuperPotere che si sta realizzando non ama chi non la pensa come lui e pertanto cerca di attuare un controllo politico del pensiero.
Siamo rimasti ripugnati quando abbiamo visto che i sistemi di sorveglianza vengono comunemente usati per allontanare da determinate aree determinati individui. Così come per i manifestanti, abbiamo visto questi sistemi venir utilizzati per allontanare i barboni dalle aree urbane o riversare una determinata criminalità in zone non visibili. E ci è apparso inquietante il loro utilizzo per monitorare il flusso dei migranti, inserirli in tante categorie di ammessi e non ammessi in base all'etnia, e rinchiuderli in centri simili a carceri. Fare di esse non-persone, fatte di dati e analisi, situate in non-luoghi, fatte di mura e cemento.
Ed abbiamo avuto paura, e tuttora l'abbiamo, di sentire che si profila la schedatura dei nostri dati genetici. Ne abbiamo avuto paura pensando alle parole di un Professore dell'Università di Princenton, Lee Silver, che auspica la creazione di una società composta da due classi di individui. Da un lato i Gen Rich, con geni sintetici innestati, come classe superiore e dall'altro tutta la popolazione normale. Ci è tornato in mente un *Mondo Nuovo*, e in silenzio, abbiamo pianto pensando che vorremmo rimanere nel Vecchio.
E abbiamo pianto ancora, stavolta di rabbia, quando abbiamo visto alcuni biologi molecolari del Progetto Genoma Umano organizzare un convegno dal titolo " I fattori genetici del crimine" che presupponeva un ritorno alle teorie della delinquenza innata. Abbiamo pianto perché ritornare a Lombroso vuol dire buttare via cent'anni di Sociologia e di Psicologia.
Alla fine del percorso ci siamo resi conto che tutti i sistemi di sorveglianza tendono ad essere utilizzati per aumentare il divario esistente fra ricchi e poveri. Fra i pochi che detengono il Potere e la massa che li guarda e si fa guardare impotente. Che anche gli strumenti che possono essere utilizzati per migliorare i processi democratici, quali il Web, si prestano ad essere usati per aumentare le maglie del nostro controllo.
Allora non può esserci soluzione ai problemi posti se l'intero sistema non viene riformulato. In ambito politico bisogna, e torniamo a Mongardini, *Ripensare la democrazia*, e far si che al processo politico partecipino tutti i soggetti interessati e, soprattutto, far si che essi dialoghino a livello paritario. In questo senso tutti gli strumenti di comunicazione che abbiamo a disposizione potrebbero essere usati per stabilire un rapporto diretto fra governati e governanti. E non essere usati come strumenti di dominio.

In ambito commerciale invece bisogna formare il Potere che le grandi corporazioni stanno sviluppando. Per ciò che riguarda il nostro settore siamo convinti che solo arrivando a tassare ogni scambio ed elaborazione dei nostri dati, e far si che questa tassa possa essere a noi pagata, si possa fermare questo sistema e far si che la nostra privacy rimanga tale.
Ora ci fermiamo. Siamo giunti davvero alla fine del viaggio. Ora dobbiamo guardare avanti. Sappiamo che le nostre parole saranno vento e come tale verranno disperse. Il futuro sarà un sogno visionario che vede le nostre città separate in tante aree con tante possibilità d'accesso in base ai redditi, con messaggi pubblicitari che ci rincorrono in ogni luogo chiamandoci per nome. Che vede le nostre esistenze piegate al volere di quello che ci vogliono far Essere, e masse di diseredati che vivono in bidonville grandi quanto megalopoli.
Il futuro se non si interviene in tempo sarà forse anche peggio.

BIBLIOGRAFIA

Abe, K., 2004, *Everyday Policing in Japan*, in International Sociology, Vol.19, n.2 Jun 2004, pp 215-231;

Anderson, B., 1991, *Comunità immaginate*, IlManifestolibri, Roma, 2000.

Ball, K., 2003, *The Labours of Surveillance*, in Surveillance & Society, Vol. 1, N. 2, pp 125-137.

Bamford, J., 2001, *L'orecchio di dio*, Roma, Fazi Editore, 2004.

Bauman, Z., 1998, *Dentro la globalizzazione*, Bari, Laterza, 1998.

Bauman, Z., 2000, *Modernità liquida*, Bari, Laterza, 2002

Bennato, D., 2002, *Le metafore del computer*, Meltemi, Roma.

Bennato, D.,2002b, *Gli archivisti di Babele. L'impatto sociale dei motori di ricerca*, in Morcellini M., Pizzaleo A.G., a cura di, *Net Sociology*, Guerini e Associati, Milano

Bettetini, G., Garassini, S., Vittadini, N., 2001, *I nuovi strumenti del comunicare*, Milano, Bompiani.

Bolter, J. D., Grusin,R., 2001, *Remediation. Competizione e integrazione tra media vecchi e nuovi*, Milano, Guerini e Associati, 2002.

Brecher, J.,Costello, T.,1995, *Contro il capitalismo globale*, Bologna, Feltrinelli, 1996.

Cammarata, M., 2002, *Principi importanti, ma l'applicazione è difficile*, in Interlex, 02/07/2002, disponibile all'indirizzo: http://www.interlex.it/675/principi.htm

Cammarata, M., 2003,*"Spyware",qualcosa non va nel Codice della Privacy*, in InterLex, n.207, 10/09/2003, disponibile all'indirizzo: http://www.interlex.it/675/spyware.htm

Cammarata, M., 2004, *E Microsoft continua a spiarci in maniera indisturbata*, in InterLex n. 227, 15/04/2004, disponibile all'indirizzo: http://www.interlex.it/675/mscontinua.htm

Cammarata M., Maccarone E., 2003, *La firma digitale sicura.Il documento informatico nell'ordinamento italiano*, Milano, Giuffrè Editore.

Castells, M., 2001, *Galassia Internet*, Milano, Feltrinelli.

Charny, B., *Cellulari per controllare i dipendenti*, CNET News.com, 27/09/2004, disponibile all'indirizzo: http://tecnologia.virgilio.it/vt_cntDefault.prn.aspx?i dcontent=182813

Clarke, R., 1987, *Information technology and dataveillance*, in Commun. ACM 31,5, May 1988, pp. 498-512.

Clarke, R., 1993, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, in Journal of Law and Information Science 4,2, December 1993, disponibile all'indirizzo http://www.anu.edu.au/people/Roger.Clarke/DV/Paper Profiling.html

Cockfield, A., 2004,*The State of Privacy Laws and Privacy- Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government*, University of Ottawa Law and Technology Journal, Spring 2004, pp.325-344.

Dal Lago, A., 1981, *La produzione della devianza,* Milano, Feltrinelli.

Davis, M., 2004, *Cronache dall'impero*, Roma, IlManifestolibri.
De Andreis P.,*Biometria e sicurezza italiane*, in Punto Informatico del 21/03/03, visibile all'indirizzo : http://punto-informatico.it/p.asp?i=43506&p=1
D'Eramo, M.,2004, *L'impronta del terrore*, in Il Manifesto, 13/01/2004.
Deleuze, G.,1990, *La società del controllo*, in *l'autre journal*, n. 1, maggio 1990, ora in Gilles Deleuze, *Pourparlers (1972-1990)*, Minuit, Paris, 1990, pp. 240-247. Traduzione di Giuseppe Caccia
Durkheim, E.,1893, *La divisione sociale del lavoro*, Milano, Edizioni di Comunità, 1962.
EFF (Electronic Frontier Foundation), 2003, *Position*
Statement on the Use of RFID on Consumer Products, 14/10/2003, disponibile all'indirizzo: http://www.eff.org/Privacy/Surveillance/RFID/RFID_Pos ition_Statement.pdf
Fazzino E., 2004, *Patriot act, il prezzo della libertà*, in IlSole24ore.com, disponibile all'indirizzo: http://www.ilsole24ore.com/fc?cmd=art&codid=20.0.670388198&chId=30.
Ferrarotti, F, 1965, *Max Weber e il destino della ragione,* Bari, Laterza.
Froomkin, M. A., 2000, *The Death of Privacy?*, in Stanford Law Review, May 01, 2000, disponibile all'indirizzo : http://static.highbeam.com/s/stanfordlawreview/may01 2000/thedeathofprivacy/.
Foucault, M., 1975, *Sorvegliare e punire*, Torino, Einaudi, 1976.
Garante per la Protezione dei dati personali, 2000, *La videosorveglianza esterna visibile: una panoramica su quattro città - Indagine esplorativa - Giugno 2000*, disponibile all'indirizzo: http://www.garanteprivacy.it/garante/doc.jsp?ID=1002987.
Garante per la Protezione dei dati personali, 2003, *Risoluzione sull'identificazione attraverso radiofrequenze (RFID),20/09/2003,* disponibile all'indirizzo: http://www.garanteprivacy.it/garante/doc.jsp?ID=4 54143.
Garassini, S., Vittadini, N., 2001, *Quali nuovi media*?, in *I nuovi strumenti del comunicare*, Bompiani, Milano 2001, pp. 177-178
Giddens, A., 1990, *Le conseguenze della modernità*, Il Mulino, Bologna,1994
Graham, S., Wood, D.,2003, *Digitizing Surveillance: Categorization, Space, Inequality*, in Critical Social Policy, May 2003, n 23, pp. 227 - 248.
Gritti R.,1999, *Le relazioni internazionali nel mondo postbipolare. Una prospettiva sociologica*, in De Nardis, Paolo, A cura di, *Le nuove frontiere della sociologia*, Roma, Carocci.
Gurtvich, G., 1947, *Il controllo sociale,* Roma, Armando, 1997.
Hobbes, T, 1651, *Leviatano,* Bari, Laterza, 2001
Lankshear, G., Cook, P., Mason, D.J., Coates, S., Button, G.,2001, *Call Centre Employees' Responses to Electronic Monitoring: Some Research Findings*, in Work Employment Society, Sep 2001, Vol.15, n.3, pp. 595 - 605.
Lyon, D.,1991,*La società dell'informazione*, Bologna, Il Mulino, 1994.
Lyon, D, 1994, *L'occhio elettronico,* Milano, Feltrinelli, 1997.
Lyon, D., 2001, *La società sorvegliata*, Milano, Feltrinelli, 2002.
Lyon, D., 2001b, *Surveillance after September 11,* in *Sociological Research Online,* vol. 6, n. 3, disponibile all'indirizzo http://www.socresonline.org.uk/6/3/lyon.html>
Lyon, D., 2004, *Globalizing Surveillance: Comparative and Sociological Perspectives*, in International Sociology, Vol. 19, n. 2, Jun 2004, pp. 135 - 149.
Kivinen, O., Varelius J.,2003,*The Emerging Field of Biotechnology—The Case of Finland*, Science, Technology & Human Values 2003 n.28, pp.141-161.
Marx, K,1867, *Il Capitale*, Roma, Editori Riuniti, 9 Volumi, 1973.
Marx, Gary T.,1985, *Undercover: police surveillance in America*, Berkeley, University of California press.
Marx, Gary T.,2001,*Surveillance and society*, in International Encyclopedia of the Social and Behavioral Sciences, disponibile all'indirizzo: http://web.mit.edu/gtmarx/www/surandsoc.html.
Marx, Gary T.,2002, *What's New About the "New Surveillance"?Classifying for Change and Continuity*, in Surveillance & Society, Vol1, n. 1, pp 9-29.

Mathesien, T.,2000, *Schengen,Europol,Eurodac e i piani di sorveglianza dell'Unione Europea*, in Telepolis del 18/06/2000, disponibile all'indirizzo: http://www.tmcrew.org/border0/dossier/sis/sis00.htm.
Mazoyer, F.,2001, *Il lucroso mercato della sorveglianza*, in Le Monde Diplomatique/Il Manifesto, settembre 2001.
Mignani, M., Bazzoffia, A., 2000, *Pubblivori del terzo millenio*, in *Fabbriche del desiderio*, 2000, Roma, Luca Sossella Editore, pp. 109-115
Mongardini, C., 2001, *Ripensare la democrazia*, Milano, Franco Angeli.
Morin, E., 1973, *Il paradigma perduto,* Milano, Feltrinelli, 1974.
Nicholson, M., 1998, *Introduzione allo studio delle relazioni internazionali*, Bologna, Il Mulino, 2000.
Olgiati, V. Tomeo, V., 1991, *Agenti e agenzie del controllo sociale,* Milano, Franco Angeli.
Parthasarathy, S., 2004, *Regulating Risk Defining Genetic Privacy in the United States and Britain*, in Science, Technology & Human Values 2004, n. 29, pp.332- 352.
Patierno, C., 2004, *Viaggio nel mondo RFID (I,II,III,IV,V)* dossier in più parti in Punto Informatico, disponibile all'indirizzo: http://puntoinformatico. it/archivio/trovato.asp?sel=0&sand=Viaggio %20nel%20mondo%20RFID.
Ponti, G.,1999, *Compendio di criminologia*, Bologna, Ed.Cortina.
Poster, M., 1990, *The mode of information,* Polity Press, Cambridge.
Rampini, F., *Google e la nuova legge sulla privacy delle e-mail*, in Affari e Finanza del 31/10/2004.
Reidenberg, R.J., 2001, *Privacy protection and the interdependence of law, technology and selfregulation*, rapporto presentato alla 23rd Conference of Data Protection Commissioners, Paris 2001.
Rodotà, S., 2003, *Se il mercato scheda la salute del cittadino*, in La repubblica del 14/07/2003.
Romagnolo S., *Un GPS sottocutaneo per controllare bambini, vecchi, animali. O voi?*, in Apogeonline Webzine, 3/06/2003, disponibile all'indirizzo: http://www.apogeonline.com/webzine/2003/06/03/ 06/200306030601
Rifkin, J., 1998, *Il secolo Biotech*, Milano, Baldini e Castoldi, 1998.
Rust, R.T, Kannan, P.K., Peng, N., 2002, *The Customer Economics of Internet Privacy*, in Journal of the Academy of Marketing Science, Vol.30, n.4, pp.455- 464
Santini, A., 2000, *Fare comunicazione pubblitaria su Internet*, in *Fabbriche del desiderio*, 2000, Roma, Luca Sossella Editore, pp. 211-224.
Shenk, D,2003, *Sorvegliati a vista*, in National Geographic, 11/2003, pp.2-29
Solove, J., 2001, *Privacy and Power:Computer Databases and Metaphors For Information Privacy,* in Stanford Law Review, July 01 2001, disponibile all'indirizzo: http://ssrn.com/abstract=248300
Stallman, R.,2002, *Puoi fidarti del tuo computer?*, in InterLex, n.190, 31/10/02, disponibile all'indirizzo: http://www.interlex.it/675/stallman.htm
Statera, G.,1996,*Manuale di sociologia scientifica,* Roma, Seam.
Statewatch, 2003, *Biometrics - the EU takes another step down the road to 1984*, 19/09/2003, disponibile all'indirizzo: http://www.statewatch.org/news/2003/sep/19eubi ometric.htm
Strano, M., 2000, *Computer Crime*, Milano, Apogeo.
Tomlinson, J.,1999, *Sentirsi a casa nel mondo*,Milano, Feltrinelli, 2001.
Van Burren, J., *I tentacoli dell'accordo di Schengen*, in Le Monde Diplomatique/Il Manifesto, Marzo 2003.
Virilio, P., 1989, *La macchina che vede*, Milano, SugarCo.
Wacquant, L., 1999, *I "Sorvegliati a vita"degli Stati Uniti*, in Le Monde Diplomatique/Il Manifesto, dicembre 1999.
Wallach, L., Sforza, M, 1999, *Wto*, Bologna, Feltrinelli, 2000.
Weber, M, 1922, *Economia e società,* Milano, Edizioni di Comunità, 2 Volumi, 1961.
Weber, M, 1919, *Parlamento e governo*, Roma, Laterza, 1993.

Zureik, E.,2001, *Constructing Palestine through Surveillance Practices*, in British Journal of Middle Eastern Studies, Vol. 8, N.2, pp. 205-228.
ZureiK, E., Rohozinski, R., 2004, *Information Technologies & Information Societies:Critical Issues in the MENA Region,* Workshop in 5th MSPR Meeting (2004).

NOTE

1 Si veda a questo proposito : Engels F.,1974, *L'origine della famiglia, della proprietà privata, dello stato,* Roma,Newton Compton Editori.
2 Weber sottolinea il fatto che creare delle corporazioni professionali che siano corpo elettorale per il parlamento renderebbe quest'ultimo un "mercato per compromessi di interessi puramente materiali", che le elezioni verrebbero influenzate dai finanziamenti elettorali, e che lo stesso corpo elettorale sarebbe poco funzionale in quanto andrebbero a costituirsi all'interno delle lotte di potenza (Weber, 1919, p.29).
3 Si può vedere a questo proposito Virilio P., 1989.
4 Sono alcune delle tassonomie che vengono usate da alcuni istituti di ricerca sui consumi.
5 Per Giddens, ad esempio, la sorveglianza insieme al capitalismo, all'industrialismo e al potere militare è una delle quattro dimensioni che costituiscono la modernità (Giddens A., 1990).
6 Per analizzare il cambiamento della cultura in relazione ai processi di globalizzazione si veda Tomlinson J.,1999.
7 Sul ruolo giocato dagli organismi transnazionali nelle politiche governative si veda Wallach L., Sforza M, 1999.
8 Per una analisi approfondita di questi programmi si rimanda al libro citato nella nota precedente e a Brecher J.,Costello T.,1995.
9 Se si vuole analizzare il ruolo delle multinazionali si vedano i libri citati nellenote precedenti.
10 Manifesto di protesta dell'associazione *Il secolo della rete* al decreto-legge, http://www.snark.it/modules.php?name=News&file=article&sid=742).
11 Si veda D'Eramo M., 2004.
12 Si veda l'articolo di Shenk D,2003.
13 Il rimando è alla doppia elica con cui è costituito il DNA.
14 Per le teorie criminali basate sui geni si rimanda al libro di Ponti (vedi bibliografia).
15 Deborah Radcliff, *A Cry for Privacy*, Computer World, May 17, 1999
16 Cfr. Rampini F., *Google e la nuova legge sulla privacy delle e-mail*, in *Affari e Finanza* del 31/10/2004.
17 Assante E., *Jason lo spione che rischia grosso*, in *Il Venerdì di Repubblica* del 9/04/2004.
18 *Se il mercato scheda la salute del cittadino*, in *La repubblica* del 14/07/2003.
19 È il caso del decoder digitale terrestre in Italia che è stato lanciato sul mercato in tutta fretta più per rispondere ad esigenze politiche, non mandare ReteQuatrro sul satellite, che per un suo reale sviluppo.
20 L'informativa è visualizzabile all'indirizzo: http://www.skytv.it/Offerta/PopUp_Privacy.htm
21 Si veda nota precedente
22 L'informativa sulla privacy della XBox Live è disponibile all'indirizzo: http://www.xbox.com/it-IT/live/privacystatement.htm
23 Il documento è visionabile in lingua inglese all'indirizzo: http://www.interlex.it/testi/pdf/wd5035.pdf
24 http://www.realnetworks.com/local/it/guids.html
25 Fonte Logitech :http://www.logitech.com/index.cfm?page=utilities/home&contentid=4056&countryid=16&languageid=5
26 A questo proposto si veda l'articolo su *Punto Informatico* all'indirizzo http://puntoinformatico.it/p.asp?i=47390b
27 L'indirizzo è:

http://www.microsoft.com/windows/windowsmedia/IT/software/v7/privacy.asp#_What_personal_identifiable

28 Fonte My tech :http://www.mytech.it/news/articolo/idA006012003380.art

29 Le informazioni di seguito riportate sono prese dal sito della Tesar che è un'azienda che fornisce tecnologie per la gestione aziendale. Il sito è www.tesar.it.

30 http://www.tesar.it/articolo.asp?idarea=14&idsarea=4&idssarea=3

31 Vedi nota ventinove

32 L'indagine è disponibile dal sito del Garante per la protezione dei dati personali all'indirizzo: http://www.garanteprivacy.it/garante/doc.jsp?ID=1002987

33 In Italia questo impiego non'è permesso.

34 De Andreis P.,*Biometria e sicurezza italiane*, in Punto Informatico del 21/03/03, visibile all'indirizzo : http://punto-informatico.it/p.asp?i=43506&p=1

35 Romagnolo S., *Un GPS sottocutaneo per controllare bambini, vecchi, animali. O voi?*, in Apogeonline Webzine, 3/06/2003, disponibile all'indirizzo: http://www.apogeonline.com/webzine/2003/06/03/06/200306030601

36 Vengono utilizzati due diversi tipi di protocolli per le chiamate e per lo scambio dati. In quest'ultimo caso il protocollo è lo stesso, TCP/IP, usato in Internet.

37 Uno di questi è il servizio *DomusLife* di *Tim*, che permette di interrogare la telecamera ogni volta che vogliamo o di programmarla per mandarci un MMS ogni tot. orario.

38 Ben Charny, 27/09/2004, *Cellulari per controllare i dipendenti*, CNET News.com. disponibile all'indirizzo: http://tecnologia.virgilio.it/vt_cntDefault.prn.aspx?idcontent=182813

39 Si veda Cammarata M., Maccarone E., 2003.

40 Si veda il sito del Governo Italiano all'indirizzo: http://www.governo.it/GovernoInforma/Dossier/carta_nazionale_servizi/cie.html

41 A tutt'oggi non si sa se la *Metrebus card* possa fornire informazioni circa la localizzazione dei possessori e, se possibile, come i dati vengano trattati.

42 Le informazioni di seguito elencate sono prese dallo speciale che Patierno su *Punto Informatico* ha dedicato all'argomento. Lo speciale è visualizzabile all'indirizzo: http://puntoinformatico. it/archivio/trovato.asp?sel=0&sand=Viaggio%20nel%20mondo%20R FID

43 Si veda il comunicato stampa della Nokia all'indirizzo: http://www.nokia.it/nokia/0,0,56455,0,0.html

44 Vedi nota quaranta

45 Fonte Smau. Articolo disponibile all'indirizzo: http://www.smau.it/smau/view_NO.php?IDcontent=23111

46 La risoluzione è visionabile dal sito Del Garante per la Protezione dei dati personali all'indirizzo: http://www.garanteprivacy.it/garante/doc.jsp?ID=454143

47 Si veda a questo proposito il rapporto che l'*EFF* (*Electronic Frontier Foundation*) ha dedicato alle tags. Il dosssier è scaricabile all'indirizzo: http://www.eff.org/Privacy/Surveillance/RFID/RFID_Position_Statement.pdf

48 Si veda Wacquant L., 1999.

49 Questo è il termine con cui Bamford chiama il quartier generale dell'NSA nel Maryland.

50 L'ìndirizzo è: http://www.fbi.gov/congress/congress00/kerr090600.htm

51 Fonte Andrea Iolis,Vice Procuratore Onorario presso la Procura della Repubblica del Tribunale di Roma, http://www.lucernaiuris.it/informatica/carnivore.html

52 Vedi nota precedente

53 Fonte Punto Informatico. Indirizzo: http://punto-informatico.it/p.asp?i=38126

54 Si vedano gli articoli apparsi su MediaMente, http://www.mediamente.rai.it/docs/approfondimenti/010531.asp, e su La Repubblica.it, http://www.repubblica.it/online/tecnologie/echelon/enfopol/enfopol.html.

55 Si veda il Sito dell'Unione Europea alla sezione Giustizia e affari interni. Indirizzo: http://europa.eu.int/scadplus/leg/it/s22000.htm

56 Per la procedura d'accesso ai dati si veda il sito del Garante per la Protezione dei dati personali. Indirizzo: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp
57 Statewatch, Settembre 2003, *Biometrics - the EU takes another step down the road to 1984*, disponibile all'indirizzo: http://www.statewatch.org/news/2003/sep/19eubiometric.htm
58 Si vedano a proposito i dossier effettuati sull'argomento da *Statewatch* (www.statewatch.org) e l'articolo di Van Burren J., *I tentacoli dell'accordo di Schengen*, in Le Monde Diplomatique/Il Manifesto, Marzo 2003.