La Sapienza
Università degli Studi di Roma

Facoltà di Scienze della Comunicazione

Tesi di Laurea

TEORIE E TECNOLOGIE DEI SISTEMI DI SORVEGLIANZA

Candidato
Igor Jan Occelli

Relatore
Prof. Alberto Abruzzese

Correlatore
Prof. Andrea Granelli

Anno Accademico 2003/2004

INDICE

"...chi comanda non è disposto
a fare distinzioni poetiche.
Il pensiero è come l'oceano,
non lo puoi bloccare,
non lo puoi recintare.
Così stanno bruciando il mare..."

Lucio Dalla, *Com'è profondo il mare*.

INTRODUZIONE

Quando abbiamo cominciato a scrivere la tesi, ci siamo resi conto che tutte le persone a cui parlavamo dei sistemi di sorveglianza sgranavano gli occhi come a voler dire “Di che stai parlando?”, e quando non lo facevano pensavano che ci riferissimo ad antifurti o simili. Anche coloro i quali avevano una conoscenza dell’argomento sembrava conoscessero solo *Echelon*, magari perché avevano visto un film che più o meno ne parlava, e ci guardavano come dei paranoici con la fobia del *Grande Fratello*.

E forse un po’ paranoici lo siamo stati. Ma senza sentire voci nella testa, senza vedere teorie del complotto e, soprattutto, senza fobie. Ci siamo ricordati di una frase ascoltata vedendo *Strange Days* che diceva che la “paranoia è un modo più sottile di vedere la realtà”, e l’abbiamo fatta nostra. Abbiamo cercato di far luce dove è buio, e di mostrare quello che c’è sotto la superficie su cui ogni giorno camminiamo. Semplicemente abbiamo cercato di guardare dietro a tutte quelle tecnologie che ogni giorno utilizziamo. Siamo andati sotto le interfacce studiando i processi. E abbiamo messo i nostri risultati nero su bianco. Se questo vuol dire essere paranoici lo siamo stati. A voi la risposta.

Più di ogni altra cosa comunque, abbiamo cercato di spiegare, usando la semplicità, cosa sono i sistemi di sorveglianza, il loro funzionamento, e perché essi riguardino tutti noi nessuno escluso.

Come tali intendiamo tutti quei sistemi che attuano un monitoraggio delle nostre attività, raccogliendo informazioni su di noi, usando una molteplicità di strumenti che possono spaziare dall'occhio agli applicativi informatici.

Per essere chiari abbiamo diviso la nostra tesi in tre parti, in maniera tale da farla diventare una guida, una sorta di manuale, per tutti coloro che dell'argomento non sanno nulla o sanno poco. Ma anche coloro che tutto sanno sulla sorveglianza troveranno che essa può essere per loro un utile strumento nel momento in cui si trova a spiegare il funzionamento delle tecnologie.

Nella prima parte ci siamo occupati delle Teorie che hanno accompagnato la nascita di questo settore di studio. Siamo partiti dalla necessità del controllo sociale come strumento attraverso cui si può garantire ordine per qualsiasi forma di società. Abbiamo visto nascere dei sistemi di sorveglianza basati sull'occhio e sul concetto che "tutti sono i guardiani di tutti", fino ad arrivare alla nascita della società moderna e alla Norma quale strumento di regolamentazione dei conflitti. E da questo punto in poi è cominciato veramente il nostro viaggio.

Nel primo capitolo attraverso gli studi di Marx, considerato da noi uno dei Padri degli studi sulla sorveglianza, abbiamo visto nascere una sorveglianza sui lavoratori attuata dal capitalista e, successivamente dal *management*, con lo scopo di gestire la produzione e sottomettere gli operai a quello che lui ha definito come *regime di fabbrica*. Con Weber abbiamo visto come il sistema capitalistico abbia la necessità di avere un organo di

gestione che garantisca stabilità. La burocrazia fondata sul calcolo e sul raziocinio garantisce questo obiettivo e va a formare un sistema di sorveglianza astratto, impersonale, che imprigiona lo spirito in quella che definisce “gabbia d’acciaio”, basato su di un Sapere specializzato che genera Potere e consente di assoggettare la popolazione. Attraverso Foucault abbiamo analizzato il Potere e abbiamo visto che questo non si *possiede*, ma si *esercita* grazie ad un sistema di scarti e differenze dove ogni individuo è inserito in un rango. Che le società moderne attuano la messa a punto di una serie di *dispositivi*, caserme, fabbriche, scuole, che come fine hanno quello di far rientrare tutto nella Norma. Abbiamo visto nascere sistemi di sorveglianza basati sui dossier, che cercano di prevenire devianze e disordini, e siamo approdati a quella che lui ha definito come *società disciplinare*.

Nel secondo capitolo abbiamo visto nascere un nuovo tipo di sorveglianza. Deleuze ci ha fatto capire che si è passati dalle discipline ai moduli. Ad un controllo esercitato in ogni luogo, in maniera diversa. Alla formazione di sistemi di sorveglianza che per esercitarsi non hanno più bisogno di spazi chiusi, ma possono modularsi e cambiare in base al luogo. Attraverso Gary T. Marx, abbiamo visto che la *nuova sorveglianza* diventa meno visibile e sfrutta tutte le nuove tecnologie per esercitarsi. Che il baricentro viene spostato dalla *repressione* dei reati alla *prevenzione*. Che diventa centrale la raccolta delle informazioni e il loro immagazzinamento. Clarke ci ha mostrato che le informazioni raccolte servono per creare *profili* delle persone che vengono utilizzati

dalle polizie per prevenire i reati, chi può commettere un determinato tipo di reato, e alle aziende per vendere, chi può comprare un determinato tipo di prodotto. Poster invece ci ha mostrato come il database, che raccoglie tutte le nostre informazioni, sia una tecnologia fortemente discriminante che porta con sé la formazione di un alter-ego virtuale del soggetto che può influenzare in maniera diretta le nostre esistenze. Infine Lyon ci ha fatto capire come il corpo stesso diventi uno strumento da cui prelevare le informazioni divenendo così fonte e fine dei discorsi del Potere. Tutti gli autori ci hanno mostrato la nascita di sistemi di sorveglianza elettronici che fanno emergere la *data-veglianza*, basata sulle informazioni che riguardano le nostre attività, e ci hanno evidenziato la centralità della raccolta dati.

Nella seconda parte ci siamo occupati delle strategie che vengono adottate dagli apparati statali e dalle imprese commerciali per sviluppare i sistemi di sorveglianza, per raccogliere informazioni su di noi, o semplicemente per gestire la loro attività. In questo senso per strategia intendiamo l'individuazione degli obiettivi da raggiungere e il mezzo ed i modi opportuni per raggiungerli.

Nel capitolo terzo prendiamo in considerazione l'apparato statale e vediamo come esso compia una serie di strategie diverse in funzione dei suoi scopi. Abbiamo in questo caso effettuato una nostra teorizzazione basandoci sulle informazioni raccolte. Così possiamo avere una *strategia normalizzatrice* compiuta con lo scopo di mantenere l'ordine attuata attraverso il diritto e la Norma dall'apparato statale in genere, e una *strategia gestionale* propria

dell'apparato burocratico che ha come obiettivo la gestione dei beni statali e della popolazione e viene attuata raccogliendo informazioni sulla popolazione stessa. Infine abbiamo rielaborato le teorie del professor Mongardini e siamo giunti a vedere come gli organismi statali attuino una *strategia dell'emergenza* per sviluppare i sistemi di sorveglianza che viene giustificata avendo come obiettivo quello della "lotta al terrorismo" e viene attuata ampliando i sistemi di controllo e le aree in cui prelevare informazioni. Infine abbiamo una *strategia dell'esclusione/inclusione* che serve a categorizzare gli individui e a farli rientrare in determinate tassonomie e permette allo Stato di ampliare il Sapere sugli individui stessi.

Nel capitolo quarto invece ci siamo soffermati sulle imprese commerciali e vediamo che esse ripropongono due delle strategie sopra delineate: quella *dell'esclusione/inclusione* e quella *gestionale*. La prima viene usata per individuare quali consumatori possono essere inclusi o esclusi da particolari promozioni, o, in ambito lavorativo, quali soggetti possono accedere a determinati settori o ottenere posti lavorativi. in questo caso i sistemi di sorveglianza servono per ottenere maggiori informazioni possibili sui soggetti d'interesse. Nel secondo caso la *strategia gestionale* viene attuata per gestire la catena di produzione e snellire il suo processo, in questo caso i sistemi di sorveglianza mostrano la loro flessibilità permettendo da un lato di monitorare le attività produttive e dall'altro l'operaio o l'impiegato.

Nell'ultima parte abbiamo analizzato il funzionamento delle tecnologie che vengono usate dai sistemi di sorveglianza. Per identificarle abbiamo utilizzato la tripartizione che fa Castells suddividendole in *tecnologie d'identificazione*, tutte quelle che servono per identificare o autenticare un soggetto o un programma, *tecnologie di sorveglianza*, che hanno il solo scopo di monitorare una determinata attività, e infine *tecnologie d'indagine*, che sono quelle che permettono un'archiviazione dei dati.

Nello strutturare i capitoli però non abbiamo potuto tener conto di questa tripartizione perché, come si vedrà, in molti casi il confine fra le tecnologie è molto sottile e, a tratti, inesistente. Pertanto abbiamo preferito suddividere i capitoli in base ai luoghi in cui le tecnologie vengono esercitate.

Nel quinto per cui parliamo di tutte le tecnologie che vanno ad esercitarsi nelle nostre abitazioni, come i pc, i decoder e le consolle, e quelle che trovano applicazione nei luoghi di lavoro come i gatekeeper o i processi gestionali.

Nel sesto capitolo studiamo quella che abbiamo definito come sorveglianza ubiqua, che tende ad essere applicata negli spazi cittadini, nel caso della videosorveglianza, o in ogni luogo in cui utilizziamo particolari strumenti come i cellulari o le carte di credito.

Per ultimo abbiamo tenuto tutte quelle tecnologie che non hanno un luogo preciso in cui esercitarsi, ma che fanno di ogni luogo un punto di monitoraggio, come i sistemi per la sorveglianza globale. E inoltre tutte quelle tecnologie che indipendentemente dal

luogo, come nel caso del database, esercitano o possono esercitare una forma di Potere.

Quello che si è delineato è che i sistemi di sorveglianza tendono a rempire ogni spazio. A seguirci ovunque anche quando siamo comodamente seduti in casa sui nostri divani a guardare la televisione. Stiamo vivendo in un'epoca in cui una serie d'agenzie, fra loro più o meno staccate, attua un monitoraggio continuo ed insistente sulle nostre esistenze. Il confine fra sfera pubblica e sfera privata grazie alle nuove tecnologie appare essere sempre più sfumato fino ad andare ad erodere definitivamente il concetto di privacy.

Inoltre si è visto come i sistemi di sorveglianza siano strumenti fortemente discriminanti che agiscono allargando il divario sociale fra chi può avere accesso a determinati servizi e chi non può. Si noterà come per la maggioranza della popolazione il controllo esercitato sia di tipo morbido, basato sulle seduzioni consumistiche, mentre per altri ancora sarà duro e rigido fino ad approdare all'emarginazione in determinate aree.

Alla fine anche togliendo le paranoie su grandi fratelli e simili, si è potuti arrivare alla conclusione che si sta delineando un nuovo *SuperPotere*, formato dalla convergenza delle imprese commerciali con gli apparati statali, i cui tratti distintivi ad oggi appaiono sfumati e indecifrabili. L'individuo diventa solo un numero a cui corrisponde un profilo creato attraverso i dati, da questi influenzato, e permette a questo nuovo Potere di estendere il suo dominio.

Il problema riguarda tutti, nessuno escluso, ed è ora che le conseguenze di tutto questo vengano maggiormente approfondite.

PARTE PRIMA TEORIE

1. SOCIETÀ, FABBRICA, STATO.

1.1 Cenni storici

Analizzare il controllo sociale vuol dire innanzitutto considerare questo come una componente fondamentale ed imprescindibile del vivere insieme. Non è possibile pensare una società dove non esistano norme che vadano ad imporre un ordine, che traccino i confini fra ciò che è lecito e ciò che non lo è, altrimenti l'anarchia prenderebbe il sopravvento. Regnerebbe il caos. Logica conseguenza di questo è l'istituzione di un'autorità che si faccia carico di vigilare sul rispetto di tali norme e perciò applichi un controllo sugli individui della società.
Fin dai primordi della nostra esistenza si affacciano forme di controllo basate sul concetto di " dominazione di una classe su un'altra" (Morin,1973, p.71). Nell'era degli ominidi è la classe dei maschi ad imporsi sul resto della popolazione e si crea una divisione del lavoro basata sui sessi (Morin,1973).
Un secondo stadio è visibile in quella che Morin chiama *protosocietà* in cui viene sanzionata la poligamia e si costituisce il nucleo familiare, che tende a riprodurre le divisioni fra i gruppi presenti nella società: il padre-sposo fa parte della classe dei maschi, la madre-sposa a quella delle femmine e il figlio al gruppo dei non iniziati. La classe dominante dei maschi si trasforma in classe dirigente e viene

creato un sistema di regole imperniato dei caratteri sacri del rito e della magia:

> l'identità individuale e collettiva non si afferma più nell'appartenenza immediata a un dato gruppo, come nella società di primati,bensì mediante e nell'insieme dei legami che uniscono l'individuo alla sua parentela reale e mitica e che danno a una cultura la sua particolare identità.(Morin,1973, op.cit. p.165)

In queste società prevale quella forma di solidarietà che Durkheim ha definito meccanica. Una solidarietà basata sull'uguaglianza degli individui, sulle loro radici comuni. Che poggia su un sistema di valori, norme e costumi condivisi che tracciano una linea di demarcazione netta fra ciò che è giusto e ciò che non lo è, che impone un modello culturale che spinge verso l'omologazione, sopprimendo le spinte individuali, per la creazione della “coscienza collettiva”.

La tradizione è il collante che regge il sistema. Si sviluppa così un controllo rigido che non permette e non accetta nessuna devianza, perché il bene comune è l'unico obiettivo da perseguire. Non vige un'autorità unica che si occupi di far rispettare le norme, ma tutti gli individui sono sia controllori che controllati. In queste società tutto il diritto è penale, il popolo giudica chi compie un reato, e tale è ogni atto che violi le pratiche collettive; la pena non serve per correggere il colpevole, ma assolve solo la funzione di mantenere intatta la coesione sociale (Durkheim,1893,).

Successivamente, nel momento in cui queste società entrano in contatto con popolazioni esterne allargandosi, nasce la società storica che va a porre nuovi problemi di ordine e di controllo. I principi organici che si basavano su un antenato comune non

bastano più a garantire l'ordine e non è più possibile una differenziazione del lavoro fra i due sessi. Le guerre danno la possibilità di avere degli schiavi che entrano a pieno nel circuito produttivo. Incomincia una nuova divisione fra liberi e schiavi e, successivamente, attraverso la nascita della proprietà privata, fra ricchi e poveri[1].

Una delle prime forme di questa società è la città-stato. La specializzazione dei lavori diventa più estesa, perché aumentano i bisogni della popolazione e di conseguenza le funzioni da svolgere per poter soddisfarli. Nascono le figure dei signori con il compito di governare, vengono creati le prime forme di burocrazia per la raccolta ed il calcolo delle ricchezze, si creano le corporazioni di mestieri e avviene una prima divisione fra lavoro intellettuale e lavoro manuale. In questa società la cultura non è più unica, ma si creano tante sottoculture in base alla classe di appartenenza. Dalla solidarietà meccanica si passa a quella organica: non più basata sull'omologazione degli individui, ma sulla differenza. Per sfuggire agli effetti dannosi della competizione vengono differenziati i compiti, dall'uniformità si passa alla complementarità. Il diritto penale viene limitato e nascono quello privato, civile e amministrativo, la sanzione diventa di tipo restituitivo, (comporta la riparazione) (Durkheim,1893).

È qui che vengono poste le basi del controllo sociale in due forme ben precise: istituzionale ed informale.

[1] Si veda a questo proposito : Engels F.,1974, *L'origine della famiglia, della proprietà privata, dello stato,* Roma,Newton Compton Editori.

> Il controllo di tipo istituzionale è dotato di significatività e credibilità, è durevole nel tempo e nello spazio e soprattutto visibile socialmente;si tratta di un controllo identificabile e formale il cui compito specifico è di verificare che non vengano oltrepassati i confini simbolici della normalità… il controllo di tipo informale si costituisce attraverso l'interazione sociale di soggetti… rappresenta la parte sommersa del controllo, la meno individuabile in quanto attiene alla normalità della vita quotidiana (Tomeo,Olgiati,1991, p.71-72).

Il controllo istituzionale racchiuso nel diritto, nel palazzo del signore, nella milizia. Il controllo informale dove ogni membro vigila (e viene vigilato) affinché nessuno oltrepassi la sfera del lecito (Gurtvich,1947).

Dobbiamo soffermarci su alcune caratteristiche. Nella città-stato il principe o il feudatario sono padroni assoluti. L'architettura serve a mantenere alcuni privilegi. La piazza centrale dove vengono svolte le funzioni di mercato, liturgiche e d'incontro è situata davanti al palazzo del sovrano. Basta affacciarsi per controllare il tutto. L'occhio è senso di controllo per eccellenza. E dove esso non può arrivare, dove serve anche l'udito, ecco che il compito di vigilanza viene assegnato alla milizia che pattuglia le strade e i vicoli.

Vengono create le corporazioni di mestieri il cui scopo è mantenere l'ordine esistente non permettendo la mobilità sociale (Durkheim, 1893).

Problemi nuovi nascono nel momento in cui la città stato si allarga. Si passa alla contea, al ducato e infine allo stato. Leviatano.

Bisogna comunque garantire l'ordine ed il controllo, ma l'occhio non basta più. Ne tantomeno le milizie. Solo le sottoculture possono ancora compiere il loro compito, ma il loro è un controllo di tipo

informale. C'è bisogno di una specializzazione dell'apparato burocratico. Usando la metafora hobbesiana c'è bisogno di una serie di *organi* che svolgano funzioni differenti, ma complementari. Magistrati e funzionari con compiti giudiziari ed esecutivi che rappresentino le *articolazioni*, sistemi di ricompense e punizioni che fungano da *nervi*, consiglieri che diventino la sua memoria, ed infine il monarca come *cervello* di questo *Uomo Artificiale* .Un apparato burocratico che, diversificandosi, amministri la giustizia, censisca la popolazione ed i possedimenti, in maniera tale da dare a tutto un nome e vedere chi deve e quanto pagare le tasse, che sia visibile socialmente. Il diritto come strumento normativo si diversifica e va a toccare ogni aspetto sia della vita pubblica che di quella privata. L'ordine è tutto quello che si deve ottenere. Quello che permette la prosperità e garantisce allo stato di persistere e sono proprio tutti questi diversi organi,dotati di autorità, che lo rendono possibile, (Hobbes,1651).

Democrazia o monarchia si crea un sistema che vincola e schiaccia il cittadino-suddito e lo lega a se, come sottolinea Morin :

> Lo Stato centralizzatore,costruttore,repressore costituisce un nuovo modo di organizzazione della complessità che muove da un apparato centrale. Questa complessità si sviluppa secondo principi analoghi a quelli dello sviluppo degli organismi pluricellulari:gerarchia e specializzazione del lavoro…di conseguenza si creano le divisioni radicali fra lavoro di esecuzione e di decisione, lavoro manuale e lavoro intellettuale … Congiuntamente la nuova disuguaglianza sociale comporta,per la massa degli oppressi, un enorme sottoimpiego delle capacità individuali. L'autorità repressiva dello Stato, la gerarchia, l'asservimento costituiscono per

> queste stesse masse un considerevole aggravio delle costrizioni in confronto alla protosocietà,fatto al quale bisognerà aggiungere gli effetti del mostruoso parassitismo dello Stato, dei signori e dei possidenti sull'insieme della società. Lo sfruttamento dell'uomo sull'uomo è una delle grandi invenzioni della società storica (Morin,1973,op. cit. p.176-177).

Con l'avvento della rivoluzione industriale cambieranno gli stati, le agenzie del controllo, le specializzazioni dei lavori, ma anche le condizioni economiche.

1.2 Marx e il controllo sul luogo del lavoro

Con l'avvento della rivoluzione industriale la stessa società cambia forma e diventa società industriale. Le trasformazioni come abbiamo detto riguardano tutta la sfera che essa occupa: le attività economiche tendono a differenziarsi maggiormente e si aprono verso nuovi mercati; l'organizzazione del lavoro per la manifattura cambia radicalmente e si passerà da un lavoro artigianale e privato ad uno svolto parzialmente in fabbrica; andranno a modificarsi le fonti di legittimazione del potere; il conflitto sociale anche vedrà emergere nuovi soggetti, gli operai, e la borghesia, che chiederanno nuove forme di partecipazione; il ruolo dello stato in quanto regolatore dello stesso conflitto sociale andrà mutando(Statera,1996). Per quello che ci interessa avviene una trasformazione fondamentale: la nascita del capitalismo.

Caratteristica di questa nuova formazione socio-economica è quella di basarsi su istanze razionalizzanti, dove nessuna cosa deve essere lasciata al caso, ma tutto deve essere frutto di calcolo. È l'inizio, grazie all'avvento delle macchine, del predominio della scienza sull'uomo.

L'avvento della classe capitalistica ha due importanti conseguenze. La prima è di carattere politico, la seconda sociale.

Nella politica assistiamo all'ascesa di questa nuova classe, che, avendo a disposizioni grandi risorse economiche, vuole essere anche rappresentata in maniera adeguata nelle sedi decisionali. In questo modo si va a creare una collisione fra il potere politico e quello economico ed emergono delle vere e proprie *elitè* di governo.

Nel sociale assistiamo alla ristrutturazione delle organizzazioni del lavoro. Ed è questo il punto che ci interessa da vicino.

La caratteristica della società industriale è quella di avere un'industria manifatturiera di tipo moderno che si basa su investimenti di capitale in grandi fabbriche. Queste fabbriche al loro interno sono caratterizzate dalla predominanza dei ritrovati della ricerca scientifica e dalla produzione in modo standardizzato. Per analizzare le trasformazioni che porta con se la fabbrica dobbiamo usare un testo fondamentale: *Il Capitale* di Karl Marx.

Secondo Marx esistono essenzialmente due tipi di divisione del lavoro: la prima è naturale, tipica della famiglia, della tribù, e si basa sulle differenze naturali di ciascun individuo; la seconda è la divisione economica del lavoro che è frutto di esigenze

economiche. L'analisi che lui compie si concentra nella stragrande maggioranza su quest'ultima e tende a considerare la fabbrica come punto centrale:

> L'operare di un numero piuttosto considerevole di operai, allo stesso tempo, nello stesso luogo (o, se si vuole, nello stesso corpo di lavoro), per la produzione dello stesso genere di merci, sotto il comando dello stesso capitalista, costituisce storicamente il *punto di partenza della produzione capitalistica*" (Marx,1867, Libro I2 p.18,corsivi nel testo).

È proprio la fabbrica che rende possibile tutto il processo. La tesi centrale di Marx è quella dell'alienazione dell'operaio. Prima dell'avvento della società industriale l'artigiano operava in una bottega per conto proprio o sotto padrone e aveva una serie di capacità individuali che gli permettevano di realizzare un determinato prodotto che successivamente avrebbe rivenduto. Con l'avvento della produzione standardizzata l'artigiano diventa operaio. Ora non ha più bisogno di avere determinate capacità individuali in quanto deve compiere solo pochi compiti sempre uguali, così diventa una parte della catena di produzione. In questo modo l'operaio si aliena dal prodotto stesso perché ne lavora solo una parte e perché il prodotto non gli appartiene (Marx, 1867).

Un'altra tesi sostenuta da Marx con vigore è quella dello sfruttamento e del controllo degli operai per mano del capitalista. Tutto ciò è reso possibile dalla fabbrica. È proprio grazie alla concentrazione degli operai sotto lo stesso tetto che è possibile appianare le differenze lavorative individuali in funzione di un principio produttivo medio ed uniforme. Questo rende possibile quella che lui chiama *legge di valorizzazione* anche perché i mezzi di produzione,

inseriti in un processo comune, vengono consumati da tanti individui e perciò i costi del capitale per il loro acquisto viene ammortizzato più rapidamente.

Lavorando molte persone una accanto all'altra a funzioni differenti, ma complementari, il cui fine è la realizzazione di un prodotto, la forma del lavoro cambia e diventa di tipo cooperativo. A questo cambiamento ne consegue un altro: c'è bisogno di una funzione di coordinamento, di direzione e di sorveglianza. Questa funzione viene svolta da principio dal capitalista. Ancora le parole di Marx riescono a spiegare a pieno la situazione:

> All'interno del processo produttivo di produzione il capitale si è sviluppato in *comando sul lavoro*,cioè sulla forza lavoro in attività, ossia sull'operaio stesso. *Il capitale personificato*, il capitalista, vigila affinché l'operaio compia il suo lavoro regolarmente e con il dovuto grado d'intensità (Marx,1867,Libro I, p.338,corsivi nel testo).

Una volta che però la massa degli operai si accresce si accrescono i contrasti all'interno della fabbrica. L'operaio che prima nella manifattura artigianale controllava il proprio lavoro ed acquisiva capacità manuali in grado di fargli svolgere appieno il processo produttivo, entrando in fabbrica perde tale capacità. Il lavoro diventa parcellizzato e l'operaio è solo un ingranaggio, schiacciato dalla scienza delle macchine, e sottomesso al potere del padrone. Per Marx questo fa diventare la fabbrica quasi una prigione, o una caserma, perché, nel momento in cui il capitalista da solo non riesce a controllare tutte le fasi della produzione, si crea una schiera di suoi subordinati a cui viene deputato il compito di sorveglianza. Questa specializzazione comporta una

divisione netta fra *operai manovali* e *sorveglianti del lavoro* che fa si che venga inaugurato il *regime di fabbrica* (Marx, 1867). Gli operai non possono opporsi e ritornare a compiere il proprio lavoro come prima perché, come nota Weber, i mezzi materiali che gli servono per poterlo fare sono nelle mani del capitalista (Weber, 1919).

Se la critica a Marx è quella di avere un 'ideale romantico del lavoro artigianale, la stessa critica non può essere fatta a Durkheim che è fra quelli che propongono una crescente divisione del lavoro per risolvere i conflitti della società. La sua solidarietà organica, tipica delle società moderne, si basa sulla funzionalità delle parti. Su individui che cooperino fra di loro in favore di un progetto comune svolgendo compiti diversi, ma complementari. Come Marx anche Durkheim trova che la società di tipo capitalistico a crescente specializzazione del lavoro siano negative. Dal Lago analizzando la devianza dice che:

> tra le forme anormali egli riconosce infatti le caratteristiche costanti del capitalismo, cioè le crisi economiche e l'antagonismo fra capitale e lavoro. Per Durkheim ad esempio è *anormale,*in quanto non implica solidarietà ma conflitto istituzionalizzato, la divisione tecnica del lavoro, cioè la fabbrica capitalistica (Dal Lago,1981,p.33).

E se Durkheim auspica la creazione di corporazioni, che siano differenti da quelle medievali presenti nelle città stato, con il compito di regolamentare i lavoratori e sappiano tutelare i propri interessi, avendo un peso politico all'interno del governo, Dal Lago evidenzia come proprio la regolamentazione sia fonte di tensioni e conflitti, mentre Weber sottolinea come le corporazioni non

possano essere un organizzazione politica adeguata in quanto tenderebbero a privilegiare solo i propri specifici interessi[2].

La fabbrica di Marx però non è il punto di arrivo. Se in essa è l'occhio la tecnologia di controllo, nel novecento verrà sostituito. La crescente razionalizzazione porterà l'ingegner Taylor a sviluppare un sistema di produzione in cui la misurazione dei tempi di lavoro di ciascun operaio per ciascuna operazione alla macchina avrebbe portato alla *best way*, ossia alla maniera unica e migliore per poter svolgere questa funzione. Questo avrebbe permesso una rigida pianificazione delle operazioni da compiere che sarebbero state legate a tempi specifici (Statera, 1996).

Con l'avvento della catena di montaggio ad opera di Ford il processo viene migliorato: l'operaio deve effettuare il suo compito nel tempo prestabilito pena l'inceppo della catena stessa. Si può vedere che il controllo in questi contesti non viene più effettuato attraverso l'occhio. È il criterio razionalizzante stesso che controlla l'operaio e lo costringe a non fuoriuscire mai dai binari che gli sono stati imposti. E, infine, lo sottomette ancora di più al padrone perché tende a svolgere compiti di routine. Dopo l'alienazione marxiana del prodotto abbiamo l'alienazione del lavoratore da se stesso.

[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).

Siamo convinti che la fabbrica non è stata creata solo per avere un maggiore controllo sugli operai, tuttavia, come Lyon, crediamo che questo, insieme alla tendenza alla massimizzazione dell'efficienza tecnologica delle macchine, siano i motivi basilari, e che quello che viene denominato come management “gestione aziendale” sia stato sviluppato essenzialmente per monitorare gli operai e fare in modo di disciplinarli (Lyon,1994).

1.3 La gabbia d'acciaio dell'apparato burocratico

Le istanze razionalizzanti fatte proprie dal capitalismo, fanno parte di un processo che coinvolge tutta la storia moderna. Ogni settore della vita subirà la loro influenza. La formazione stessa dello Stato occidentale, nella forma che conosciamo, è loro frutto. Questo comporta una grande trasformazione: la mutazione delle forme di potere.

Analizzando i cambiamenti delle società si è potuto vedere come da un tipo di governo totalmente incentrato sulla tradizione, si è passati ad uno in cui il governo è incentrato nelle mani di chi possiede le ricchezze economiche. Questo potere Weber lo ha definito di tipo tradizionale, ossia un potere che va a basarsi su antichi privilegi e ordinamenti di signoria (Weber, 1922). Colui che lo detiene non è un “superiore”, ma bensì un signore. Il suo apparato amministrativo non è composto da funzionari, ma da servitori. Servitori che occupano le diverse cariche in

funzione dei rapporti privilegiati che intrattengono con il signore e per scopi di giovamento personale. È un apparato che non può funzionare in uno stato moderno in quanto manca di: una *competenza specifica* del settore di cui ci si occupa; una *divisione funzionale dei compiti* fra i diversi organi amministrativi, in maniera tale da non permettere sovrapposizione o concorrenza fra di essi; una *gerarchia* fra le cariche occupate; uno *stipendio* fisso e stabile di modo che il funzionario amministrativo non possa entrare in possesso di beni arbitrariamente attraverso il proprio ufficio (Weber, 1922). Un apparato che, privo di tutto questo, basa la sua supremazia solo su privilegi.

La costante espansione della città, come abbiamo visto, avrà il suo culmine nella costituzione dello Stato. Uno stato che deve garantire l'ordine e la sicurezza a tutti i cittadini, gestire in maniera adeguata tutti i mezzi di comunicazione, decentrare i propri compiti diversificando i ruoli e le funzioni in maniera tale da essere presente in ogni angolo del territorio. Il potere diventa di tipo legale. Questo potere non può più basarsi su criteri particolari, ma deve basarsi sull'oggettività delle norme e sulla competenza di chi le fa rispettare.

La competenza, ossia il sapere specializzato, è il nodo centrale della trattazione di Weber sulla burocrazia. La competenza permette una gestione ottimale di ogni settore. Viene attuata una divisione dei diversi organi dello stato e ad ognuno viene assegnata una specifica funzione. Si crea una gerarchizzazione fra essi e fra i funzionari che vi lavorano e si procede ad una sistemizzazione dove ogni parte diventa

complementare all'altra. Il principio comune diventa il calcolo. Solo attraverso di esso è possibile avere una pianificazione ottimale, quantificare i beni, dividerli, amministrare in maniera imparziale. La creazione di una burocrazia all'interno dell'amministrazione è sicuramente il modo migliore per assolvere tutte le funzioni di uno stato moderno.

Weber sottolinea inoltre come lo sviluppo del capitalismo e della burocrazia vadano di pari passo. Il capitalismo per svilupparsi ha bisogno di un sistema che gli garantisca stabilità, mentre la burocrazia trova nel capitalismo la forma migliore per sostentarsi, infine entrambi basano i loro processi attraverso il calcolo. Questo processo non è però statico, ma dinamico. Sia in *Economia e società* che in *Parlamento e governo* viene evidenziato come la forma di organizzazione di tipo burocratico diventi la forma di tutte le istituzioni che operano all'interno dello stato. Chiesa, esercito, impresa capitalistica, fondazioni, gruppi di interesse, partiti, e così via, si basano tutte sui suoi stessi principi: divisione dei compiti in base alle singole competenze dei funzionari; principi gerarchici fra gli uffici e fra i funzionari ; assoggettamento alle norme da parte di chi comanda e assoggettamento di chi esegue non all'autorità, ma alla norma; divieto di appropriazione degli uffici.

Questo sviluppo comporta la formazione di una classe di plutocrati che domina sulla maggioranza della popolazione e, nell'ambito dell'apparato amministrativo, vuol dire la nascita di una classe di tecnocrati il cui sviluppo può comportare due grandi conseguenze. La prima è che

> l'amministrazione burocratica designa un potere esercitato sul sapere: questo è il suo specifico carattere razionale. Al di là dell'enorme posizione di potenza che il sapere specializzato comporta, la burocrazia…ha la tendenza ad accrescere ancora di più la sua potenza mediante la competenza acquisita nel servizio, cioè mediante le cognizioni dei fatti apprese nel corso del servizio"(Weber,1922, p.219 vol. I).

In secondo

> la burocrazia una volta che si sia realizzata costituisce una delle formazioni sociali più difficilmente abbattibili . La burocratizzazione è il mezzo specifico per trasformare un "agire di comunità" in un "agire sociale" ordinato razionalmente…essa è un mezzo di potenza di primissimo ordine per chi dispone dell'apparato burocratico (Weber,1922, p. 300 voll. II).

Si crea un apparato che tende ad allargare se stesso, che può diventare strumento politico di potere da parte di chi ne gestisce i vertici e che, fondamentale, non rappresenta né il potere politico né quello culturale (Statera, 1996). La soluzione per ovviare a questa crescita di potenza sta, secondo Weber, nella creazione, da parte del Parlamento, di un apposito organismo di vigilanza che attui un controllo sull'amministrazione di tipo burocratico (Weber, 1919).

Il problema non è il solo. Il sapere, il calcolo, la norma sono tutti aspetti che concorrono alla formazione della "gabbia d'acciaio". La razionalizzazione spinge l'individuo al conformismo, leva la creatività, costringe il funzionario a compiere compiti seguendo norme e modelli precostituiti. È fine di ogni lotta sociale in quanto l'istituzione contro cui

ribellarsi è una rappresentazione della società stessa (Weber, 1919).

La razionalizzazione non è un aspetto che invade solo ed esclusivamente le istituzioni, ma tende a propagarsi, come un virus, su tutta la società. L'individuo diventa schiavo di principi e compiti che invadono ogni aspetto della propria vita. La burocrazia composta di funzionari che detengono il *sapere*, basata su tecniche di archiviazione *scritta*, che vengono elaborate in maniera impersonale, rappresenta il sistema migliore per la gestione, ma al tempo stesso anche per il controllo sociale. Cosa c'è di più naturale di un sistema che agisce in maniera neutrale, senza preferenze, basato sul calcolo? Ma il sistema per funzionare, calcolare, prevedere, sapere, pianificare deve raccogliere informazioni. Deve gestire dati, deve sapere tutto di tutti. Deve costituire dei dossier.

Questo tipo di sorveglianza ha scopi di gestione e di mantenimento dell'ordine che sono fondamentali in uno stato di tipo moderno, ma permette al sapere e alla disciplina di fondersi (Lyon, 1994). La creazione dell'apparato burocratico non permette nessuna via d'uscita all'individuo, nessuna scappatoia, non accetta devianze. Il principio razionalizzante incasella sia lo spirito del funzionario che del cittadino. Non c'è via d'uscita a questo. Nodo cruciale in Weber che non trova soluzione. Ce n'è solo una. Il “dominato”, per difendersi dall'onnipresenza dell'amministrazione burocratica, può creare un'altra organizzazione come la stessa con il compito di sorvegliarla. Burocrazia contro burocrazia. Ma sarebbe del tutto inutile in quanto l'organo di contrasto avrebbe le stesse

caratteristiche dell'organo da contrastare (Weber, 1922).

L'organismo statale diventa sempre più oppressivo, ma non solo lui. Ogni settore della vita moderna, come abbiamo visto, si sviluppa secondo le logiche dell'apparato burocratico. Fabbriche, aziende, caserme, università, scuole, sono tutti settori che operano basandosi su un sapere nelle mani di pochi che opera in maniera discriminante, su un ordine gerarchico, e sulla raccolta continua di informazioni per prevedere ed effettuare politiche. In un discorso tenuto all'assemblea della Verein fur Sozialpolitik nel 1909 Weber ci avverte:

> è terribile pensare che il mondo potrebbe un giorno essere pieno di nient'altro che di piccoli denti d'ingranaggio, di piccoli uomini aggrappati a piccole occupazioni che ne mettono in moto altre più grandi… questo affanno burocratico porta alla disperazione… e il mondo un giorno potrebbe non conoscere nient'altro che uomini di questo stampo: è in un'evoluzione di tal fatta che noi ci ritroviamo già invischiati, e il grande problema non verte su come sia possibile promuoverla o accelerarla, ma sui mezzi - viceversa - da opporre a questo meccanismo, al fine di serbare una parte di umanità libera da questo smembramento dell'anima, da questo dominio assoluto di una concezione burocratica della vita (cit. in Ferrarotti, 1965,p.123).

Il dominio però si sviluppa in maniera tale che non ce ne accorgiamo. Non c'è più una sola autorità centrale, ma una serie di autorità che gestiscono e operano controlli in differenti settori. Questo tipo di controllo sociale sembra prediligere l'estensione all'intensità, ma permea ogni aspetto della nostra esistenza in maniera invasiva. L'apparato burocratico

attraverso i dossier raccoglie tutte le informazioni sul nostro vivere. Non viene percepito come un pericolo in quanto leggi e modelli, creati da loro, sono lì a dirci che tutto è giusto e corretto. Dopo l'occhio, il diritto e la routine, sarà il dossier la tecnologia del controllo.

1.4 La società disciplinare

Lo studioso che ha fatto del Potere il suo punto d'osservazione centrale è Foucault. I suoi scritti cercano di portare l'attenzione su tutti quei meccanismi, quelle istanze, che assoggettano l'uomo. Siano esse apparati di controllo rigidi, siano esse norme sociali non codificate che riguardino la sfera sessuale.

La migliore analisi dei rapporti di potere la troviamo in *Sorvegliare e Punire*, in cui Foucault, ripercorrendo le fasi storiche che hanno portato alla nascita della prigione, analizza i cambiamenti del potere. Il punto di partenza per il filosofo francese è che il potere tende ad essere esercitato sui corpi. E questo potere non deve essere considerato come una proprietà che viene detenuta da quella che è la classe dominante, ma bensì come una strategia che viene attuata da quest'ultima. Il potere non lo si possiede, il potere si esercita. Il potere travalica quella che è la classe dominante e investe anch'essa (Foucault, 1975). Come per Weber anche per Foucault il potere è in correlazzione diretta con il sapere. Su di esso si

fonda e trova tutti quei meccanismi che permettono di mantenere il controllo.

Nel suo scritto, per portare alla luce la situazione attuale della società, si porta l'attenzione sul cambiamento del supplizio. Fino all'inizio del diciottesimo secolo la punizione per i reati era pubblica, avveniva in piazza. Erano punizioni spettacolari. Avevano il duplice compito di punire il reo, vendetta della società sul deviante, ma soprattutto quello di rivolgersi a tutta quella popolazione che non aveva commesso reati (Ponti, 2001). Nei riti punitivi andava ad esercitarsi tutta la meccanica del potere.

> Di un potere che non solamente non nasconde di esercitarsi direttamente sul corpo, ma si esalta e si rinforza nelle sue manifestazioni fisiche.. di un potere che in mancanza di una sorveglianza ininterrotta, cerca il rinnovamento del proprio effetto nello splendore di manifestazioni eccezionali;di un potere che si ritempra facendo risplendere ritualmente la propria realtà di superpotere (Foucault, 1975, p. 62).

Ma questo meccanismo porta con se dei grandi svantaggi. La massa della popolazione chiamata in piazza a partecipare al supplizio si identifica non con il potere, ma con il condannato in quanto uomo del popolo. E così assistiamo alla nascita della prigione come luogo di espiazione della propria pena. Luogo in cui il reo può essere rieducato (Ponti, 2001; Foucault, 1975). L'opera dei riformatori reca con se anche il cambiamento della prevenzione del crimine. Le grandi bande vengono smantellate, e si cerca di isolare dalla popolazione tutta quella parte di delinquenza che era al suo interno creando un'altra popolazione composta da devianti. Viene creato un efficace apparato di polizia che ha il compito di monitorare ogni aspetto

della vita dei cittadini. Come sottolinea Foucault il riordino del diritto criminale deve essere letto come:

> una strategia per il riassetto del potere di punire,secondo modalità che lo rendano più regolare, più efficace, più costante e meglio dettagliato nei suoi effetti;in breve che aumentino gli effetti diminuendone il costo economico… ed il costo politico (dissociandolo dall'arbitrio del potere monarchico) (Foucault,1975, p. 88).

Si afferma un potere che va ad esercitarsi in maniera capillare su ogni singolo aspetto della vita. Con l'avvento della società capitalistica tutta la serie di illegalismi che era tollerata viene meno perché il potere deve preservare l'economia.Si fa strada quella che Foucault definisce come “teoria del contratto”: si presuppone che il cittadino abbia accettato le leggi imposte dal vivere in società, anche quelle che lo puniscono. Il criminale per cui diventa il nemico comune. Colui che ha violato un patto. Ha commesso un male contro l'intera società, per questo è necessaria la creazione di un apparato di polizia che non solo vigili e punisca i colpevoli, ma abbia anche il compito di prevenire il crimine. Polizia e carcere entrambe soddisfano quest'ultimo punto. Nel carcere abbiamo la formazione di un sapere sull'individuo fatta da un continuo monitoraggio su di lui. Il sapere che si crea ha lo scopo di far capire la pericolosità sociale dell'individuo. La sua propensione alla commissione di reati e così via.

Ma la tesi veramente centrale in Foucault è quella che vede la trasformazione della società. In analogia alla prigione si creano una serie di apparati che hanno come scopo quello di incasellare l'individuo dentro le maglie di un sistema già dato. Di un sistema che

continua a riprodurre se stesso ed i suoi meccanismi. Si va a creare un sistema di potere che non viene più visto come poteri di alcuni su alcuni, ma come reazione immediata di tutti nei riguardi di ciascuno (Foucault, 1975). Ma attraverso quali strumenti viene esercitato questo controllo capillare della società?

Qui entrano in gioco quelle che Foucault definisce come discipline. Ossia tutte quelle pratiche che cercano di assoggettare il corpo dell'uomo. Il controllo minuzioso dei suoi movimenti. E queste discipline si differenziano dal passato perché non sono semplici rapporti di sottomissione come potevano essere prima verso il re o il feudatario, come potevano e possono essere per il *pater familias*, sono forze che agiscono sul corpo sezionandolo, fornendogli un'attitudine ed una capacità, ma tutto già dato.

Le discipline agiscono sullo spazio restringendo il campo d'azione del corpo incasellandolo in un luogo. Si assiste alla creazione di caserme, di ospedali, di scuole, di associazioni, di fabbriche, dove ogni corpo ha una ed una sola funzione. Dove esistono regole di comportamento diverse da quelle della società che agiscono costantemente in misura assoggettivante verso l'individuo. Il principio di sorveglianza marxiano va ad applicarsi a tutti i settori della società. Il potere ha bisogno di conoscere in ogni istante il posto dove è ubicato l'individuo, la sua mansione e così via. Centrale in questo è che nelle discipline l'unità che tiene insieme i soggetti non è il luogo che si occupa, ma il rango, oggi diremo lo status, che un individuo occupa in relazione agli altri. È una sistema di differenze e scarti quello che tiene unite le discipline (Foucault, 1975). Come dice Foucault:

> La prima fra le grandi operazioni della disciplina è dunque la costituzione di “quadri viventi” che trasformino le moltitudini confuse, inutili o pericolose in molteplicità ordinate (Foucault,1975, p.160).

La disciplina va a formare un indidualità composta da quattro caratteri: cellulare, ogni corpo è inserito in uno spazio; organica, un compito assegnato ad ognuno; genetica, perché configura il perpetuarsi nel tempo della stessa attività; combinatoria, perché unisce le individualità in funzione di un obiettivo. E per compiere tutto ciò mette in scena quattro tecniche: costruisce dei quadri, prescrive delle manovre, impone deegli esercizi e organizza delle tattiche (Foucault,1975).

Il potere disciplinare in pratica serve ad “addestrare” la massa della popolazione. Il successo di questo potere deriva da tre strumenti: il controllo gerarchico,la sanzione normalizzatrice e l'esame (Foucault, 1975).

Il primo lo si costituisce creando spazi di visibilità completa. Dove nulla viene lasciato al caso. Fabbriche, strade, piazze, ospedali, e tutte le opere architettoniche vengono costruite in maniera tale da avere sempre la possibilità di vedere tutti i corpi. Si pensi a questo proposito all'eccesso di Brasilia. Una città costruita secondo l'utopia modernista dove nulla doveva essere lasciato al caso. Una città costruita non a misura d'uomo, ma per misurare l'uomo, dove non ci dovevano essere imprevisti, dove tutto è controllabile. Una città, come osserva Bauman, che fu ”uno spazio perfettamente strutturato per ospitare omuncoli, nati e allevati in provetta; per creature raffazzonate da

funzioni amministrative e definizioni giuridiche" (Bauman,1998, p.51). È sempre l'occhio la tecnologia, ma in questo la tecnologia subisce una modifica. Il controllo, la sorveglianza, come abbiamo visto per la fabbrica, viene attuata da agenti predisposti a questo compito, sono corpi che controllano altri corpi in base a differenze di rango. In questo contesto si crea una rete di relazioni che attraversa tutti i corpi, in cui anche tutti i sorveglianti sono sorvegliati. Anche se c'è un capo è tutta l'"organizzazione piramidale" a produrre potere. È la rete di relazioni che diventa tecnologia di controllo.

L'altro strumento di cui si serve il potere disciplinare è la sanzione normalizzatrice. All'interno di ogni luogo si creano delle proprie leggi. Le discipline hanno la caratteristica di riempire lo spazio lasciato vuoto dalle leggi codificate. Vanno a costituire un'"infra-penalità", vanno a reprimere o a qualificare una serie di comportamenti (Foucault, 1975). In questo contesto agisce un doppio meccanismo che è quello della sanzione-gratificazione, in maniera tale da poter addestrare a pieno i corpi. Grazie a questo metodo si crea una differenziazione dei corpi in buoni o cattivi, giusti e sbagliati. Dicotomie fondamentali. Così facendo si creano scale di valore degli individui non tanto in base alle capacità, ma in base al loro grado di assoggettamento all'ordine. In base al grado di *normalizzazione* che il corpo ottiene. Più si è vicini alla norma più si è considerati "bravi".

Infine l'ultimo strumento di cui si serve il potere disciplinare è l'esame. Quest'ultimo coniuga le tecniche della gerarchia che sorveglia e quelle della sanzione che normalizza. È una sorveglianza che

permette al potere di classificare i corpi. L'esame fa si che i corpi vadano a trasformarsi in oggetti, in numeri, dove ad ognuno di essi viene dato un punteggio. Si crea una documentazione scritta di ogni corpo che ha la duplice funzione di costituire l'individuo come oggetto descrivibile e , al tempo stesso, comparabile con gli altri. Così facendo la vita di un individuo viene incasellata in spazi, descritta minuziosamente, per poi poter essere riutilizzata in futuro. La descrizione diventa così un mezzo di assoggettamento (Foucault, 1975). Nell'esame troviamo la manifestazione completa che lega sapere e potere. L'uomo diventa calcolabile in tutti i suoi aspetti.

Una volta descritto questo Foucault passa ad analizzare il panottismo. Il Panopticon Benthamiano è una prigione lavoro a forma circolare dove i detenuti possono essere visti, ma dove i sorveglianti non si vedono mai. Dove il sorvegliato non sa mai quando e come viene visto. E questa insicurezza assoggetta il corpo dell'individuo alla Norma, alla regola. Naturalmente, come osserva Bauman, il Panopticon ha il grande inconveniente di legare nello stesso luogo e sotto lo stesso principio di potere, sia i sorveglianti che i sorvegliati (Bauman, 1998). Ma Foucault, a differenza di Bentham, non vede il Panopticon come uno spazio chiuso, ma come uno spazio adattabile e trasportabile all'interno della società. Uno spazio riproducibile:

> è il diagramma di un meccanismo di potere ricondotto alla sua forma ideale; il suo funzionamento, astratto da ogni ostacolo, resistenza o attrito, può felicemente essere rappresentato come un puro sistema architettonico e ottico: è in effetti una figura di tecnologia politica che si può e si

> deve distaccare da ogni uso specifico. Esso è polivalente nelle sue aplicazioni; serve ad emendare i prigionieri, ma anche a curare gli ammalati, istruire gli scolari, custodire i pazzi, sorvegliare gli operai, far lavorare i mendicanti e gli oziosi. È un tipo di inserimento dei corpi nello spazio, di distribuzione degli individui gli uni in rapporto agli altri, di organizzazione gerarchica, di disposizione dei centri e dei canali di potere, di definizione dei suoi strumenti e dei suoi modi d'intervento, che si possono mettere in opera in ospedali, fabbriche, scuole, prigioni (Foucault,1975, p.224).

Foucault vede la progressiva espansione di questi dispositivi disciplinari e pertanto arriva alla conclusione della creazione di una società disciplinare. Una società che poco a poco ha sempre meno bisogno di questi luoghi chiusi in quanto i loro meccanismi tendono a permeare ogni singolo aspetto del vivere quotidiano. La società disciplinare ha la caratteristica di non avere bisogno di incasellare gli individui in spazi chiusi. Le discipline omogeneizzano,rendono tutti uguali. In questo contesto vediamo che la disciplina stessa non va a configurarsi come un'istituzione o come un apparato, ma come un meccanismo per esercitare il potere. È la disciplina, con tutti gli strumenti che reca, la tecnologia del controllo (Foucault, 1975).

2. LIQUIDI, RETI, DATI

2.1 Società del controllo e nuova sorveglianza

Per approdare alla coercizione della società disciplinare, al suo grado di omogeneizzazione alla norma, i poteri hanno impiegato quasi mille anni, dalla nascita della città- stato fino al diciannovesimo secolo. Giunti al ventesimo abbiamo pensato che il sistema di controllo difficilmente potesse essere migliorato, ma ci sbagliavamo. Il nuovo secolo porta con se trasformazioni fondamentali nell'attività della sorveglianza, e si affacciano nuovi settori in cui applicarsi. Partiamo dall'inizio.

Le polizie di tutto il mondo incominciano a disporre di nuovi metodi d'investigazione, che vanno dalle impronte digitali alle macchine fotografiche[3]. Entrambi rappresentano strumenti in grado di marcare l'individuo, di segnarlo in maniera unica. Si fa strada l'idea che il corpo non possa soltanto essere un oggetto del controllo, ma rechi con se dati che permettano di essere identificato sempre. L'attività di polizia incomincia a spostare il baricentro delle sue attività dalla prevenzione attuata attraverso la visibilità verso quella basata sulla raccolta dati di ogni attività supportata da strumenti scientifici.

Ma quello che cambia veramente le carte in tavola è l'avvento di una nuova tecnologia: il computer.

[3] Si può vedere a questo proposito Virilio P., 1989.

Artefatto tecnico che non solo trasforma le attività umane, ma, configurandosi come *tecnologia caratterizzante* , riescie a modicare le strutture cognitive dell'uomo (Bennato,2002). La rivoluzione digitale trasforma la fabbrica fordista introducendo in essa macchine ad elevato grado di automazione, fa nascere nuovi settori prima sconosciuti. Si affacciano tutte quelle imprese che forniscono servizi, non più beni materiali tangibili, ma beni virtuali quali conoscenza e informazioni. Si afferma in sintesi quella che viene chiamata *information society*, una società in cui il bene di maggior valore sono proprio i dati. Il computer in questa nuova impresa ha il compito, come prima per il telefono, di mettere in comunicazione le varie parti, i rami dell'impresa stessa fra loro, e di gestire tutta la mole di dati (Lyon,1991; Bennato 2002). Il computer pertanto ha il compito,o meglio la capacità, di controllare e monitorare le varie attività.

Il cambiamento investe tutti settori, nasce quello che Bauman definisce *capitalismo leggero*: non più un modello di produzione basata sul luogo di origine dell'azienda, ma un modello di produzione delocalizzato, dislocato in ogni possibile parte del globo (Bauman,1998, 2002). I capitali diventano cifre che possono viaggiare in qualsiasi parte del globo. I capitalisti non hanno più bisogno di essere ancorati alla loro fabbrica, perché grazie al computer e alle reti telematiche possono essere presenti al suo interno ovunque essa sia. Ma per far questo hanno bisogno di monitare costantemente tutta la produzione, di sapere sempre dove ogni cosa sia, di seguire dall'inizio alla fine tutta la filiera produttiva. E tutto questo viene raggiunto creando sempre maggiori sistemi di

sorveglianza. Nulla può o deve essere lasciato al caso. Si fa avanti un controllo continuo ed ininterotto. E questo controllo non si estende soltanto alla produzione, ma trapela e valica ogni aspetto del quotidiano.

Come sottolineano gli studiosi di scienza politica, più uno stato ha rapporti di scambio con altri stati, più i cittadini sono liberi di muoversi, più interdipendenze si creano, maggiore è il controllo che lo stato deve avere sui suoi cittadini (Gritti,1999;Mongardini,2001). La libertà di movimenti, di scambi che offrono la crescente globalizzazione e le reti telematiche, scardina l'idea stessa di stato-nazione e l'unica possibilità che ha per mantenere salde le maglie della sua "catena" è quella di sapere sempre ogni cosa. Ancora una volta, e più del passato, si fa avanti l'idea che è proprio il sapere a costituire il potere (Foucault,1975). In questo contesto assistiamo ad un passaggio fondamentale: da una società disciplinare si passa ad una società del controllo (Deleuze,1999).

Questo cambiamento investe ogni ramo della società ed è tipico dell'epoca in cui viviamo. Un'epoca in cui sono finite le certezze per tutti. Bauman osserva a proposito che nei tempi passati un operaio che cominciava la sua vita alla Ford, era certo che l'avrebbe finita là dentro. Oggi invece questa rimane soltanto un'utopia per pochi. Il capitalismo leggero si disimpegna e lo stato-nazione demolisce il welfare. I cittadini rimangono inchiodati al suolo mentre i pochi, quelli che detengono i fili del potere, si muovono alla stessa velocità dei loro capitali. L'impresa sostituisce la fabbrica e a differenza delle società disciplinari dove un individuo non faceva altro che ricominiciare

sempre, prima la famiglia, poi la scuola, poi la fabbrica, nelle società del controllo non si finisce mai con nulla: “ la formazione permanente tende a rimpiazzare la scuola ed il controllo continuo a prendere il posto dell'esame” (Deleuze,1999,p.2).

Nella società del controllo i sistemi di disciplina chiusi, quali scuole e fabbriche, cedono il passo e si passa alla creazione di ambienti aperti, in cui in ogni luogo si può essere sorvegliati. Deleuze sottolinea come tutti gli ambienti in cui l'uomo passi siano moduli: tutti hanno le stesse caratteristiche e si riproducono in ogni settore. Non c'è più una differenza netta, delle leggi proprie per ogni ambiente, come nella società disciplinare. Il controllo diventa una modulazione, qualcosa che riesce a modificarsi da un settore all'altro apparendo sfumato e quasi invisibile (Deleuze, 1999). I corpi vengono lasciati in balia di se stessi senza avere più la certezza di niente.

In questo contesto si afferma quella che per primo Gary T. Marx ha definito come *nuova sorveglianza*. Caratteristica centrale di quest'ultima è quella di spostare la questione visibilità. Come abbiamo potuto notare, fin da principio, il sorvegliante non faceva altro che esibire e manifestare la sua presenza. I segni del suo potere e del controllo erano sempre visibili. Basti pensare alla magnificenza e alla collocazione del palazzo del signore o del vescovo, su alture in grado di controllare la piazza, alla presenza della polizia in ogni angolo della città. La stessa struttura del Panopticon era articolata mettendo in primo piano la visibilità. E se i sorveglianti erano invisibili i segni del controllo, della dominazione, erano sempre e comunque manifesti. Marx, Gary.T, invece ci fa notare

come la nuova sorveglianza sposti totalmente l'accento. Il potere scappa, e i suoi segni diventano meno visibili, coperti. Caratteristica della nuova sorveglianza è quello di non manifestarsi attraverso apparati o quando lo fa ed è palese, pensiamo alle videocamere, tende a celarli, a mimettizzarli. L'occhio stesso, senso di controllo per eccellenza, cede il passo e viene affiancato da nuovi sensi. La nuova sorveglianza sfrutta ed analizza ogni senso. Le conversazioni si sentono e si analizzano. Le modulazioni della voce vengono registrate per diventare chiavi d'accesso, il tatto diventa un'impronta, un segno. Il corpo stesso non è più solo visibile o misurabile antropomorficamente (Marx,G.T, 1999). Il corpo diventa un insieme di dati con caratteristiche biometriche uniche per ogni individuo. Il corpo non è più soltanto l'oggetto del discorso del controllo, ma diventa lo strumento attraverso il quale entriamo nella società dell'informazione. Il corpo diventa la password d'accesso ai vari settori che regolamentano la nostra esistenza (Deleuze, 1999; Marx, G.T., 1999; Lyon, 1994, 2001).

Marx analizza il cambiamento avvenuto a cavallo fra i due secoli e ci porta al motivo per cui il controllo cambia. Prima la raccolta dati serviva allo stato per amministrare la nazione, bisognava sapere quanto si doveva pagare di tasse, chi erano i poscritti alla leva, chi dovesse beneficiare di assistenza pubblica e così via. Nel nostro secolo invece si fanno strada nuovi settori in cui viene richiesta la raccolta dei dati. Assicurazioni, cliniche private, agenzie commerciali, hanno tutte bisogno di sapere sempre maggiori cose sugli individui. La diminuzione dell'interazione faccia a

faccia in favore di altre mediate dal computer o da altri strumenti tecnologici comporta la formazione di un'identità, di caratteri di riconoscimento, di cui le aziende, e gli stati hanno necessariamente bisogno.

Questa nuova sorveglianza si applica quindi ad ogni singolo aspetto del vivere e in molti casi è proprio il sorvegliato che fornisce volontariamente i mezzi del controllo. Pensiamo alle carte che ci permettono di ottenere sconti o simili. Si afferma un monitoraggio continuo dei nostri dati.

2.2 La dataveglianza

L'odierna globalizzazione che stiamo vivendo attraversa tutti i settori della nostra esistenza: dalle telecomunicazioni agli scambi commerciali, dal transito dei migranti alla delocalizzazione delle imprese. Questo processo che per molti versi soltanto ora, nelle cronache degli ultimi anni, appare essere non lineare, in realtà non lo è mai stato. Quello che ci hanno reso evidente e palese gli ultimi sviluppi però evidenzia una delle principali cause della crescente sorveglianza: la *Modernità liquida*, è un'epoca che si fonda sull'incertezza e sul rischio. Tutti i sociologi, siano essi BecK, Giddens, Bauman, Lyon, Castells, solo per citarne alcuni, convertono sulla constatazione che quest'epoca si fondi sull'incertezza. Sul dubbio. Crollano tutti i sistemi di valori che hanno sempre fatto da guida all'uomo: lo stato-nazione che aveva sconfitto la comunità si scardina cedendo il passo ad organismi

internazionali; la fabbrica che aveva accolto le masse dell'ottocento si disperde in ogni luogo del globo in base ad interessi economici; la famiglia, da sempre centro dell'individuo, si dissolve; la cultura popolare prima e nazionale poi, sfuma fino a con-fondersi con un miscuglio di altre; le grandi religioni perdono la loro capacità d'attrazione per le masse e si ripiegano nei grandi fanatismi. L'individuo si perde e sembra diventare davvero soltanto uno. La personalizzazione delle relazioni sociali, delle attività, dei sistemi culturali di riferimento, sembrano essere i fenomeni maggiormente significativi degli ultimi anni. Tutto questo si tramuta in incertezza, in insicurezza. Questo vale per l'individuo, ma di riflesso, anche per chi governa l'individuo stesso.

Lo stato si trova scisso fra il suo progressivo smantellamento e l'esigenza e il bisogno che questo non avvenga. Le aziende devono fari i conti con un mercato mondiale in cui ogni minimo cambiamento nei rapporti geo-politici comporta una ripercussione in ogni settore. Da ciò deriva l'esigenza di prevenire ogni situazione, di sapere sempre prima degli altri ciò che potrebbe avvenire. Formulare ipotesi, calcolare rischi. Si fa strada proprio una politica del rischio che prevede di avere maggiori informazioni su ogni cosa in maniera da pianificare le attività. Questo si traduce in prevenzione del crimine da parte degli apparati di polizia, e in marketing per le aziende. E la sorveglianza si accresce in ogni settore.

Uno dei primi studiosi ad occuparsi dei problemi relativi alla crescente informatizzazione della società fu Roger Clarke. In un articolo, divenuto oramai celebre, *Information technology and dataveillance*,

coniò proprio il termine di dataveglianza per indicare la crescente diffusione di database che immagazzinavano, ed immagazzinano, informazioni, dati, relativi agli individui.

Clarke parte dal presupposto che “ la sorveglianza è uno degli elementi della tirannia” (Clarke,1987, p. 2, trad. mia), incentrando così da subito l' attenzione sull'aspetto problematico della sorveglianza stessa. Nel suo studio la intende come:

> la sistematica investigazione o monitoraggio delle azioni o delle comunicazioni di una o più persone. Cui scopo primario è, generalmente, collezionare informazioni su loro, le loro attività o le loro associazioni. E, potenzialmente, il secondo scopo è quello di dissuadere l'intera popolazione dall'intrapendere determinati generi d'attività (Clarke,1987, p. 3, trad. mia).

L'attenzione qui deve essere posta su una delle parole che Clarke usa. La sistematicità della sorveglianza ci fa capire che essa permea ogni aspetto del quotidiano, espletandosi attraverso diverse modalità che spaziano dai sistemi di audio e videosorveglianza, fino ad approdare ai sistemi computerizzati. In questa maniera si va ad effettuare una vera e propria raccolta di dati sulle persone e proprio quest'attività prende il nome di *dataveglianza*:

> Il sistematico uso di sistemi di dati personali nelle investigazioni o nel monitoraggio delle azioni o delle comunicazioni di una o più persone (Clarke, 1987, op.cit. p. 3, trad. mia).

Per l'autore esistono due tipi diversi di sorveglianza.

La prima è quella personale che prevede via sia un rapporto, una relazione diretta, fra l'organizzazione che sorveglia e l'individuo. Mentre la seconda è quella di massa che tende ad applicarsi a gruppi di persone ad associazioni, senza bisogno di relazione diretta (Clarke,1987). Nel primo caso il rapporto con l'organizzazione può spaziare dall'essere cittadini di uno stato, per cui il controllo verterà sui pagamenti delle tasse o simili, all'essere clienti di una banca, per cui il monitoraggio riguarderà le transazioni, all'acquistare con carta di credito, allora le informazioni prelevate riguarderanno le preferenze d'acquisto.

Per la sorveglianza di massa invece il controllo tralascia la sfera individuale ed entra in quella collettiva: tutti vengono controllati e categorizzati in determinate tassonomie di individui. Portando così alla creazione di gruppi di individui "sospetti", a cui, come vedremo in seguito, si applicherà un diverso tipo di controllo (Bauman,2002, Lyon,2001), oppure, in ambito commerciale, alla creazione di statistiche.

Viene osservato come la crescente diffusione delle nuove tecnologie comporti una maggiore dipendenza dalle informazioni che si possiedono. In maniera sempre crescente si afferma il collegamento fra computer, come strumento d'elaborazione, e le comunicazioni, che permettono lo scambio dei dati. Gli stati, le aziende, hanno sempre maggiore bisogno di essere a conoscenza di ogni aspetto che riguardi gli individui. In questo contesto una tecnologia come l'*EFT* (*Electronic Found Transfer*), che verrà esaminata nello specifico nella seconda parte del volume, che serve per trasferire fondi da una parte all'altra, può essere presa a modello per spiegare il

funzionamento del sistema. I collegamenti necessari allo scambio dati fra le banche sono gli stessi che vengono utilizzati per permettere alle società aeree di monitorare il traffico, alle polizie urbane di identificare i veicoli, per schedare i criminali, alle amministrazione per registrare i cambiamenti anagrafici, al fisco per prelevare le imposte, alle aziende per dispensare premi fedeltà. Tutto questo, e qui il punto centrale, reso possibile dalla creazione di database che raccolgono tutte le informazioni e le smistano da una parte all'altra dei sistemi (Clarke,1987).

È proprio lo sviluppo dei database che per Clarke rappresenta un vero e proprio problema. E se anche nota come siano preoccupanti la creazione di database immensi come quello che hanno gli U.S.A sui loro cittadini, a cui le diverse agenzie statali possono attingere, sottolinea come la creazione di una società della sorveglianza non abbia bisogno di centralizzazzione , ma soltanto di:

> una gamma di gestione dei dati personali, collegati da reti di telecomunicazione, dotati di uno schema di identificazione compatibile (Lyon,1994, p. 74).

Infatti i sistemi decentralizzati sono maggiormente economici degli altri. Inoltre le diverse agenzie, siano esse statali o commerciali, tendono a scambiare i dati fra loro non facendo altro che aumentare le informazioni raccolte su ciascun individuo. Altro aspetto rilevante è che tutte le pratiche di raccolta e archiviazione procedono attraverso procedure routinizzate.

Tuttavia, sottolinea Clarke, lo scambio dei dati attualmente non riesce ad essere pienamente

sviluppato. Il motivo di questo risiede nei differenti modi in cui i dati vengono archiviati. In alcuni casi assistiamo all'assegnazione, da parte di alcune organizzazioni, di un codice alfanumerico che identifica un individuo, in altri casi agli individui vengono lasciati il nome ed il cognome e in altri gli si aggiungono le date di nascita. Tutto questo genera confusione fra gli algoritmi dei diversi sistemi e non permette il pieno scambio dei dati (Clarke,1987). A tutt'oggi si cerca di sviluppare un sistema *UPI* (*Universal Personal Identifiers*) che sia condiviso da tutti e non solo da un singolo stato o azienda. Le recenti tendenze sembrano voler convergere su un sistema di identificazione personale basato su Dna. Se avvenisse una cosa del genere ci troveremo di fronte a quello che Lyon definisce come il sogno della "dataveglianza".

Il vero problema però è quello che avviene all'interno dei database. Questo punto tocca da vicino altri studiosi oltre a Clarke. Proprio Poster in *The Mode of Information*, sottolinea l'immenso potere che questo possiede. Per l'autore il database impone nuove modalità di dominio sugli individui. Il suo compito non è solo quello di raccogliere dati, ma quello più specifico di mettere questi dati in relazione fra di loro. In questa maniera l'informazione raccolta viene suddivisa in categorie o campi che sono definiti in maniera rigida. L'esempio che l'autore ci fa è riscontrabile quotidianamente nelle nostre vite. Quando ci troviamo di fronte ad un modulo riempiano dei campi che per noi non hanno nessuna relazione fra loro. Ma in questo caso la relazione non deve esserci fra i dati raccolti, bensì fra i valori che a quei

campi vengano assegnati. Così leggere un determinato quotidiano o periodico viene assocciato ad una scala di valori diversa per ciascuno:

> la struttura o la grammatica dei database crea le relazioni fra parti di informazione che non esistono in quelle relazioni che sono al di fuori del database. In questo senso i database formano gli individui manipolando le relazioni fra porzioni d'informazione (Poster,1990, p.76).

Il potere del database risiede pertanto nella capacità di formare da una parte aggregati di dati utilizzabili per ricerche di mercato o altro, e dall'altro nella creazione di una *data-image* di un individuo. Cos'è lo vediamo subito.

2.3 Alter-ego virtuali

Lo stato assorbe informazioni sugli individui, le loro date di nascita, i loro studi, i loro beni, le combina fra di loro aggregandole in dati. Dati che vengono classificati, introdotti in matrici ed analizzati. Ricombinate escono fuori sotto forma di: *devianti*, *pericolosi socialmente*, *asociali*, *antisociali*, *socialmente integrati*, per gli apparati di polizia; *pagatori*, *moros*i, *evasor*i per gli apparati fiscali; *progressisti*, *reazionar*i, *rivoluzionari*, *antagonisti*, *moderati*, per quelli politici. E di seguito per tutti gli apparati.

Le aziende cercano di scoprire le tendenze in atto, cercano di prevedere dove vadano i gusti del

consumatore, per poter indirizzare le sue scelte. Promettendo sconti, offerte, regali, raccolgono dati. Li immagazzinano e li convertono, come per magia in : *delfini*, *avventati*, *accorti*, *ese*cutori, oppure in *impegnati*, *radicals*, *frugali*, *benpensanti*[4] .

Altrettanto avviene nei luoghi di lavoro, nelle scuole ed in ogni settore.

L'individuo in base al *ruolo* che occupa in determinato contesto, rientra in una precisa tassonomia, ottenuta attraverso i dati in possesso del sistema di riferimento. Attraverso la combinazione degli stessi si crea una *data-image*, come la definisce Gary T. Marx, dell'individuo. Un alter-ego virtuale del soggetto. Non un corpo, ma una forma incorporea ottenuta attraverso la combinazione di numeri.

Proprio questa sparizione del corpo fisico è centrale nella tesi di Lyon. È in questa nuova forma del corpo, in questo processo che sta alle spalle dell'individuo che risiede la vera novità e, quindi il carattere ploblematico, della sorveglianza. Infatti per lui l'invisibilità che la nuova sorveglianza introduce non è tanto quella fisica, la sparizione dei sistemi di sorveglianza, come per Gary T. Marx, ma soprattutto quella che sta alla base di tutti i processi di classificazione, di categorizzazione sistematica che sono effettuabili (Lyon,2001). Per l'autore da un lato ci troviamo di fronte all'avvento di una società in cui

[4] Sono alcune delle tassonomie che vengono usate da alcuni istituti di ricerca sui consumi.

> le pratiche di sorveglianza tendono sempre più a basarsi su astrazioni, anzichè su persone concrete. La “data-image” ricavata da un assemblaggio di comportamenti registrati è cio che conta. In un mondo mobile che si muove rapidamente, i nostri modi di interagire socialmente sono sempre più astratti e le pratiche di sorveglianza cercano di restare al passo coi tempi. Esse ci localizzano,ci puntano, tentano di coordinare le nostre attività (Lyon,2001,p.35).

Dall'altro lato ci troviamo di fronte a strutture di dominio che sono invisibili:

> Le società sorvegliate del ventunesimo secolo dipendono da una complessa rete di tecnologie d'informazione e di comunicazione. La rete non è visibile, ma supporta ogni tipo di monitoraggio, inclusa la sorveglianza video, quella satellitare e la biometria (Lyon,2001, p.37).

Per Lyon uno dei problemi centrali riguarda proprio l'arbitrarietà dei giudizi che possono venir fuori da questi dati. Perchè il soggetto reale, l'individuo in carne ed ossa, è sempre all'oscuro di ciò. E lo *status* che possiede l'alter-ego virtuale dell'individuo, agisce condizionando l'esistenza reale dello stesso. Riprendendo lo studio di Gary T. Marx sui metodi di polizia, lo accresce fino a svilupparlo all'intera società.

Marx aveva notato come la polizia per le sue indagini si trovasse sempre indirizzata verso determinati tipi di individui in quanto essi venivano definiti come dei "sospetti categoriali". Tutte le persone con un determinato reddito, che vivevano in determinate zone, con determinate caratteristiche andavano a confluire in un database che li indirizzava come primi sospetti per determinati tipi di reato (Marx G.T., 1985). Questo metodo da Lyon viene ampliato. La categorizzazione crescente degli individui, va a

determinare zone d'esclusione e di inclusione. In questa maniera la sorveglianza diventa uno strumento di regolamentazione sociale. Può decidere chi e come può entrare in determinati luoghi e con quale status, e il problema si accresce pensando che tutti i sistemi di classificazione sono totalmente automatizzati. La sorveglianza per Lyon diventa veramente problematica allorchè agisce come uno strumento di selezione sociale (Lyon,2001).

Le telecamere installate nelle città consentono di avere il controllo delle masse e al tempo stesso, come avviene nella city londinese, non permettere a chi non può di stare in determinati luoghi. L'elitè si costruisce i propri recinti in zone in cui non è permesso l'accesso ad altri (Bauman,2002). Le aziende ricorrono sempre più spesso a metodi d'analisi verso i lavoratori per scoprire la possibilità di malattie genetiche o simili, e si profilano tecniche di biosorveglianza per capire quali sono i soggetti maggiormente a rischio da altri, per tutelare l' azienda e le compagnie assicurative (Lyon,2001;) . Le carte fedeltà diventano strumenti di marketing ed il consumatore diventa il bersaglio di campagne mirate (Castells,2002;Lyon ,2001).

Lyon inoltre ci spiega il perchè tutto quello che sta avvenendo non può considerarsi non preoccupante, evidenziando come tutto ciò che facciamo venga controllato e finisca in database: dalle telecomunicazioni, alle nostre spese, alle nostre cartelle mediche,alle nostre valutazioni scolastiche (Lyon,1994;2001).

I profili che da questi dati possono essere ottenuti non siamo noi. L'individuo non è formato da ciò che compra, che guarda, che mangia, che fa. L'individuo

possiede un'interiorità che gli è propria. I filosofi direbbero che possiede un'essenza (forse che ne è alla ricerca). Mentre per coloro che possiedono i nostri dati siamo soltanto un numero, un codice identificativo, a cui è corrisposta una categoria e a cui questa categoria corrisponde ad un determinato atteggiamento da manifestare nei nostri riguardi. Nella raccolta dati di tipo moderno si ripropone lo stesso sistema di assoggettamento che Foucault aveva individuato per l'esame: la descrizione. È essa infatti che permette l'accrescimento del Sapere sugli individui (Foucault,1975).

Inoltre come evidenzia Gary. T. Marx si può rientrare ad essere un "sospetto categoriale" solo perchè si possiedono determinate caratteristiche, siano anche solo fisiche (Marx G.T,1985). La sorveglianza reca con se quindi un potere discriminatorio immenso. Maggiore pensando che tutte le nostre società si stanno sviluppando verso quelle che Lyon definisce società sorvegliate. Cosa sono?

2.4 Gabbie

Le società attuali vengono considerate società dell'informazione. I processi gestionali, sia che si parli di un'impresa di piccole dimensioni sia che si tratti di apparati burocratici statali, vengono svolti attraverso l'utilizzo di sistemi computerizzati. Così avviene per le transazioni economiche, per lo scambio delle informazioni, per le telecomunicazioni in genere. Tutto

ciò comporta un passaggio di dati fra i vari computer, in tutte le parti del globo, che rappresentano una mole di dati talmente ampia da non poter essere misurata con precisione. Ogni singolo dato viene raccolto. Indipendentemente dall'utilizzo che ne venga poi fatto, i dati vengono immagazzinati. Tutto ciò per alcuni studiosi comporta l'affermarsi di una società in cui la sorveglianza non solo sia un aspetto rilevante del vivere, ma sia la base stessa[5]. Arrivando a sostenere che

> pochi dubbi possono sussistere circa il fatto che la sorveglianza sia oggi da considerarsi come il mezzo essenziale dell'ordine e delle orchestrazioni sociali. Le società dell'informazione sono società sorvegliate. I mezzi di gestione sociale attualmente disponibili e in uso servono in varia maniera a classificare, coordinare e controllare le popolazioni in modi che trascendono le più moderne divisioni fondate sulla posizione di classe o sui processi burocratici di classificazione basati sulla documentazione cartacea. Iniziamo solo ora a capire come i profili biografici, le informazioni inerenti alla popolazione e i dati biometrici stiano emergendo quali fonti dinamiche di potere nel mutato ambiente sociale globale. Di quanto essi rafforzino i già esistenti progetti (in particolar modo di tipo capitalistico), e quali effetti essi abbiano sulle già presenti divisioni basate sul reddito, il genere, il carattere etnico e l'area geografica di provenienza, dev'essere ancora indagato. Ma è perfettamente chiaro che i flussi di dati relativi alla sorveglianza sono cruciali rispetto alle condizioni di esistenza di tutti coloro vivono nelle odierne società globali dell'informazione (Lyon, 2001, p.13).

[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).

Inoltre grazie all'utilizzo della rete sembra configurarsi un "nuovo ambiente di polizia globale" che possa minacciare le più comuni libertà come quella della libera manifestazione del proprio pensiero (Castells,2001). Pensando così, ci sembra di stare seduti su un divano con in mano un libro con sopra scritto *1984,* o di stare a guardare un film che parla di matrici, di illusioni. Davvero si sono avverate le distopie Orwelliane? Le visioni di Dick?

Su questo punto gli studiosi si trovano discordanti. Tutti avvertono il problema, ma la struttura che ha il *sistema sorveglianza* appare diversa per ognuno di loro.

La maggior parte di essi ripropone il modello foucaultiano di Panopticon. Analizzandolo precedentemente abbiamo visto come per Foucault il Panopticon non rappresenti una figura architettonica come per Bentham, bensì sia un dispositivo qualunque in grado di sottomettere gli individui alla Norma. Di agire su di loro quale strumento disciplinante. Pertanto non basato sulla coercizione fisica a cui sarebbero stati soggetti i detenuti del carcere benthamiano, ma su una coercizione basata sulle norme. Come nel Panopticon si sarebbero osservati i più piccoli cambiamenti del detenuto in maniera tale da poterlo "rieducare", così, nelle società discliplinari, la conoscenza sugli individui si trasforma in una forma di dominio sugli stessi (Foucalt, 1975).

Proprio l'aspetto linguistico presente in Foucault viene ripreso da Poster per analizzare le attuali forme di dominio. L'autore sostiene che nelle società moderne è il *discorso/pratica* che prende la forma del regolamento, che assoggetta l'individuo alla norma.

Riportando l'analisi foucaltiana ai giorni nostri l' associa ai database. Analizzando il linguaggio da essi utilizzato osserva come la pratica di classificazione del database sia priva di tutte le caratteristiche di ambiguità del linguaggio parlato, perchè si basa su un linguaggio binario che elimina i "rumori". Inoltre il database impone di ordinare i dati secondo classificazioni di tipo rigido. L'accresciuta esigenza di avere sempre maggiori informazioni sugli individui, mutuata dal Panopticon, una volta entrati nelle società informatiche, impone che i database crescano in maniera esponenziale. Per Poster questo porta alla creazione di un *SuperPanopticon,*ossia:

> un sistema di sorveglianza senza muri, finestre,torri o guardiani...la popolazione è stata disciplinata alla sorveglianza e a partecipare al processo. Le tessere sulla sicurezza sociale, le patenti, le carte di credito, le tessere per la biblioteca. Ogni transazione è registrata,codificata ed aggiunta ai database (Poster, 1990, p.83)

Questo *SuperPanopticon* registra le informazioni secondo il linguaggio che gli è proprio, pertanto impone nuove modalità linguistiche, ma, soprattutto va a costituire nuovi tipi di soggetti. Va a costituire quegli alter-ego virtuali di cui abbiamo parlato in precedenza. Dei *Super-sè* come li chiama Poster. Il database in se per l'autore non è una minaccia, ma è proprio nel soggetto creato che risiede la problematica. In questa moltiplicazione dei sè del soggetto che agiscono sull'esistenza reale dello stesso condizionandola. Pertanto per Poster sono proprio i database a regolare gli individui e a definirne i devianti e il *SuperPanopticon* diventa un mezzo per controllare la massa nell'odierna società (Poster,1990).

Ripartendo dal concetto di Poster un altro autore ripensa il concetto di Foucault . Baumann in *Dentro la globalizzazione*, analizza la teoria di Poster e non si trova d'accordo. Per il sociologo il *Superpanopticon* è un sistema a cui noi ci assoggettiamo volontariamente. Invece di essere uno strumento di dominio lo considera uno strumento di selezione perchè entrare a far parte di quel mondo significa entrare a far parte della classe dei "globali" come li definisce. Una classe che ha la possibilità di abbattere le categorie di spazio e di tempo e che rappresenta la nuova classe dominante. Pertanto il database per Baumann è soltanto uno strumento di accessibilità per determinati ambiti, serve a regolamentare chi può e chi non può entrare in un luogo. Per Baumann è più efficace un'altra metafora per spiegare le nuove forme di dominio, quella del *Synopticon*, presa a prestito da Mathesien. Il *Synopticon* è un'apparato in cui i pochi guardano i molti, e questo per Baumann è l'esempio lampante di quello che stiamo vivendo (Baumann,1997). Per l'autore pertanto

> l'ubbidienza agli standard tende ad essere raggiunta attraverso la lusinga e la seduzione anzichè la coercizione, e si mostra mascherata da esercizio del libero arbitrio anzichè rivelarsi come forza esterna (Bauman,2000, p.92) .

Quello che sfugge all'analisi baumaniana è che il *SuperPanopticon* non si limita a rendere possibile l'accesso a determinate zone, ma categorizza gli individui facendoli diventare oggetti del discorso e non permettendo di sapere agli stessi nulla su questa categorizzazione. Il modello del *Synopticon* può apparire valido nell'ambito dei massa media, ma risulta

essere un modello privo di fondamento nelle analisi sulla sorveglianza.

Tuttavia va riconosciuto a Bauman il merito di aver tracciato con chiarezza il funzionamento dei sistemi di sorveglianza. Infatti nota come alla massa dei globali si applicchi il tipo di controllo di cui parlato, mentre per la massa dei locali, dei diseredati, si applichi un controllo ancora basato sulla coercizione. Nella sua analisi sulla società moderna vede come le attuali costruzioni architettoniche e le soluzioni urbanistiche non facciano altro che relegare ai margini della società le fette di popolazione maggiormente svantaggiate. Su queste si tende ancora ad esercitare, come notato anche da Lyon, un controllo coercitivo di tipo panottico (Bauman, 1997;2000).

Lyon invece tende a scartare entrambe le ipotesi. Non prende nemmeno in considerazione quella di Bauman, e vede quella di Poster come un punto di partenza. Per l'autore non ci troviamo di fronte alla creazione di un Grande Fratello mondiale, o di un dispositivo unico che genera dominio e controllo. È soltanto nella molteplicità in cui la sorveglianza è messa in atto, nelle sue diversità che possiamo cogliere appieno la portata delle trasformazioni che stanno avvenendo. Il problema dei corpi che scompaiono, l'alter ego-virtuale, risulta centrale per Lyon, ma è anche centrale la ricollocazione nello spazio fisico dei corpi reali. Nella crescente videosorveglianza e nelle recenti tecniche biometriche sono annidati fantasmi ancor più pericolosi perchè fantasmi rimangono. Pertanto Lyon può arrivare a parlare di un"orchestrazione sociale". Utilizzando la metafora dell'orchestra vede che nell'attuale

condizione può esistere un direttore, che in questo caso sono i codici della rete, che può definire le linee guida, ma i musicanti sono diversi e disparati e anche noi ne facciamo parte ogni volta utilizziamo i nostri dati per fare acquisti o simili. Per Lyon quindi quello che avviene è più un'improvvisazione jazz piuttosto che un concerto classico. Il Grande Fratello orwelliano non sembra profilarsi all'orizzonte perchè. ad oggi, sembra non esserci un centro unico di controllo e gestione (Lyon,2001).

Questa tesi viene condivisa anche da Castells, il quale dichiara che

> la questione non è la paura del *Grande Fratello* perchè, in realtà gran parte di questa sorveglianza non avrà per noi nessuna diretta o indiretta dannosa conseguenza. L'aspetto più preoccupante è la mancanza di regole esplicite e comporta il pericolo che il nostro comportamento possa essere giudicato o interpretatato da parte di una varietà d'attori che stanno dietro la nosta casa di vetro. Non è il grande fratello, ma una moltitidine di piccole sorelle che registrano per sempre il nostro comportamento e formano un database che accompagna la nostra vita, a partire dal nostro Dna alle nostre caratteristiche personali. Negli stati autoritari questa sorveglianza può colpire direttamente le nostre vite (Castells,2001, p.172, corsivo nostro).

Ma la maggior parte della sorveglianza elettronica va a fondare gli ordinamenti democratici, e in questo tutti gli autori convergono. Se la distopia di Orwell potrà trovare applicazione non necessiterà di uno stato autoritario.

Ora ci rimane da capire attraverso quali strategie e tecniche la sorveglianza si espleti e le tecnologie che utilizza. Nei prossimi capitoli è proprio quello che analizzeremo.

PARTE SECONDA STRATEGIE

3. THE LEVIATHAN

"Il punto è che oggi in America qualsiasi gruppo o organizzazione, per il semplice fatto di operare sotto la copertura di un'espressione come Libertà di Stampa o Sicurezza Nazionale o Lega Anti-Sovversione, può postulare a suo favore la completa immunità riguardo alla violazione dell'individualità di chiunque non sia a sua volta membro di un qualche gruppo o una qualche organizzazione abbastanza potente da far spaventare e tenere tutti alla larga"

W.Faulkner, *Privacy*,1955

3.1 Lo Stato leggero

Lo stato-nazione è la formazione che governa le nostre esistenze. Tutti noi alla nostra nascita acquisiamo una cittadinanza e dei privilegi politici, e siamo sottoposti ad una serie di vincoli che ci permettono di esercitare dei diritti.

Ci sottominiamo a determinati doveri, a determinate norme, sapendo che i privilegi che ne riceviamo in cambio sono maggiori rispetto alle limitazioni dei nostri comportamenti. Quello che quotidianamente noi facciamo è cedere parte della nostra libertà in funzione di una stabilità che altrimenti non avremmo.

Lasciamo che sia l'apparato militare dello stato ad avere il monopolio della violenza per non dover sottostare alla legge del più forte. Lasciamo allo stato il diritto di prelevare parte dei nostri stipendi per far si che esso possa costruire e mantenere tutto ciò di cui

ha bisogno, attraverso le imposte, e far si che esso gestica le nostre pensioni, attraverso i contributi.

Lo stato-nazione per poter gestire se stesso ha bisogno, pertanto, di avere il controllo della popolazione al fine di coordinare la sua attività per poter rispondere alle esigenze della popolazione stessa. Lo stato deve sorvegliare la sua popolazione. Tutto questo non è soltanto giusto, ma è necessario. Lo stato avrà pertanto bisogno di sapere quali sono i suoi obiettivi e come fare per raggiungerli. Deve definire strategie. Una economica, una politica, una ambientale e ognuna in base alle sue diverse aree di interesse.

La prima che esso deve sviluppare è quella che definiamo come *strategia normalizzatrice*: lo stato deve emanare una serie di leggi, che sanciscano quali sono le attività, intese come pratiche, lecite e quali non. Deve tracciare il banale vincolo del bene o male, del giusto o sbagliato. Deve pertanto far si che l'individuo si pieghi alla norma accetandone, più o meno consciamente, i costi ed i benefici. E deve essere in grado di far rispettare le sue leggi sanzionando i comportamenti illeciti. Per ottenere questo crea degli apparati di polizia con il compito di mantenere il monopolio della violenza da parte dello stato agendo da guardiani. Al tempo stesso opera la costituzione di una serie di apparati burocratici, amministrativo, sanitario, e così via, con lo scopo di poter attuare una serie di misure d'intervento che permettano di far rientrare tutto nei limiti della *norma* .

L'aspetto problematico dello Stato-nazione in relazione al tema della sorveglianza appare nel momento in cui lo si inserisce nelle attuali dinamiche

globali. È nell'attuale contesto storico che emerge con vigore il successivo smembrarsi dello stato nazione ad opera di agenzie sovranazionali, di organismi internazionali, di imprese commerciali transnazionali, di relazioni e di accordi fra stati-nazione.

È bene ricordare che lo Stato-nazione è l'organizzazione sociale risultata vincente nel corso dei secoli. La sua formazione ha richiesto il cambiamento del concetto di sovranità stesso.

> La sovranità da attributo divino diventa un principio giuridico e sostiene la creazione e lo sviluppo dello Stato-apparato che si fa portatore di un principio di "bene comune", cioè si dà come compito la costruzione di un modello di società capace di realizzare i valori più rappresentativi di una cultura (Mongardini ,2001,p.48).

Lo Stato-nazione non è soltanto un'organismo astratto di gestione, ma è portatore anche di una serie di valori che vengono condivisi a livello culturale. Ed è proprio attraverso questi valori, sedimentati nell'immaginario collettivo di un popolo che viene fuori il concetto di nazione. Nella creazione dello stato moderno la cultura gioca un ruolo centrale. Lo Stato-nazione diventa una *comunità immaginata* (Anderson,1991).

A sfaldare questa comunità convergono delle dinamiche che la investono in tutti i suoi livelli, agendo sia a livello micro (sul cittadino) che a livello macro (sullo Stato).

A livello culturale possiamo assistere alla crescente mescolanza delle diverse culture. Il sistema dei mass-media e le nuove tecnologie rendono sempre più possibile la conoscenza di culture *altre*

andando così ad erodere quella che prima era considerata la cultura nazionale. L'individuo si sente sempre meno ancorato agli ideali nazionali in funzione di altri maggiormente internazionalizzati[6].

A livello economico lo Stato-nazione si trova ad essere sempre meno padrone di gestire in maniera indipendente la propria economia. Sia esso uno stato del primo o del terzo mondo. Organismi internazionali quali il *Wto* regolano gli accordi di scambio fra i Paesi, decidendo le quote di sussidi che possono essere destinate a determinate attività, stabilendo le portate degli scambi internazionali, facendo pressione sui governi agendo come organismi politici non essendolo[7]. L'*Fmi* e la *Banca mondiale* stabiliscono le strategie d'intervento che uno Stato-nazione deve attuare per poter essere in linea nei loro parametri; nei paesi che beneficiano dei loro prestiti stabiliscono i settori e le modalità delle privatizzazioni, i cosidetti *programmi di aggiustamento strutturale*[8] (Nicholson,1998). Nel caso europeo la Ue stabilisce i parametri a cui i singoli stati devono attenersi, le quote di produzione dei diversi settori, la destinazione dei fondi monetari alle imprese.

Infine le multinazionali agiscono in maniera diretta sui governi facendo pressione su di essi affinchè le favoriscano in qualche modo[9].

---

[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.

In ultimo, a livello politico lo stato-nazione si trova inserito in una serie di organismi internazionali quali l'*Onu*, la *Nato*, e in una serie di accordi che limitano sempre maggiormente la propria autonomia.

Lo Stato nazione perde gran parte della sua sovranità, ma al tempo stesso riesce a crearne di nuova. Infatti, inserito nei processi di globalizzazione, lo Stato deve fare i conti con minacce che diventano globali. Come gli scambi commerciali legali avvengono in mercati internazionali, così quelli illegali si internazionalizzano. Le organizzazioni criminali tendono ad agire sempre più come *attori* nelle relazioni internazionali (Nicholson,1998). Lo Stato si trova a far fronte al fenomeno dell'immigrazione clandestina, della lotta al narcotraffico, al contrabbando, al terrorismo che operano a livello mondiale. E deve agire in un contesto internazionale se vuol fermare tutto questo.

In questo contesto lo Stato da un lato perde la propria sovranità in ambito internazionale, ma dall'altro, configurandosi come unico freno ai crescenti pericoli, accresce la propria sovranità all'interno, perché il cittadino vede in lui la sola ancora di salvezza al caos. Lo Stato passa ad essere uno strumento di *unificazione sociale* , diventa uno stato di gestione dei meccanismi sociali; si afferma una "cittadinaza secondaria" che viene svuotata dei significati morali e collettivi ed è fondata sul calcolo. Lo Stato, inserito nei processi di globalizzazione, non può più farsi carico di difendere la morale sociale e i valori condivisi, ma per restare ad essere strumento unificante aumenta le maglie di controllo sulla vita del cittadino, moltiplica l'uso della forza e i meccanismi di dominio

(Mongardini,2001). Per ottenere ciò lo Stato attua due strategie precise che sono complementari.

La prima è quella che definiamo *strategia d'emergenza*. Lo Stato stabilisce quali siano i maggiori pericoli per se stesso, li presenta all'opinione pubblica all'allarmandola, e crea una nuova legislazione per risolvere il problema. Questa legislazione opera una limitazione delle libertà civili dei cittadini, i quali cedono questa libertà per avere una maggiore sicurezza. La definiamo strategia in quanto nell'attuale momento storico essa non si presenta essere come eccezionalità bensì come pratica sistematica.

> In questa aggregazione si scambia la protezione con una maggiore soggezione al potere che fa saltare tutte le garanzie della democrazia. La sicurezza si paga in termini di libertà. La situazione eccezionale si stabilizza e permette qualunque restrizione della libertà… in più l'efficacia dell'immagine di "lotta al terrorismo" permette di eliminare ogni movimento anti-sistema all'interno dei singoli paesi. Infatti il terrorismo, oltrechè una realtà diventa anche un'idea-forza nell'immaginario collettivo, un'ideologia fondata sulla paura che permette al potere di legittimare azioni che non sarebbero legittime in tempi normali (Mongardini,2001, p.117).

In Italia ne abbiamo avuto esempio con la legge Reale adottata per combattere contro le brigate rosse, e, attualmente, in tutto il mondo assistiamo all'emanazioni di leggi che violano o restringono le libertà civili.

L'altra strategia complementare alla prima è quella che definiamo dell'*esclusione/ inclusione*. Lo Stato ha bisogno di indirizzare la *strategia d'emergenza* a determinate categorie di individui, ha bisogno di

trovare un pericolo reale, o, a volte, un capro espiatorio. Come sottolinea Dal Lago, lo Stato ha bisogno di creare una determinata devianza per mantenere inalterati i rapporti di potere e di dominio. La costruzione della devianza è centrale nei moderni Stati (Dal Lago,1981). Anderson a questo proposito cita l'esempio dell'India, ai tempi in cui era una colonia inglese, evidenziando come proprio la categorizzazione degli individui è stata usata per controllare la popolazione (Anderson,1991).
Pertanto lo Stato dovrà stabilire quali caratteristiche debbano avere gli *inclus*i e quali gli *esclusi* e lascerà che siano i propri apparati di volta in volta a stabilire quali debbano essere. Vediamo.

3.2 Apparato poliziesco

Negli ultimi anni le strategie di prevenzione del crimine attuate dalle polizie hanno subito un cambiamento radicale. Le nuove tecnologie hanno permesso uno stravolgimento totale di queste e soprattutto sono riuscite a modificare, come abbiamo visto, il concetto di visibilità. Se infatti agli inizi del secolo la visibilità degli apparati di polizia era centrale (Foucault, 1975), i nuovi strumenti elettronici permettono alla polizia un controllo maggiormente esercitato a distanza piuttosto che in presenza (Lyon D.,2001;Marx G.T.,1989).

Questo comporta la creazione di pratiche specifiche per andare ad attuare le misure preventive.

Come infatti fa notare Marx Gary T. nel suo saggio sui metodi investigativi della polizia americana, questa tende a concentrare le indagini sui crimini in base a dei “sospetti categoriali” (Marx G.T., 1985). Ossia vengono utilizzate delle tecniche di profiling per individuare quali possono essere i soggetti maggiormente propensi alla commissione di determinati tipi di reato.

Il *profiling* non è nient’altro che una delle tecniche della *dataveglianza* che prevede la creazione di profili riguardo gli individui in base all’esperienze passate di ques’ultimi. Si situa pertanto in quella che Clarke ha definito come sorveglianza di massa, ossia non concerne il monitoraggio quotidiano come quella individuale, ma invece fa rientrare una serie di individui in determinate tassonomie (Clarke,1993). Come l’autore sottolinea questo per l’apparato di polizia si traduce nella creazione di una serie di profili: molestatori sessuali, serial killers, rapinatori, truffatori, esibizionisti e così via. Si passa dal cercare il sospetto per un crimine avvenuto a quella di prevedere chi potrà essere il sospetto per un crimine che verrà commesso. Tutto questo è reso possibile dalla creazione dei database e dalla *data-matching*, o *computer-matching*: il controllo incrociato dei dati fra i vari database permette infatti la creazione di profili sempre più precisi.

Da un lato questo comporta una maggiore possibilità di arrivare prima alla soluzione dei delitti, da un altro la tecnica del *profiling* attua una forte discriminazione. Entrambi gli autori, Marx e Clarke, sottolineano proprio il fatto di come la polizia tenda sempre di più a fare affidamento sui dati raccolti

tramite le tecniche di *profiling* piuttosto che sulla ricerca del colpevole in base alle prove (Clarke,1987, 1993; Marx G.T., 1985). La *strategia dell' esclusione/inclusione* fa rientrare determinati individui fra i sospetti e ne scagiona altri.

L'applicazione del *profiling* inoltre travalica la sfera dell'individuo e viene prestata ad altri ambiti. Lo Stato, e di conseguenza i suoi apparati, si trovano a far fronte ad un'incessante gestione del rischio. Il passaggio dalla *repressione* alla *prevenzione* comporta un'analisi delle propabilità che un determinato evento avvenga. In parole povere lo Stato deve ipotizzare scenari possibili e saper reagire ad essi. Deve sapere ad esempio, dove un attacco terroristico potrà avvenire, con quali armi, chi lo potrebbe effettuare e, sopratutto, come reagire a quest'eventualità. Pertanto effettuerà delle *simulazioni* riguardanti un evento. Traducendo questo nella concreta attività di polizia dello Stato, vediamo che la tecnica del *profiling* viene ampliata fino ad arrivare a creare tassonomie di aree. Non assistiamo soltanto alla creazione dei "sospetti categoriali", ma, conseguenza al dover saper dove un evento può accadere, alla creazione di "zone calde" (Lyon,2001). Così come negli ultimi tempi, in seguito ad allarmi lanciati dall'intelligence, abbiamo assistito al concentrarsi di controlli in determinati luoghi considerati a rischio, in maniera sistematica si creano delle categorie di luoghi dove determinati tipi di reati possono avvenire. Unendo il *profiling* geografico a quello individuale la polizia può sapere chi dovrebbe commettere determinati tipi di reato e in quali luoghi, e in base a questo attuare diversi tipi di sorveglianza.

Le nuove tecnologie infatti permettono alla polizia di poter scegliere dove attuarne un tipo e dove un altro. La crescente diffusione della videosorveglianza permette alla polizia di monitorare costantemente un determintato luogo e tenere sotto controllo la situazione anche non essendo fisicamente presente sul luogo. Come nel *Panopticon* in queste aree, che nelle città diventano sempre più frequenti, il cittadino sa di essere costamente monitorato e non ha la possibilità si sapere se il guardiano in quel momento sta osservando lui o no. La telecamera rappresenta un segno visibile del potere e come tale agisce da deterrente. Unita alle tecniche di *profiling* inoltre permette di sapere alla polizia quali delle persone che passano in quel momento sono "sospette". Come sottolineano sia Marx Gary T. e Lyon , per essere considerati tali basta possedere anche solo determinate caratteristiche fisiche o essere vestiti in un determinato modo (Lyon, 2001; Marx G.T., 1985). Dove possono avvenire altri tipi di reati come ad esempio furti o scippi, la polizia utilizzerà ancora la sua presenza quale deterrente al crimine. Diverse aree, diversi sospetti, diversa sorveglianza.

Proprio nella crescente diffusione delle telecamere noi possiamo vedere l'applicazione concreta della *strategia dell'emergenza*. In Inghilterra dopo la crescente ondata di attentati da parte dell'Ira e il dilagare del fenomeno hooligans, lo Stato ha varato una serie di strumenti normativi che hanno permesso l'installazione di sistemi di videosorveglianza in ogni luogo: strade, parchi, scuole, ospedali, centri commerciali. Fino a far diventare Londra una delle

città maggiormente sorvegliate al mondo (Chiesa, 2000; Froomkin, 2000).
In Giappone lo stesso fenomeno hooligans, attesi per i campionati del mondo del 2002 in Corea del Sud, ha permesso lo sviluppo di sistemi di sorveglianza, come dice Abe:

> Possiamo osservare un tipico effetto della "morale del panico" nella campagna dell'"invasione degli hooligans". Giocando sulla pubblica ansietà è stato facile per il governo introdurre sistemi di sorveglianza molto avanzati…L'introduzione di una nuova sorveglianza elettronica è stata legittimata senza una discussione critica circa la necessità o la plausibilità di questi sistemi (Abe, 2004, p.225;trad. mia).

Gli utilizzi delle videocamere variano dal prendere il numero di targa di chi passa con il rosso fino all'essere utilizzate per rintracciare degli individui. Froomkin a proposito cita un fatto molto importante. Nel 1998 a Londra durante una manifestazione violenta la polizia risalì ai colpevoli pubblicando le foto ottenute dai video delle telecamere su Internet, chiedendo alle persone di riconoscerle (Froomkin, 2000).

La polizia ha la possibilità di avere a disposizione un software di analisi facciale che permette di confrontare fra loro due fotografie, una delle quali inserita nel proprio database, per individuare l'identità di un individuo. La polizia in questo caso viene fornita della possibilità di identificare qualunque persona si trovi in un luogo se la sua immagine è presente all'interno dei propri database. Si potrebbe arrivare ad essere "schedati" in un modo, rientrare in una delle tante categorie, solo perché un giorno ci si trovava in

un determinato posto. Naturalmente senza che l'individuo in questione ne sia mai a conoscenza.

Come si può notare queste tecniche sono fortemente sterotipizzate, basandosi in molti casi solo sull'aspetto fisico, e permettono di concentrare un particolare tipo di sorveglianza su alcuni soggetti a scapito di altri. In Palestina possiamo vedere come un controllo di tipo rigido venga applicato soltanto ai palestinesi, siano essi cittadini o meno dello stato d'Israele (Zureik,2001).

Le nuove tecnologie comunque non portano soltanto vantaggi alla polizia. Il computer e la rete recano con sè la nascita di nuove tipologie di reati che devono essere fronteggiati: si passa dalla pedofilia informatica alla semplice pirateria, dalla violazione di server alle truffe in rete. Le polizie pertanto si trovano a dover far fronte ad una serie di reati che travalicano le proprie frontiere nazionali. Il flusso dei dati è globale. Come sono globali molte altre attività illecite. La soluzione al problema sta nella creazione di un flusso di dati fra le varie polizie che permetta lo scambio delle informazioni. La sorveglianza in questo contesto si globalizza (Lyon,2001;2004). E questo è uno dei primi aspetti da rilevare. Altri riguardano la particolare natura dei reati.

Le nuove tecnologie non offrono soltanto la possibilità di far nascere nuove tipologie di reati, ma permettono di essere un ottimo strumento di comunicazione per gruppi criminali. La rete in particolare si presta ad essere sia il luogo di commissione di reati, sia uno strumento attraverso il quale si possono organizzarne di vecchi (Strano,2000). Per fronteggiare questo gli Stati

cercano di attuare strumenti normativi in grado di arginare il fenomeno. Tuttavia la natura della rete offre particolari problemi ai governanti. Come ricordano Bennato e Castells, la natura del web è democratica, basata su uno scambio orizzontale delle informazioni e sulla libera circolazione delle stesse (Bennato, 2002; Castells, 2001). Il web sembra rifiutare censure. Lo Stato allora reagisce a ciò in maniera diversa in base alla sua natura politica. Nei regimi autoritari l'utilizzo delle nuove tecnologie, anche se riservato a pochi, è strettamente sorvegliato. Si veda il caso cinese dove le imprese collaborano con lo stato per incrementare la sua capacità di monitorare le comunicazioni in rete, in quanto il Web rappresenta uno dei pochi strumenti che i dissidenti politici possono utilizzare (Lyon,2004). La Cina attua allora strategie di censura dei siti e sorveglia gli Internet Cafè. Alcuni Stati reagiscono al fenomeno addirittura in maniera paradossale come hanno osservato Elia Zureik e Rafal Rohozinski al 5°Congresso sulle ricerche politiche e sociali del Mediterraneo: la Tunisia da un lato esalta le potenzialità offerte dalla rete e si fa promotrice di politiche di sviluppo dello stesso; dall'altro arresta e punisce severamente alcuni cittadini soltanto perché avevano visitato dei siti islamici (ZureiK, Rohozinski, 2004).

Nei regimi democratici invece si attuano restrizioni normative attuate secondo i canoni della *strategia dell'emergenza*. Viene gettato il panico riguardo l'accrescersi di determinati fenomeni e si cerca di regolamentare la rete. Ne abbiamo un esempio con l'allarme lanciato riguardo la pedofilia. Negli U.S.A. per rispondere al fenomeno viene varato il

Communications Decency Act del 1995 che prevede la censura per determinate tipologie di siti. L'atto è successivamente dichiarato incostituzionale dalla Corte Suprema perché viola le libertà individuali. In Italia lo stesso allarme sulla pedofilia ha generato la creazione della *legge n.269 del 3/8/1998*, che punisce lo scambio telematico, limita l'art.15 della Costituzione sull'inviolabilità delle comunicazioni, sancisce la possibilità per gli investigatori ad adescare i criminali, ossia permette loro d'istigare al reato. Ma i due esempi sono il passato.

Gli Stati si sono resi conto che i tentativi di controllare internet censurandolo producono gridi d'allarme da parte di tutte le organizzazioni che si occupano di libertà civili, pertanto sono passati allo sviluppare sistemi in grado di monitorare ciò che avviene nella rete delle telecomunicazioni. Lo sviluppo della tecnologia ha permesso la creazioni d'applicativi che sono in grado di identificare le traccie della comunicazione soprattutto se si parla del Web. La stragrande maggioranza di queste tecnologie, che affronteremo in dettaglio nella terza parte, permette di analizzare milioni di comunicazioni al giorno semplicemente usando delle parole chiave specifiche. Quando un utente utilizza in un discorso una determinata parola, questi programmi sono in grado di far scattare un campanello d'allarme (Bamford, 2001; Lyon, 2001). Un esempio può essere il software *Carnivore* dell'Fbi che operando in collaborazione con i service provider, registra tutto il traffico delle e-mail e smista le informazioni desiderate basandosi su campionamenti e parole chiave (Castells,2001).

Il problema da risolvere in questo caso è quello di poter riuscire ad utilizzare le informazioni ottenute per poter incriminare qualcuno. La maggior parte degli Stati democratici infatti sancisce la riservatezza delle comunicazioni personali. E questa riservatezza può essere violata soltanto con un'esplicita richiesta da parte degli apparati polizieschi a quelli giudiziari. Pertanto sistemi di controllo indiscriminato e sistematico sarebbero definiti incostituzionali. Ed è attraverso l'emanazione di *leggi eccezionali*, che viene risolto il problema. Negli U.S.A. Il 24 ottobre 2001, in seguito agli attentati alle torri gemelle, il Presidente vara il *Patriot Act*. È importante vedere cosa implica per verificare l'esattezza della strategia da noi definita. La legge

- permette intercettazioni telefoniche su un individuo, invece che su un numero di telefono specifico, senza necessità di mandati separati per numeri diversi;
- autorizza le forze dell'ordine che si occupano della criminalità comune a monitorare e intercettare le e-mail e i siti Internet visitati da una persona senza dimostrarne al giudice la necessità;
- autorizza il governo a intercettare le comunicazioni elettroniche di un "hacker" senza ordine del tribunale se c'è il consenso del proprietario del computer attaccato;
- autorizza gli agenti federali ad acquisire la documentazione su cosa leggono o cercano gli utenti di biblioteche, librerie e altre imprese o istituzioni;
- autorizza lo scambio d'informazioni, permettendo che le informazioni su attività terroristiche raccolte dalla polizia o presentate davanti a un "grand jury" federale siano trasmesse alle agenzie d'intelligence;
-amplia il programma di monitoraggio degli studenti stranieri a istituzioni come scuole di volo, corsi di lingua o di formazione professionale;

- triplica il numero di agenti – compresi quelli di dogane e immigrazione – lungo le frontiere Usa;
- richiede la raccolta del Dna di terroristi già riconosciuti colpevoli (Fazzino 2004),

In Italia assistiamo alla creazione del *Decreto-legge 24 dicembre 2003, n. 354* che obbliga i service provider, le compagnie telefoniche e, più in generale, tutti i fornitori d'accesso alle telecomunicazioni, a mantenere per la durata di cinque anni tutti i dati relativi alle comunicazioni telefoniche, via sms, via internet e via email. Il decreto legge non riguarda i contenuti delle comunicazioni ma come viene rilevato

> è quindi proprio sotto il profilo di merito che il decreto appare inadeguato, anche al di là dei suoi specifici contenuti. Infatti - nonostante dal decreto sia esclusa la registrazione dei contenuti delle comunicazioni - con la telematica, soprattutto nel caso dei dati del traffico internet, una chiara distinzione fra contatti e contenuti viene meno: poiche' i "contatti" riguardano il numero del chiamante, del chiamato, la data e l'ora e la zona per i telefoni mobili ma anche altri dati come il tragitto di una comunicazione, mittente e destinatario, numero dei caratteri inviati per e-mail, la loro registrazione puo' essere usata per ricostruire gli interessi e la rete delle relazioni sociali di ciascuno. Tali informazioni possono pertanto essere finalizzate ad una profilazione dei soggetti da cui e' possibile ricavare i loro dati sensibili, cioe' le opinioni politiche e religiose, lo stato di salute e l'orientamento sessuale, ma anche le abitudini d'acquisto e altri comportamenti sociali e personali.[10]

In Canada nel 2003 è stata introdotta una legislazione che potrebbe permettere di rilevare le

[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).

informazioni relative al traffico dati degli utenti (Cockfield, 2004).

Attraverso lo spettro del “cyber-terrorismo” quindi si giustifica l’incremento della censura e della sorveglianza sulle reti di computer (ZureiK, Rohozinski, 2004). Grazie al concetto di “lotta al terrorismo” in generale vengono varate misure eccezionali che poi si stabilizzano diventando ordinarie (Abe, 2004; Mongardini, 2001).

Lo Stato in questi contesti non fa altro che continuare a fare ciò che ha sempre effettuato. Una raccolta sistematica di informazioni sulla popolazione che finisce per essere totalmente schedata. In questo contesto, come negli anni Settanta in Italia, si tenevano dei dossier sugli individui in base alle loro simpatie politiche, si profila la creazione di dossier che includano ogni preferenza di questi. Con tanti saluti alla privacy.

Questo dato può destare ulteriore preoccupazione se lo uniamo al flusso globale dei dati. Le informazioni sugli individui vengono infatti passate fra i vari paesi. Recentemente proprio con la creazione del *Patriot Act* gli U.S.A. hanno obbligato tutte le compagnie aeree che atterrano nei suoi aereoporti a fornire le liste dei passeggeri, e le relative informazioni personali (che in molti casi contengono anche le preferenze alimentari) alle autorità competenti. In pratica quello che stiamo notando è una sempre maggiore convergenza fra il settore pubblico e quello privato nello scambio delle informazioni raccolte nei database (Cockfieldf, 2004; Lyon, 2001, 2004; Graham, Wood, 2003). Inoltre le autorità americane impongono a tutti coloro si rechino

nel loro paese per più di novanta giorni di lasciare le loro impronte digitali.

La polizia per verificare l'esattezza dell'identità fornite, cerca sempre di più di usare strumenti biometrici. Anche L'Unione Europea nel 1997 ha approvato un programma per la raccolta delle impronte digitali che riguarda tutti i richiedenti asilo. Quello che appare evidente è che questa raccolta dati avviene in maniera asimmetrica ed è fortemente stereotipizzata. La raccolta dei dati biometrici non avviene in maniera identica per tutta la popolazione, gli U.S.A., ad esempio, la applicano a tutti i cittadini che non appartengono ai suoi ventisette alleati, e a tutti i delinquenti, e non accetta che altri facciano lo stesso. Il Brasile, accusato di essere uno stato che ha nel terittorio centri di addestramento dei terroristi, ha emesso un'ordine che obbligava gli agenti di frontiera a prendere le impronte digitali agli americani ed è successo uno scandalo diplomatico[11]. L'Europa la applica verso tutta quella frangia di popolazione più svantaggiata quali i migranti. La creazione dello Schengen Information System, che è un sistema integrato di dati, infatti porta a scambiare le informazioni, fra i vari paesi dell'Unione, per arginare i fenomeni di criminalità transnazionale e di immigrazione clandestina (Davis,2004, Mathesien, 2000). L'aspetto negativo di ciò risiede, come evidenzia Lyon, nel metodo.

Per controllare i fenomeni si analizzano i flussi delle attività e si finisce per identificare determinati gruppi etnici con determinate attività criminali, ossia si "etnicizza"la sorveglianza (Lyon,2001). Cockfield a

[11] Si veda D'Eramo M., 2004.

questo proposito evidenzia il fatto che in Canada si attui una discriminazione molto forte verso gli islamici a cui si riserva un maggior controllo perché sospettati di terrorismo (Cockfield, 2004), mentre la Zureik analizzando il caso della Palestina sottolinea come i cittadini d'Israele vengano categorizzati in base all'etnia e alla religione con privilegi diversi in base all'appartenza ad una categoria (ZureiK, 2001). In più il Sis è stato utilizzato per bloccare alle frontiere dei rispettivi paesi alcuni contestatori politici in occasione dei vertici del G8 (Mathesien, 2000). A ciò va aggiunto che, con la creazione di sistemi quali L'Eurodac, nell'Unione Europea, si prevelano le impronte digitali soltanto dei richiedenti asilo, lasciando escluso il resto della popolazione. Proprio nell'Unione possiamo vedere l'applicazione della *strategia dell'esclusione/inclusione*.

La stragrande maggioranza della popolazione viene inclusa nei vantaggi che il libero transito delle persone e delle merci comporta. A loro viene attuata una sorveglianza a distanza, costante, ma comunque morbida. Agli altri, gli esclusi, si applica una sorveglianza dura, rigida. Si creano centri di prima accoglienza per offrire un soccorso al travaglio dei migranti che arrivano. Ma queste centri diventano luoghi simili a prigioni dove gli individui, non essendo imputati di nessun reato, aspettano di poter accedere, i pochi fortunati, nella "Fortezza Europa", o di essere rispediti, la stragrande maggioranza, al proprio paese. Si cerca di attuare delle "zone di protezione" nei paesi di maggior transito, fuori dell'Unione, dove stanziare i potenziali profughi (Davis, 2004).

Nelle frontiere vengono appliacati controlli sempre più ferrei utilizzando le più svariate tecnologie. Negli U.S.A. lungo il confine vengono innalzate torrette dotate di videocamera controllate in maniera remota, le guardie sono dotate di visori notturni, vengono applicati sensori di movimento e si utilizzano i satelliti per monitare le zone adiacenti. In Europa, nel tunnel della Manica, vengono utilizzati per scovare i clandestini dentro i camion, rilevatori di anidride carbonica, e particolari strumenti a raggi "X"[12]. Non solo è diverso il tipo di sorveglianza, ma anche le tecnologie che la stessa utilizza.

Un ultimo aspetto da rilevare nello scambio crescente dei dati fra i vari paesi, è la preoccupazione di quando questo avviene fra uno stato democratico e uno totalitario, che può sollevare alcuni interrogativi. Ad esempio, se un cittadino iraniano andasse a visitare un sito gay negli U.S.A. e questi fornissero al suo Paese questo dato, il soggetto potrebbe essere accusato di sodomia. La configurazione di un "sistema di polizia globale" potrebbe avere conseguenze devastanti perché ad esso non segue la globalizzazione dei diritti.

3.2.1 L'intelligence

Fra gli apparati che uno Stato utilizza per controllare gli eventi, c'è anche quello dei servizi segreti. Essi svolgono un ruolo determinante nel mantenimento della sicurezza esterna, ed interna. Loro compito primario è quello di raccogliere informazioni, in

[12] Si veda l'articolo di Shenk D,2003.

determinati settori, per permettere allo Stato di saper reagire a determinate situazioni. Pertanto utilizzeranno tutti gli strumenti di sorveglianza disponibili per spiare il nemico, concentrando la loro attenzione al settore delle comunicazioni. Proprio grazie allo spionaggio dei messaggi criptati tedeschi gli americani riuscirono a scovare l'esistenza del codice "Enigma" e, attraverso una serie di geni matematici specializzati in crittografia, a decriptarlo scovando le posizioni dei loro sommergibili.

La fine della Seconda Guerra Mondiale invece di portare ad una diminuzione del lavoro d'intelligence lo incrementò notevolmente. L'affermarsi di due blocchi ideologici ed economici contrapposti diede l'avvio alla Guerra Fredda e alla nascita della *strategia della deterrenza*. Viene chiamata della deterrenza in quanto entrambi i blocchi possedevano la bomba atomica e sapevano che utilizzandola si sarebbe arrivati alla catastrofe nucleare: come uno dei due avesse effettuato un'attaco atomico, l'altro avrebbe risposto. Il deterrente era appunto la bomba H (Nicholson, 1998). In questo contesto il ruolo dell'intelligence era fondamentale. Bisognava infatti creare un'apparato (in gergo 3CI: comando, controllo, comunicazione ed informazione) che riuscisse a rispondere prontamente ad un attacco. Che potesse sapere in anticipo quando questo sarebbe potuto accadere. Inoltre, essendo una guerra quella in atto, era centrale l'essere a conoscenza di tutti i settori d'interesse del nemico, in maniera tale da riuscire a batterlo.

Si incominciò ad affermare uno spionaggio sempre più ampio su tutte le comunicazioni. Negli U.S.A. l'*NSA* (*National Security Agency*) vide aumentare

notevolmente il suo budget e i settori di suo interesse. Se infatti in principio essa doveva occuparsi soltanto di intercettare i messaggi di guerra e decriptarli, ora le zone di competenza erano maggiori perché riguardavano tutti i canali di comunicazione (Bambford,2001).

Il 5 marzo del 1946 venne firmato il patto UKUSA fra U.S.A., Gran Bretagna, Australia, Nuova Zelanda ed il Canada. Il patto prevedeva un reciproco scambio d'informazione fra le varie agenzie *Sigint* dei rispettivi paesi. Come *Sigint* (*Segnal intelligence*) viene definito tutto il lavoro che ruota intorno all'Intelligence dei segnali. Esso racchiude sia l'intellingence delle comunicazioni (*Comint*) che l'intelligence elettronica (*Elint*), ossia quella dei radar (Bambford, 2001). Il patto di collaborazione fra le nazioni suddivideva il pianeta in determinate aree di competenza, ognuna delle quali veniva affidata ad una determinata nazione. Nell'area assegnata si cercavano d'intercettare tutte le informazioni disponibili, catalogarle, farne una prima analisi e poi inviare i dati significativi all'attenzione degli altri alleati.

Alla fine degli anni settanta si arrivò alla creazione di una rete informatica, *Platform*, capace di collegare tutti i cinquantuadue sistemi computerizzzati delle cinque nazioni. I dati rilevanti confluivano direttamente in un "nucleo centrale" che non era altro che il quartier generale dell'NSA a Fort Meade. Alla fine degli anni Ottanta non c'era un angolo del pianeta in cui le postazioni d'ascolto dei paesi alleati non arrivassero. Satelliti, radar, aerei spia, cavi sottomarini, raccoglievano tutte le informazioni disponibili e tramite

il sistema computerizzato chiamato *Echelon* le rendevano disponibili a tutte le nazioni del patto.

Tutti i diciasette satelliti INTELSAT che garantiscono le comunicazioni fra le varie regioni del mondo, di e-mail, fax, telefonate, vengono costantemente spiati dall'*orecchio di dio*, come Bamford chiama il sistema dell'NSA (Bambford, 2001). A livello pratico le postazioni d'ascolto riescono a monitorare costantemente tutte le comunicazioni che passano nel mondo. Vengono utilizzati "dizionari", liste di parole chiave, che ogni qual volta viene utilizzata una determinata parola sottopongono, in maniera automatica, il messaggio ad un'analisi più accurata.

Questo sistema di spionaggio venne tenuto strettamente nascosto e solo intorno al 1997 si arrivò alla conferma della sua esistenza. Una cosa da rilevare, come evidenzia Chiesa, è che la Gran Bretagna attraverso il suo coinvolgimento nell'UKUSA viola in maniera esplicita il trattato di Maastricht che prevede la parità in tutti gli scambi fra gli stati membri (Chiesa,2000).

Le tecnologie d'utilizzo verranno da noi trattate successivamente. In questa parte quello che ci preme rilevare è che il sistema Echelon non è stato, e non viene, utilizzato solo per avere delle informazioni di carattere militare. Come Bamford evidenzia, e lo stesso Lyon fa, il sistema di sorveglianza dagli anni Ottanta in poi è stato configurato per raccogliere informazioni di carattere commerciale riguardanti concorrenti dell'America e delle nazioni del patto.

> Invece di fornire direttamente dati d'intelligence alle compagnie americane, alla NSA fu ordinato di supportare le iniziative commerciali, e con esse tutta l'economia

> americana, per vie più tortose. Uno di questi metodi consisteva nel rafforzare le indagini sulle possibili pratiche illegali e ingannevoli, come ad esempio la corruzione, impiegate da concorrenti stranieri al fine di sottrarre le commesse alle compagnie americane. Un altro era devolvere più risorse per la raccolta di informazioni da trasmettere ai negoziatori governativi statunitensi in sede di importanti accordi commerciali (Bamford, 2001, p.400).

Questo passo evidenzia un'aspetto molto preoccupante di questi sistemi di sorveglianza: la forte asimmetria in quanto una superpotenza spia tutte le altre. Infatti come evidenzia Cockfield, anche i paesi alleati quali il Canada, sono sottoposti ad una sorveglianza dei propri cittadini da parte degli U.S.A. (Cockfield,2004).

Altresì l'attenzione deve essere posta sullo smantellamento del concetto di privacy individuale. Tutte le informazioni sono sottoposte ad intercettazione e basta un'errore di un'analista a far finire un'individuo su una lista nera. Differenza fondamentale: le informazioni su un americano possono rimanere in archivio per solo un anno, per tutti gli altri non c'è limite di tempo (Bamford,2001). La preoccupazione è che

> senza i dovuti controlli, la rete mondiale di intercettazione dell'UKUSA potrebbe divenire una specie di polizia segreta cibernetica, senza tribunali, senza giurie e senza alcun diritto di difesa (Bamford, 2001, p.403).

La risposta europea a questo sistema fu *Enfopol* :

> un sistema di controllo e spionaggio pianificato per collegare i diversi circuiti di polizia internazionale responsabili di polizia

> locale, dogana, immigrazione e sicurezza interna del Paese (Chiesa, 2000, p.15).

In pratica un sistema che metteva in collaborazione le varie polizie dei paesi coinvolti. Tuttavia questo sistema fu proposto dall'FBI per cercare di intercettare tutte le comunicazioni mobili, e pertanto si configura come un secondo orecchio degli U.S.A. in Europa. Da rilevare che il progetto *Enfopol* e il suo attuale sviluppo non sono stati votati nè dal Parlamento Europeo nè in nessuno dei parlamenti dei paesi membri dell'Unione. Attualmente il sistema sembra identificare le persone attraverso il numero delle loro carte di credito (Chiesa,2000), mentre non sappiamo l'*UPI* che viene utilizzato da *Echelon*.

Come fanno rilevare ZureiK e Rohozinski, l'accrescersi delle potenzialità, dei budget, dei settori di competenza, delle agenzie d'intelligence in seguito agli attachi dell'undici settembre, sta comportando una ridefinizione dei diritti relativi alla privacy a livello globale. Nella maggioranza dei paesi occidentali vengono limate le libertà civili sancite dalle rispettive costituzioni (ZureiK, Rohozinski, 2004). Situazione questa avvertita da associazioni internazionali come *Amnesty International* e *Report Sans Frontier* che nei loro rapporti del 2004 richiamano l'attenzione sulle continue violazioni alle libertà e al diritto internazionale subite da cittadini, stranieri e non, in nome della "guerra al terrorismo".

3.3 L'apparato burocratico

La burocrazia trova il suo fondamento attraverso pratiche razionalizzanti che permettono il funzionamento della stessa (Weber, 1922). È attraverso il calcolo che la gestione dello Stato avviene. Appare pertanto scontato che la raccolta delle informazioni, più sistematica possibile, sia centrale: soltanto attraverso la conoscenza sulla popolazione si può provvedere al mantenimento della stessa. Le nuove tecnologie non fanno altro che aumentare la capacità di uno stato di raccogliere informazioni sui propri cittadini e gestirle nella maniera più adeguata.

La possibilità offerta dalle reti di comunicazione permette lo scambio dei dati fra le amministrazioni locali e quelle centrali, rende possibile lo scambio delle informazioni fra le varie agenzie. Aumenta la capacità gestionale dello Stato in maniera esponenziale in base alla velocità del flusso e della quantità di dati che nel flusso passano. Riduce la spesa economica dello Stato in maniera sensibile, diminuendo le risorse umane necessarie ai controlli e alla raccolta dati.

Le amministrazioni attraverso la raccolta delle informazioni, aggregandole in categorie, e sottoponendole a statistiche possono avere un controllo adeguato relativo ai fabbisogni della popolazione. Soltanto sapendo il tasso di povertà in maniera adeguata, sapere dove è maggiormente localizzato, quale fasce della popolazione interessa, si possono adottare precise politiche di sviluppo. L'apparato burocratico quindi non fa niente che non sia strettamente necessario.

Il fisco attraverso la comparazione dei redditi, delle spese, e dei beni in possesso riesce a determinare il grado di evasione fiscale nel paese, e, avendo informazioni relative ai singoli individui, è in grado di rintracciare gli evasori. A capire chi riceve sussidi di disoccupazione o indennità civili non dovendole ricevere. La creazioni di database, il controllo incrociato dei dati fra questi, la tecnica del *profiling*, vengono utilizzate in maniera sistematica ed automatizzata facilitando il processo di individuazione delle anomalie.

Come nel settore fiscale così in tutti gli altri le nuove tecnologie riescono a snellire le pratiche d'archiviazione burocratica. Siamo di fronte ad una semplice *strategia gestionale*, che vede come obiettivo quello di ridurre le spese e velocizzare gli scambi, e vede nelle nuove tecnologie, nelle reti, il mezzo migliore per attuarlo.

Questo sviluppo permette l'accrescersi di quella che Foucault ha identificato come "società dei dossier", basilare nei moderni stati-nazione. L'aumento delle informazioni riguardo agli individui permette la nascita del "concetto di persona integrale", nient'altro che una data-immagine che lo stato ha riguardo ai suoi individui (Lyon, 1994; 2001). Non c'è più bisogno di avere venti file su ogni cittadino, come aveva il Canada qualche anno fa, in quanto tutti questi file possono essere raggruppati in un unico soggetto, richiamabile attraverso l'*UPI* che uno Stato ha deciso di adottare (nella maggioranza dei casi quelli che vengono utilizzati sono i numeri di previdenza sociale o le tessere sanitarie).

La tendenza delle amministrazioni negli ultimi anni è stata quella di passare dall'autocertificazione al controllo diretto: si chiedono sempre meno informazioni in maniera diretta agli individui e si passa ad effettuare controlli diretti, attraverso le informazioni contenute nei database, sugli stessi (Lyon,2001). L'individuo non è a conoscenza della sua data-immagine, né tantomeno sa quando questa viene utilizzata.

Quello che appare rilevante negli ultimi anni è la tendenza della sorveglianza ad accrescere le informazioni riguardo gli individui e ad inserire nei suoi database anche dati sensibili. Uno degli aspetti da rilevare infatti è l'utilizzo dei dati biometrici, che sta prendendo piede nella maggior parte degli Stati, nelle data-immagine degli individui.

Questo punto è importante focalizzarlo. La maggioranza degli stati occidentali sta attuando politiche per sviluppare l'implementazione di tessere sanitarie elettroniche. Che esse siano delle "smart card" oppure dei semplici numeri identificativi non cambia molto, in quanto in esse sarebbe contenuta tutta la "storia" delle malattie di un individuo. La possibilità offerte da questo sistema sarebbero immense. Attraverso studi statistici e comparando la storia di un individuo con altre si potrebbe scoprire quali soggetti siano più propensi a determinate malattie. Si potrebbero applicare terapie di prevenzione per tutte le malattie ereditarie, o per quelle che compaiono solo in determinate aree. Lyon a questo proposito cita un fatto. In Francia alcuni ricercatori scoprirono che una forma di glaucoma che provoca la cecità era stata tramandata da una coppia

di coniugi quattrocento anni fa. Risalendo ai pronipoti si arrivò ad identificare 30.000 possibili soggetti in pericolo, ma il governo impedì la comunicazione della notizia in quanto sarebbe stata lesiva della privacy (Lyon,2001). L'utilizzo di simili strumenti potrebbe servire per curare in anticipo milioni di persone. Ma al tempo stesso possono realizzare la configurazione di sistemi di sorveglianza sempre più accurati e discriminatori.

In questo contesto dobbiamo effettuare una disgressione per poter capire bene il concetto. Attualmente quello che si sta attuando è una sempre maggiore convergenza fra il settore privato e quello pubblico. Possiamo assistere a casi come il Canada e gli Stati Uniti dove i governi si rivolgono alle aziende private per avere informazioni relative alle transazioni commerciali e alle comunicazioni degli individui (Cockfield,2004), o alla Finlandia dove i progetti di ricerca sulle biotecnologie sono affidati a quello che Osmo Kivinen e Jukka Varelius definiscono come "triplice elica"[13] formato dal governo, dalle università e dalle imprese commerciali (Kivinen, Varelius, 2004). Al Progetto Genoma Umano effettuato in ambito internazionale fra diverse equipe di ricerca, private e pubbliche, finalizzato alla mappatura genetica (Rifkin,1998). In pratica dalla medicina ai settori finanziari siamo di fronte ad un sempre maggiore scambio d'informazioni, e una maggiore collaborazione, fra settore pubblico e privato (Cockfield, 2004; Lyon,2001).

Attraverso questo scambio di dati si possono configurare utilizzi non previsti degli stessi. La

[13] Il rimando è alla doppia elica con cui è costituito il DNA.

possibilità di identificare le caratteristiche genetiche degli individui da parte delle aziende può comportare la nascita di politiche di discriminazione basate sulla possibilità o meno di essere predisposti a determinate malattie. Sia Lyon che Cockfield evidenziano infatti come le aziende private cerchino sempre di più di ottenere questi dati sensibili in maniera tale da potersi tutelare (Cockfield, 2004; Lyon, 2001). Immaginare che le compagnie assicurative possano avere accesso a determinate informazioni vuol dire che ad alcune persone, soltanto perché maggiormente predisposte ad una malattia, verrebbe negata la possibilità di tutelarsi. A ciò va aggiunto che in alcuni casi, come negli U.S.A, è obbligatorio effettuare le assicurazioni ai propri dipendenti, e pertanto si potrebbe restare totalmente esclusi dal mondo del lavoro. Le tecniche biometriche nel passaggio dallo Stato alle aziende potrebbero essere strumenti di forte discriminazione andando ad aumentare il potere delle *strategie d'esclusione/inclusione.*

Un'ulteriore considerazione deve essere effettuata riguardo le politiche di sviluppo delle ricerche. La raccolta dei dati biometrici, come abbiamo visto, permette di poter individuare i soggetti maggiormente predisposti a determinate malattie. Nel momento in cui la ricerca medica viene finanziata da soggetti privati, quali case farmaceutiche, la possibilità che i dati che lo Stato raccoglie possano finire nelle loro mani desta preoccupazione. Alla luce attuale già possiamo vedere come la ricerca farmaceutica sia finalizzata a rivolgersi verso tutte quelle malattie che sono "remunerative", questo vuol dire dedicare maggiore attenzione al guadagno piuttosto che al malato. L'attuazione della

strategia dell'esclusione/inclusione nel contesto verrebbe a determinare l'esclusione di determinate malattie quali aree di ricerca e l'inclusione di altre, e questa sembra essere l'attuale tendenza (Kivinen, Varelius, 2003).

La preoccupazione risiede nel forte potere discriminatorio che questa strategia possiede. Potrebbero restare fuori dalle ricerche mediche non solo le malattie che tendono a verificarsi in aree geograficamente svantaggiate, vedi il caso della malaria, ma anche malattie che colpiscono particolari fascie di popolazione o particolari etnie laddove esse risultassero essere soggetti economicamente deboli (Cockfield, 2004; Lyon,2001). Ci sono già alcuni casi in cui si può vedere come particolari malattie tendano a colpire una determinata etnia: gli ebrei risultano essere maggiormente predisposti alla sindrome di Tay-Sachs e i greci e gli afroamericani all'anemia falciforme (Rifkin,1998).

Inoltre bisogna considerare che le ricerche biologiche stanno segnando un ritorno impressionante all'eugenetica. Può sembrare assurdo parlare di eugenetica ma come evidenzia Rifkin,

> ogniqualvolta il DNA ricombinante, la fusione cellulare e altre tecniche simili vengono usati per "migliorare" i tratti genetici di un microbo, di una pianta, di un animale o di un essere umano, sorge una considerazione eugenetica nel processo. Nei laboratori di tutto il mondo, i biologi molecolari operano scelte quotidiane a proposito di quale gene alterare, inserire o eliminare dal codice genetico di varie specie. Tutte queste sono decisioni di tipo eugenetico (Rifkin,1998,p.210).

Si sta configurando un sistema il cui i tratti genetici degli individui assumono sempre maggiore importanza

fino ad arrivare al punto di effettuare analisi sui feti per vedere se i futuri bambini possano essere soggetti a determinate malattie, come la sindrome di Down, e in funzione di esse decidere se portare avanti la gravidanza o meno. O decidere se i geni della propria futura moglie, o marito, siano compatibili con i propri (Rifkin, 1998). In alcuni casi possiamo assistere ad un ritorno delle teorie criminali basate sull'idea della delinquenza innata[14], e gli stessi ricercatori del Progetto Genoma Umano hanno organizzato un convegno dal titolo " I fattori genetici del crimine" in cui gli organizzatori sottolineavano come la ricerca genetica offra buone opportunità per identificare i possibili individui propensi alla commissione di particolari tipologie di reato (Rifkin,1998).

Un ultimo aspetto da evidenziare riguarda il possibile utilizzo dei dati biometrici degli individui come identificatori universali personali (*UPI*). Nel momento in cui gli Stati decidessero di adottare il DNA quale identificatore universale assisterremmo davvero a quello che precedentemente abbiamo osservato essere il sogno della *data-veglianza*, in quanto esso porterebbe con se tutte le nostre informazioni genetiche oltre l'insieme dei profili che ci riguardano.

Nel momento in cui gli Stati comunicano fra di loro, e con le aziende, non solo la nostra privacy verrebbe lesa in maniera significativa, ma potremmo essere soggetti a misure discriminatorie senza esserne a conoscenza.

[14] Per le teorie criminali basate sui geni si rimanda al libro di Ponti (vedi bibliografia).

4. Aziende

"You have zero privacy. Get over it".[15]

Scott McNealy, chief executive officer di Sun MicroSystem

La società dell'informazione ristruttura le imprese commerciali sia a livello produttivo, sia a livello gestionale che in quello relativo al consumatore. Come sottolinea Bauman si afferma un capitalismo di tipo leggero che pone l'accento sul controllo gestionale dei prodotti. La tendenza è quella di delocalizzare la produzione delle diverse componenti, in funzione del risparmio economico, per poi riassemblarle in sede (Bauman,2000). Inoltre le nuove tecnologie, come abbiamo notato precedentemente, forniscono nuovi settori di espansione commerciale, si pensi al Web, e nuove modalità d'erogazione dei servizi.

Tutti questi campi vengono attraversati da una serie di sistemi di sorveglianza che riescono da un lato a garantire il controllo della produzione, dall'altro riescono a fornire nuove modalità per ottenere informazioni commerciali riguardo i consumatori.

Le strategie che vengono utilizzate dalle aziende tendono a ricalcare, naturalmente escludendo quella dell'emergenza, quelle utilizzate dallo Stato.

[15] Deborah Radcliff, *A Cry for Privacy*, Computer World, May 17, 1999

La *strategia dell'esclusione/inclusione* trova il suo utilizzo nelle pratiche che riguardano il consumatore e la localizzazione delle sedi, mentre la *strategia gestionale* garantisce il monitoraggio della produzione e del lavoratore. Focalizzando la nostra attenzione su questi due settori riusciamo a individuare le caratteristiche che gli odierni sistemi di sorveglianza possiedono.

4.1 Più compri, più ti guardo

La *strategia dell'esclusione/inclusione*, trova nel consumo la sua perfetta espressione. Questo perché nelle nostre società capitalistiche il consumo si presta ad essere uno degli strumenti di controllo sociale più efficace. Sono illuminanti le parole di Lyon a proposito di questo:

> I metodi coercitivi per il mantenimento dell'ordine sociale all'interno degli stati-nazione capitalistici si sono ridotti, fino al punto di assumere un ruolo marginale. Però il margine è ancora necessario, perché lascia inalterato un gruppo di riferimento, un sottoproletariato, se preferiamo chiamarlo così, il cui destino di non consumatore è bene evitare a tutti i costi. Però per la maggioranza, il consumo è diventato l'aspetto assorbente della vita contemporanea nelle società affluenti, la guida morale e l'integratore. L'ordine sociale, e di conseguenza una forma morbida di controllo, viene preservato stimolando ed incanalando il consumo, ed è a questo punto che entra in gioco la sorveglianza dei consumi (Lyon,1994, p.196).

La strategia opera dividendo fra “sedotti” e “repressi”, fra “turisti” e “vagabondi”, seguendo le dicotomie baumaniane. Ai primi viene concesso di entrare a far parte del mondo delle merci, mentre i secondi sono totalmente esclusi da esso (Bauman,1998). Pertanto non si opererà più come nell’apparato poliziesco creando dei “sospetti categoriali”, ma si utilizzerano le tecniche di *profiling* per selezionare i consumatori. Riuscire a capire chi è affidabile nei pagamenti, chi tende a consumare cosa e così via. Si cercherà di attuare quel meccanismo sanzione/gratificazione che abbiamo incontrato in Foucault.

Le aziende, seguendo i cambiamenti della società contemporanea, cercano di rivolgersi sempre meno ad un pubblico massa, ma indirizzano le loro ricerche verso gli individui. Si afferma la “customizzazione”, ossia la produzione personalizzata solo per alcune nicchie di mercato. La tendenza del marketing è quella di rivolgersi sempre di più al singolo individuo cercando di indirizzare i suoi consumi in base a quelli precedenti, in base alla classe socioeconomica e all’area geografica di appartenenza. Per effettuare questo è normale che le aziende tendano a cercare sempre maggiori informazioni sugli individui, e queste vengono ottenute seguendo le traccie delle loro transazioni: nell’utilizzo delle carte di credito, delle carte fedeltà, delle carte premi, ecc.

È bene evidenziare che in questo genere di sorveglianza il consumatore è attore centrale in quanto non è solo l’oggetto verso cui questa viene riversata, ma è soggetto in quanto fornisce, in maniera più o meno consapevole, la serie di informazioni che le

aziende cercano ogni qual volta utilizza una serie di strumenti. Più consuma e più permette alle aziende di avere un profilo preciso su di lui (Poster,1990).

In questo scenario le strategie aziendali sembrano ricalcare quelle militari. Come nel settore dell'intelligence, e in tutti quelli dell'*information society*, l'informazione diventa bene supremo, per cui le aziende cercheranno di avere sempre una maggiore conoscenza riguardo gli individui, in maniera tale da avere maggiori vantaggi sui concorrenti. La ricerca dell'informazione rappresenta un obiettivo primario e il mezzo attraverso il quale riuscire a battere la concorrenza (Lyon,1994).

Nascono imprese che raccolgono i dati relativi agli individui e li rivendono alle aziende a cui interessano. In maniera tale da fornire, attraverso gli strumenti dell'analisi statistica, sia tendenze generali di consumo, sia, attraverso le tecniche di *profiling*, preferenze individuali. Si pensi che negli U.S.A. gli utili generati dalla vendita dei dati raggiungono la cifra di tre miliardi di dollari l'anno (Solove,2001).

È proprio nel settore commerciale che vediamo una maggior applicazione dei profili. Perché è grazie a questi che le aziende sanno con precisione a chi rivolgersi.Come per l'apparato poliziesco le tecniche di *profiling* riguardano sia le aree, sia gli individui.

Nel primo caso le aziende utilizzano i dati relativi a determinate zone per vedere quali classi, a livello socioeconomico, vi abitano. In tal modo solo grazie al c.a.p. esse possono mandare informazioni pubblicitarie, tramite posta (*junk mail*), a determinati gruppi sociali partendo dal presupposto che "ogni simile ama il suo simile" (Lyon,2001). Inoltre grazie

all'analisi dell'area una azienda può riuscire a capire qual è la zona migliore per vendere i suoi prodotti o, nel caso di un negozio o di una banca, per posizionarsi. È logico l'operare attraverso l'esclusione di determinate zone, magari particolarmente svantaggiate, in favore di altre.

Nel secondo caso le informazioni agli individui vengono raccolte per inserire i soggetti in determinate categorie d'acquirenti e riuscire, in maniera sempre più precisa, a vendere i propri prodotti. Alcune categorie ad esempio sono "giovani letterati", "mix Ispanico","mix boemo", "fucili e pick-up" includendo in esse religione, razza, e hobby (Solove,2001).

Prima di andare avanti è bene evidenziare un aspetto. Come nel caso delle biotecnologie abbiamo potuto notare una convergenza sempre più stretta fra lo Stato e le aziende, dobbiamo immaginare questa convergenza estesa anche in altri settori. Le informazioni relative agli individui infatti molte aziende le prendono in maniera diretta dagli apparati statali: numeri di previdenza sociale, residenza, numeri di telefono, anagrafica. Negli U.S.A. questo sistema è prassi consueta. In Canada attraverso il *PIPEDA* (*Personal Information Protection and Electronic Documents Act*) il governo ha obbligato le aziende che lavorano nella regione a ottenere, in maniera esplicita o meno, il consenso degli individui alla distribuzione e al trattamento dei propri dati (Cockfield, 2004). Ma il flusso delle informazioni non è unidirezionale e permette anche alle aziende di avere le informazioni dallo Stato. È anche grazie a queste informazioni che è possibile effettuare il *profiling* delle aree e degli individui Aziende quali la *Dataman Information*

Services di Atlanta possiedono un database così ampio da poter fornire in un attimo il nome, la residenza, il numero dei figli e l'età della casa di un individuo (Lyon,1994). La *Winland Services* possiede un database che comprende circa mille elementi, dalle informazioni anagrafiche ai comportamenti abituali, di circa 215 milioni di persone (Solove,2001). Basta raffrontare il reddito e le prospettive di un individuo, compararlo con il prodotto offerto ed il gioco è fatto.

In tutto questo settore le nuove tecnologie permettono un'espansione massiccia dei settori da cui ottenere informazioni e nuove modalità per farlo. Uno dei punti chiavi per le aziende diventa sapere in anticipo, data la crescente globalizzazione dei consumi, chi è affidabile o meno. Grazie all'utilizzo di carte magnetiche, di chip, e al controllo incrociato dei dati, le aziende riescono ad ottenere proprio questo.

Con l'utilizzo delle carte di credito le aziende riescono ad ottenere informazioni personali sulle preferenze d'acquisto, e al tempo stesso esse rappresentano un segno di riconoscimento, una quasi carta d'identità, che ci classifica come consumatori, quindi affidabili. L'espansione dell'utilizzo delle carte di credito per effettuare pagamenti, così come quello delle "carte fedeltà" delle compagnie petrolifere o dei supermercati, se dal consumatore viene visto come una comodità, possibilità di girare senza contanti e di rateizzare le spese o ottenere sconti e premi, alle aziende permette di ottenere informazioni dettagliate su quali prodotti preferiamo, dove siamo soliti fare spese, in quale misura siamo soliti utilizzare la carta. Attraverso lo scambio dei dati fra le diverse imprese commerciali, i produttori riescono a capire da chi viene

preferito il prodotto, da quali ceti sociali, e le aree dove vende di più, permettendogli di pianificare politiche aziendali adeguate per allargare i consumi. Lo scambio dei dati permette di sapere quali sono le aree a maggiore affluenza in maniera tale da posizionare in esse le proprie sedi.

Ma il salto avanti che le carte comportano riguarda l'individuo. Infatti se da un lato le categorie in cui si è inseriti diventano sempre più precise, dall'altro la raccolta dati individuali permette alle aziende di sapere con precisione a chi rivolgersi per vendere il loro determinato prodotto. Permette di effettuare campagne pubblicitarie mirate, sapendo chi escludere e chi includere nella vendita. Le carte di credito quindi rafforzano il potere delle statistiche, rendendole sempre più vicine alla realtà, e accrescono il Sapere sugli individui permettendo alle aziende di parlare al singolo piuttosto che alla massa.

Questo aspetto è centrale per il settore dei mass-media. Lo sviluppo di sistemi digitali quali il decoder, per le aziende che operano nel settore, permette di non parlare più ad un'audience generalizzata, ma di parlare ad un pubblico, specchio della società, composto da individui. La potenziale personalizzazione della visione dal telespettatore è vista come una liberazione in quanto ognuno può crearsi il proprio palinsesto, e non è più lui ad adattarsi alla visione, ma è essa che si adatta al tempo che lui vuole dedicargli, nel momento in cui vuole farlo. Il decoder inoltre permette l'accesso a determinati servizi, parlare con le P.A., effettuare acquisti, avere informazioni su determintati settori, che dal telespettatore vengono percepiti come un valore

aggiunto. Il vantaggio per le imprese è rilevante in quanto non solo riescono a sapere con precisione, non come con l'Auditel, chi guarda cosa e in quale momento, fornendo loro indicazioni basilari per indirizzare e progettare in futuro nuovi programmi, ma riescono ad avere informazioni sui contenuti da noi preferiti. La raccolta dati attraverso il decoder digitale viene così aggiornata con importanti riferimenti culturali. Altresì gli svantaggi sembrano non apparire evidenti. Lo sviluppo di questi sistemi, che offrono la possibilità di personalizzare il palinsesto, tende a basarsi sulla possibilità di semplificare la vita del telespettatore. La tendenza in atto è quella di fornire ad esso informazioni sui programmi da vedere, basandosi sui gusti precedentemente esposti, che secondo loro gli potrebbero piacere. Questo comporterebbe la fine della probabilità dell'imprevisto, ossia trovare inaspettatamente un programma possibilmente interessante per noi e può comportare un impoverimento culturale, in quanto tutto ciò che è altro dai nostri "gusti" verrebbe escluso dall'offerta (Bettetini, Garassini, Vittadini , 2001). Ma per il settore di nostro interesse questo comporta un'intensificazione della sorveglianza diminuendo ancora la *privacy* dell'individuo facendo lentamente diminuire la soglia che separa il pubblico dal privato (Lyon, 1994).

Sicuramente la crescente convergenza in atto fra più media in uno (pc che permettono di guardare la televisione e i film, televisori che possono navigare in internet, decoder digitali con hard- disk) che sta trasformando le nostre case, comporterà un aumento delle informazioni raccolte su noi, ma, nel presente,

non quanto quello reso possibile da tutti gli strumenti mobili che circondano le nostre esistenze, e dall'utilizzo della rete.

4.1.1 Ubiquitous Computing

Le tecnologie mobili hanno la straordinaria capacità di abbattere la barriera spaziale e mettere in comunicazione soggetti o reti fra loro distanti. Gli scenari che si prospettano realizzabili vedono la Rete come ambiente unico di collegamento fra i vari dispositivi in nostro possesso, oppure vedono questi ultimi come interfacce in grado di porci in relazione ogni volta con l'ambiente desiderato (Bolter, Grusin,2001). Quello che in entrambi i casi si prospetta è un mondo in cui le tecnologie portatili quali cellulari, pc, palmari, e simili, siano esse racchiuse in un unico dispotivo o rimangano separate ed indipendenti, diventino maggiormente importanti nelle nostre esistenze. Strumenti di comunicazione indispensabili. Su quello che questo futuro scenario possa comportare per l'incremento della sorveglianza, noi possiamo soltanto speculare. Formulare ipotesi che possano essere più o meno verosimili. Ma se invece ci soffermiamo sul momento attuale possiamo individuare delle tendenze in atto e capire meglio il presente.

Analizzando le tecnologie di comunicazione mobile quale il cellulare possiamo notare un grande salto in avanti delle possibilità commerciali delle aziende, nell'adozione di sistemi di terza generazione (UMTS). Prima di essi il telefono si configura solo

come uno strumento di comunicazione. Le aziende da esse possono ottenere informazioni importanti quali la rete di relazioni che noi abbiamo, l'utilizzo che facciamo del telefono, la quantità di traffico generata. In questi casi esse possono far rientrare noi in determinate categorie e farci partecipi di determinate offerte. Inoltre forniscono, come abbiamo evidenziato, informazioni preziose all'apparato statale su di noi. Ma niente più.

L'avvento dei cellulari di terza generazione comporta invece un cambiamento radicale in quanto il telefono si trasforma. Diventa strumento di svago con la possibilità di vedere programmi televisivi, mezzo attraverso il quale collegarsi con la rete, in pratica diventa multimediale. E questa multimedialità implica sia una serie di servizi in più che noi possiamo avere, sia l'aumento dei fornitori di questi servizi. Questo comporta una ridefinizione delle strategie aziendali, infatti come evidenziano Garassini e Vittadini,

> il sistema UMTS si configura come il luogo dei modelli di business legati alla vendita di spazi pubblicitari nella telefonia cellulare, i cui costi non vengono più a essere concepiti dalla vendita di un servizio a tempo, ma dalla vendita di un'utenza all'inserzionista (Garrasini, Vittadini, 2001,p.174).

In parole povere agli inserzionisti vengono venduti i nostri numeri di telefono per mandarci della pubblicità. L'aspetto da sottolineare è che la multimedialità del telefono, come nel caso dei decoder digitali, permette di ottenere informazioni che riguardano le nostre preferenze culturali. I cellulari UMTS incrementano in maniera significativa la

raccolta dati e migliorano il profilo che le aziende hanno su di noi. Inoltre essi, come i sistemi *Gps*, permettono la localizzazione precisa della nostra posizione. In questa maniera le informazioni, sarebbe meglio chiamarle pubblicità, da noi ricevute, riguarderanno l'area in cui ci troviamo in quel momento. Passando di fronte ad un negozio potremmo venir informati delle offerte che ci sono all'interno perché rientriamo in una delle categorie a cui è abbinata la vendita di quel prodotto (Bettetini, Garassini, Vittadini ,2001). Più che uno scenario alla *Brazil*, il futuro si prospetta essere come in *Minority Report*, dove al nostro passagio una pubblicità personalizzata ci viene offerta.

Quello che appare preoccupante in questo non è tanto la lesione della *privacy*, in quanto speriamo spetti sempre al soggetto la decisione se accedere o meno a questi servizi, ma quanto la capacità dei database di aumentare il loro potere di conoscenza su di noi, essendo essi una tecnologia, come abbiamo potuto osservare, fortemente discriminante

Il potere di conoscenza delle aziende viene aumentato non soltanto grazie ai cellulari, ma anche da altri strumenti di rilevazione. Sistemi quali il *Gps*, se sono utilissimi sia per le aziende sia per gli automobilisti per rintracciare l'automobile in caso di furto, forniscono però con estrema precisione informazioni in tempo reale sulla nostra posizione. Attraverso i dati raccolti le aziende possono analizzare i flussi di traffico e, al tempo stesso, sapere quali sono le zone da noi maggiormente attraversate e pertanto posizionare in esse i loro prodotti. Lo sviluppo di carte per i trasporti pubblici come la *Metrebus Card*, dotate

di chip, ci potrebbe rendere individuabili anche quando prendiamo i mezzi pubblici. Le nostre esistenze si prestano ad essere costantemente monitorate, sia in casa che fuori, dalle aziende.

4.1.2 Il World Wide Web

Per le imprese commerciali il Web rappresenta un nuovo scenario in cui muoversi, e al tempo stesso diventa sia un efficace strumento di promozione commerciale sia uno spazio in cui monitorare il consumatore ed ottenere preziose informazioni su di lui. Il marketing trova nella rete uno splendido alleato per ridefinire le proprie strategie e attuarne di nuove.

Attraverso Internet le aziende riescono a capire con precisione quanti clienti sono riusciti a raggiungere e qual è stato il modo in cui sono riusciti a farlo. La crescente personalizzazione della società è affrontata dalle stesse cercando di cambiare la modalità di trasmissione dei propri messaggi. Non si può più parlare ad un pubblico unico, considerato massa omogenea, ma bisogna parlare agli individui. Ai singoli. La rete offre la possibilità di valutare l'efficacia della pubblicità. L'efficacia del messaggio pertanto non viene più calcolata in base al *cost per impression*, il costo totale che è stato sostenuto per la comunicazione del messaggio diviso per il numero di consumatori raggiunti da esso, ma verrà sostituita dal *cost response*. Adesso saranno le risposte generate al messaggio da parte dei consumatori a determinare il costo/contatto,

> di conseguenza l'oggetto di transazione pubblicizzato cesserà di essere in prima istanza il prodotto, ma sarà la pura informazione sul cliente, che porterà in un secondo momento, e in un altro luogo all'acquisto (Mignani, Bazzoffia, 2000, p.110).

Bisogna fare in modo di contattare il consumatore. Avere un rapporto diretto con lui. La rete si presta ad essere il luogo in cui l'interazione fra consumatore e azienda può avvenire. Le strategie attuate per rendere possibile la comunicazione si prestano ad essere sia di tipo *orizzontale* che *verticale*. In entrambi i casi si cerca di contattare il maggior numero di persone che rappresentano il proprio target di riferimento con un costo minimo e viene attuato il *viral marketing*. Il principio è che la comunicazione deve tendere a propagarsi come un virus nella rete. Attraverso i *forum*, le *chat*, i *newsgroups*, le *newsletter*, si cerca di utilizzare quello che viene comunemente chiamato "passaparola": le aziende possono incentivare direttamente la discussione su determinati temi creando propri spazi di aggregazione, oppure possono lanciare un prodotto in spazi di discussione già esistenti sperando che il messaggio si diffonda scatenando un effetto a valanga (Santini,2000). Nei portali le strategie orizzontale e verticale vengono utilizzate in maniera simultanea: un tema viene lanciato dall'azienda e lo si lascia commentare dagli utenti facendolo diffondere grazie a loro. In questa maniera, dalle loro discussioni, si possono ottenere preziose informazioni riguardo alle preferenze del target di riferimento.

Per raccogliere informazioni sul consumatore si possono attuare tecniche come quella utilizzata dalla

Procter&Gamble per pubblicizzare i suoi nuovi prodotti. Con la creazione del sito *Winnerland* mise in atto un gioco a premi. Per poter partecipare al gioco l'utente doveva registrarsi e rispondere a determinare domande che riguardavano le sue abitudini d'acquisto, questo l'unico costo. All' azienda questo permise di ottenere preziose informazioni riguardo le preferenze d'acquisto dei consumatori, il rapporto con la concorrenza, e altresì permise di ottenere una serie di dati anagrafici dei navigatori (Santini,2000). Esempi come questo non sono altro che uno dei tanti metodi che possono essere attuati per raccogliere informazioni sugli utenti, e ci rende evidente come la rete offra alle aziende la possibilità di avere maggiori dati con cui creare statistiche, tassonomie e migliorare i profili.

Una delle prime cose da evidenziare del processo di navigazione dell'utente, in relazione alle tecniche di *profiling*, è che questo è costantemente monitorato. Ogni computer infatti una volta connesso alla rete viene fornito di un indirizzo IP che lo identifica, e quest'indirizzo viene comunicato a tutti i server a cui di volta in volta ci si appoggia. È la nostra chiave d'accesso e riconoscimento. Grazie a ciò si afferma la tecnica dell'analisi dei click: quali siti sono stati visitati, attraverso quali collegamenti, quali sono i *banner* maggiormente cliccati e così via. Le aziende attraverso questi dati possono ottenere importanti informazioni riguardo il posizionamento di un proprio annuncio nel web, sia verificare il percorso di un utente nel tempo, infatti la maggior parte dei siti tende a conservare nel proprio database le visite dell'utente. Siti come Google ad esempio mantengono tutte le

ricerche che un utente ha effettuato nell'arco degli ultimi cinque anni. Mentre altre aziende quali Internet Profile sono in grado di fornire ai propri clienti informazioni su chi ha visitato il sito e il tempo di permanenza in esso (Lyon,2001).

Come abbiamo potuto vedere con la rete cade la differenza fra contatti e contenuti, in quanto anche solo sapere quale sito abbiamo visitato comporta sapere anche a quali contenuti abbiamo accesso. In questa maniera i profili che vengono creati riguardo i navigatori sono pieni di riferimenti culturali. Basti pensare che i giornali on-line riescono a sapere con precisione quali articoli un utente ha letto e quali sono state le immagini che hanno catturato la sua attenzione (Froomkin,2000).

Un'altra pratica che si sviluppa è quella dell'inserimento dei *cookie* all'interno dell'hard disk dell'utente. Il *cookie* non è altro che un applicativo che raccoglie informazioni sulle abitudini di navigazione dell'utente. Castells a proposito cita l'esempio di DoubleClick

> la più grande azienda di vendita di spazi pubblicitari su Internet. Il suo business è piazzare milioni di "cookie" nei computer che si connettono a siti web equipaggiati della tecnologia DoubleClick. Quando un computer riceve un "cookie", diventa oggetto di specifici annunci commerciali per ciascuna visita alle migliaia di siti web che impiegano i servizi di DoubleClick….usando il database DoubleClick crea dei profili che collegano nomi e indirizzi reali di singole persone con i loro acquisti online e offline (Castells,2001, p.166).

Naturalmente tutte le informazioni che vengono raccolte vengono rivendute fra le diverse aziende.

Basti pensare che sempre Google, grazie al servizio Gmail, offre agli utenti la possibilità di avere un Gb di spazio per inviare i messaggi. In cambio di questo la sua posta viene fornita di una tecnologia penetrante che setaccia le mail alla ricerca degli interessi di ciascun individuo[16], e poi grazie alla vendita dei nominativi permette alle aziende di effettuare lo *spamming* verso gli utenti. Tutto questo tende ad essere sviluppato senza l'esplicito consenso dell'individuo e senza che esso ne riceva un guadagno, quando invece l'azienda dall'abbassamento del prezzo dell'informazione lo riceve (Rust, Kannan, Peng, 2002).

Un ulteriore settore in cui può essere analizzata l'erosione della privacy attuata dalle aziende nei confronti del consumatore per ottenere informazioni, è quello che riguarda i software. Possono essere illuminanti a proposito le parole della risoluzione adottata in data 12/09/2003 dalla Conferenza Internazionale delle Autorità di Protezione dei Dati e della Privacy:

> La Conferenza rileva con preoccupazione che le case produttrici di software in tutto il mondo fanno sempre più ricorso a meccanismi non trasparenti per trasferire aggiornamenti di software nel computer degli utenti. Così facendo, esse:
> - sono in grado di leggere e raccogliere dati personali memorizzati nel computer dei singoli utenti (ad esempio, le impostazioni dei programmi di navigazione, e informazioni sulle abitudini di navigazione del singolo utente) senza che

[16] Cfr. Rampini F., *Google e la nuova legge sulla privacy delle e-mail*, in *Affari e Finanza* del 31/10/2004.

questi abbiano la possibilità di accorgersene, intervenire o impedirlo;
- possono assumere il controllo, almeno parziale, del computer terminale e, quindi, limitare la capacità dell'utente di far fronte agli obblighi ed alle responsabilità previsti dalla legge nei suoi riguardi, in quanto titolare del trattamento, al fine di garantire la sicurezza dei dati personali eventualmente oggetto di trattamento;
- modificano il software installato sul computer, che sarà quindi utilizzato senza essere collaudato o approvato nei modi previsti, e
- possono provocare malfunzionamenti del computer senza che sia possibile individuarne la causa nell'aggiornamento.

Stallman a questo proposito evidenzia come alcune aziende stiano cercando di sviluppare la "trusted computing", letteralmente la traduzione significa computer affidabile, che permetterebbe alle aziende di controllare il computer dell'utente, riuscire a sapere quali programmi vengono fatti girare, e permettere di far aprire determinati file solo con i programmi da essi sviluppati, lasciando all'utente poco o nulla spazio per controllare il fenomeno (Stallman,2002).

Inoltre le aziende tendono ad inserire nei propri software particolari applicazioni che hanno il solo scopo di raccogliere informazioni sull'utente stesso. Il funzionamento degli stessi verrà spiegato in dettaglio nella prossima parte, qui l'importante è rilevare in quali ambiti le aziende raccolgono informazioni. Possiamo avere programmi quali il Word o PowerPoint che attraverso i *GUID* (*Globally Unique Identifier*) riescono a registrare ogni documento che viene creato al computer e a collegarlo con l'identità reale della persona che lo ha generato (Castells,2001). Inoltre la maggioranza dei programmi tende ad essere fornita di

spyware che altro non sono che altri software in grado di monitorare le attività svolte dall'utente. Il semplice Windows Media Player raccoglie tutte le informazioni relative ai cd ascoltati, alla musica scaricata, ai DvD visti, in pratica a tutti i file aperti con il lettore, e ogni volta che ci colleghiamo alla rete, li invia al proprio server di riferimento. Come fa notare Cammarata, tutto questo solleva seri interrogativi riguardo alla privacy in rapporto al potere delle aziende. Infatti l'art 23 del *Codice in materia di protezione dei dati personali* prevede che l'utente debba ogni volta esercitare il proprio assenso al trattamento delle informazioni da lui fornite, mentre nel caso esposto il trattamento comincia ogni volta l'utente utilizza il programma considerando implicito l'assenso (Cammarata,2003). In entrambi i casi è lecito il sollevarsi dei dubbi relativi alla fuga di dati sensibili.

Un aspetto preoccupante del problema è infatti che la maggior parte di questi programmi funziona in maniera indipendente dall'attività dell'utente e sono completamenti invisibili allo stesso. Nel momento in cui amministrazioni pubbliche, privati, siano essi aziende o semplici commercialisti, utilizzino questi software, i nostri dati potrebbero essere scambiati senza che noi, né tantomeno chi li detiene, ne possa essere a conoscenza. O abbia le capacità di impedirlo.

Un ulteriore aspetto da rilevare della questione è che in molti casi i governi non riescono ad arginare il fenomeno o collaborano con le aziende produttrici di software in quanto esse forniscono il *Know-how* necessario a loro per ampliare le maglie di controllo sulla vita dei cittadini (Castells,2001). Un caso interessante di questa commistione viene citato da

Froomkin: il governo degli Stati Uniti aveva proposto al Congresso di emanare un atto che avrebbe permesso di lasciare una porta aperta nei computer degli utenti in maniera tale che se un giorno gli investigatori avessero avuto bisogno di controllare il computer di qualcuno lo avrebbero potuto fare in maniera remota (Froomkin,2000). Oppure possono essere proprio le aziende a fornire informazioni ai governi quando vedono pratiche non lecite. Il portale *Aol* analizzando le comunicazioni che avvenivano nelle sue chat è riuscito a fornire agli investigatori i nomitativi di due persone che avevano violato i suoi server per ottenere circa novantamila indirizzi mail, che avrebbero in seguito utilizzato per lo *spamming*[17].

La *strategia dell'escusione/inclusione* grazie al Web viene migliorata significativamente in quanto si estendono i settori in cui si possono ottenere informazioni sugli individui, sui loro interessi, e sulla rete delle loro relazioni. I profili diventano maggiormente accurati, e permettono alle aziende di rivolgersi con precisione verso il target di riferimento.

Ultimo aspetto da evidenziare per quello che riguarda la Rete riguarda lo scenario che si sta profilando. Uno dei principali problemi che affliggono gli utenti è quello della ricerca delle informazioni. Ogni volta che effettuiamo una ricerca attraverso un motore siamo impressionati dalla mole di pagine che si presenta di fronte ai nostri occhi. Tutte queste pagine devono essere da noi visualizzate per capire se l'informazione che ci serve è presente o meno al loro interno, in quanto la ricerca che abbiamo effettuato si

[17] Assante E., *Jason lo spione che rischia grosso*, in *Il Venerdì di Repubblica* del 9/04/2004.

basa solamente su parole chiave. Per risolvere il problema il *W3C* (*World Wide Web Consortium*) di Tim Berners-Lee sta cercando di sviluppare il Web semantico. Il funzionamento dello stesso prevede che la marcatura dei documenti, oggi basata sul linguaggio *HTML* (*Hyper Text Markup Language*), avvenga attraverso l'*XML* (*eXtensible Markup Language*). In questa maniera si potrebbero avere informazioni sui documenti (metadati), che i diversi software potrebbero scambiare fra loro. Insieme a questo si utilizzerebbe L'*RDF* (*Resource Description Framework*) che è uno strumento che permetterebbe di dare un attributo semantico ad ogni documento (Bennato,2002b). In parole povere la struttura del Web semantico permetterebbe di sapere quali sono i contenuti di ciascun documento che è presente nella rete. Se a questo aggiungiamo ciò che abbiamo visto in precedenza, possiamo vedere come le preoccupazioni riguardanti la sfera della privacy siano tutt'altro che irreali in quanto ogni nostro singolo documento, ogni nostra mail, potrebbe essere classificata in base al contenuto. Lo scenario è inquietante se solo lo trasferiamo da uno Stato democratico ad uno totalitario: uno Stato potrebbe condannare qualcuno solo perché in un documento in Word ha scritto che è contrario alle politiche governative. E questo scenario è tutt'altro che irreale.

Il problema lungi da riguardare solo l'utente sembra preoccupare anche le aziende. La continua violazione della privacy a cui è sottoposto il navigatore negli ultimi tempi sta emergendo con vigore e vengono attuate misure di protezione. Sono sempre maggiori gli utenti che utilizzano sistemi anonimi per non essere

“tracciati” (Castells,2001). Come avvertono gli esperti di marketing questo comporta da un lato l’accrescersi dei costi per ottenere le informazioni, dall’altro la perdita di fiducia da parte del consumatore nei confronti dell’azienda (Rust, Kannan, Peng, 2002). Le misure adottate fino ad ora dalle aziende come l’adozione del protocollo *P3P* nei pc, che permette di decidere la protezione desiderata, rispetto alla quantità di informazioni che ogni volta vengono cedute durante la connessioni alla Rete, risultano insufficienti. Come infatti viene fatto notare esse sembrano essere misure temporanee, tampone diremmo noi, che l’attuale sviluppo tecnologico rende costantemente inefficaci (Reidenberg, 2001; Rust, Kannan, Peng,2002).

In tutto questo processo risalta fuori una delle prerogative del potere: quella dell’asimmetria del Sapere. Le aziende hanno informazioni sempre maggiori sugli individui, mentre gli stessi non sono a conoscenza di nessun aspetto circa il trattamento delle informazioni da loro fornite, né tantomeno delle modalità attraverso le quali si forniscono (Reidenberg, 2001).

Quello che sembra emergere è la richiesta di un ripensamento delle dinamiche che vengono attuate dalle aziende per cercare di ottenere informazioni sui consumatori. La soluzione, a nostro avviso, può essere ottenuta soltanto basandosi sulla strategia che ha sempre fondato la Rete: collaborazione e cooperazione. La creazione di politiche adeguate per lo sviluppo della stessa deve tener conto di tutti gli attori in campo, il popolo della rete, le aziende ed i governi, e far si che essi dialoghino a livello paritario. L’asimmetria delle relazioni oggi presente, in cui le

aziende, soprattutto quelle di software, sono ai vertici, detenendo sia il Sapere tecnologico che quello sugli individui, non può portare da nessuna parte tranne che ad un aumento massiccio della sorveglianza e del potere delle aziende stesse.

4.2 Lavoratori

La nostra escursione dei sistemi di sorveglianza è partita dalla fabbrica in quanto era il primo grande luogo in cui una serie di individui dovevano lavorare insieme ad un processo produttivo. In essa erano (e lo sono ancora) presenti la sorveglianza *del* lavoro che concerneva i processi di produzione e la sorveglianza *come* lavoro in quanto vi erano agenti che operavano da guardiani (Marx,1867). La fabbrica è uno di quelli che Foucault ha definito come *dispositivi* ,che hanno la funzione di *normalizzare* l'individuo (Foucault,1975). Il cambiamento della fabbrica e lo sviluppo delle nuove tecnologie non ha fatto altro che mantenere gli aspetti della sorveglianza, rafforzandone le capacità e aumentando i settori in cui la stessa va ad applicarsi. Una delle caratteristiche che viene evidenziata nell'adozione delle nuove tecnologie è che in moltissimi casi, come vedremmo, esse vengono adottate per un uso e finiscono in maniera indiretta per essere utilizzate come strumenti di controllo dei lavoratori.

Partendo proprio dalla fabbrica possiamo vedere in quale maniera questo è successo. La

ristrutturazione del capitalismo ha comportato, come abbiamo notato, un cambiamento delle pratiche gestionali. Nelle politiche aziendali diventa centrale la soddisfazione del cliente, e questo comporta una maggiore attenzione in quel settore che viene definito come “controllo di qualità”. Ad una richiesta del consumatore l’azienda deve sempre saper rispondere in maniera adeguata, se questo lamenta un problema riguardo un prodotto, l’azienda deve sapere da quale fabbrica il problema è partito, per quale motivo, e che tipo di falla può avere. Per risolvere il problema le aziende hanno inserito delle *tags* sui loro prodotti. Queste *tags* possono essere dei dispositivi elettronici, ma nella maggior parte dei casi sono delle semplici combinazioni alfanumeriche che possiamo vedere su ogni prodotto che abbiamo in casa, che indicano qual è lo stabilimento di produzione, la data e l’ora ed altre indicazioni che riguardano l’azienda. Si è fatto strada il concetto di *rintracciabilità* del prodotto per tutelare il consumatore. Il sistema di tracciatura per le aziende serve da un lato per tutelarsi e dall’altro, riuscendo ad individuare la causa di un problema, si presta ad essere un ottimo strumento per controllare la produzione.

Insieme a questa pratica si afferma quella del *just in time*. La produzione sul momento, alla richiesta diretta dei concessionari, degli uffici vendita. Per fare questo c’è bisogno della costruzione di sistemi informatici che operino tra loro scambiandosi le informazioni in tempo reale: l’ufficio vendita riceve un ordine; il software gestionale, comparando i dati di vendita precedenti con le scorte di magazzino, si collega alla fabbrica di produzione che gestisce la sua

area e le indica la quantità dei prodotti che le servono; la fabbrica fa partire la produzione del prodotto alla richiesta e contatta i servizi di trasporto; alla consegna monitora la spedizione attraverso le reti dell'azienda di trasporto; quest'ultima consegna il prodotto alle mani dell'ufficio vendita. Le comunicazioni fra le varie parti avvengono in tempo reale. Aziende come Cisco System vendono essenzialmente reti gestionali. Attraverso questi sistemi imprese come Zara riescono a rimodellare costantemente la propria produzione di capi d'abbigliamento seguendo giornalmente i gusti del pubblico, arrivando a produrre 12.000 capi d'abbigliamento l'anno rifornendo i propri punti vendita circa due volte al mese (Castells,2001).

L'operaio in fabbrica, grazie a questi sistemi, è praticamente estraneo al processo di produzione in quanto questo completamente automatizzato. All'operaio spetta il compito del controllo di qualità, quello di rilevare falle della produzione, possibili difetti. L'operaio, grazie ai sistemi di rintracciabilità e a sistemi di rilevamento elettronici che vengono posizionati nella sua area di lavoro per segnalare sue mancanze, sa di essere costantemente monitorato dal *management*. La tecnologia permette da un lato di gestire tutta la produzione e rilevare falle, dall'altro all'effetto, più o meno desiderato, di essere uno strumento in grado di controllare l'operaio. Controllo aumentato dall'utilizzo di sistemi di videosorveglianza ormai situati in tutti gli impianti. In questo contesto l'aumento delle nuove tecnologie in fabbrica sembra comportare per gli operai una maggiore forma di "autodisciplina". Un assoggettamento volontario in

quanto sanno che ogni loro sbaglio sarà verificabile. Inoltre, come osserva Lyon,

> più che altro le IT sembrano contribuire al mantenimento della posizione del capitale sul luogo di lavoro, preservando le relazioni diseguali tra capitale e lavoro, in un momento in cui i metrodi gestionali più antiquati cominciavano a mostrare la corda (Lyon,1994,op.cit.,p.179).

Come in Marx, a tutt'oggi possiamo vedere la stessa *strategia gestionale* essere portatrice delle pratiche di sorveglianza. Discorso diverso se invece andiamo ad analizzare lo sviluppo delle nuove tecnologie applicato in tutti quei settori che fanno dei sistemi informatici i loro strumenti di lavoro.

Le aziende che utilizzano tali strumenti si trovano a dover far fronte ad altri tipi di problemi che riguardano gli impiegati. Uno dei reati che comportano maggiori danni alle aziende è quello che viene definito come "furto di tempo macchina": l'impiegato che durante l'orario di lavoro fa un uso improrio dello strumento in sua dotazione. Questo avviene quando utilizza il telefono aziendale per telefonate personali, quando invia e-mail private utilizzando il pc dell'impresa, quando naviga in rete per i propri interessi attraverso la connessione aziendale. I danni causati dalla sottrazione del tempo all'orario di lavoro e dall'utilizzo improprio delle macchine si stima siano la causa, potrà sembrare assurdo, di circa il trenta per cento dei fallimenti aziendali negli U.S.A (Strano, 2000). Un altro danno rilevante per aziende che lavorano in determinati settori è quello comportato dal cosidetto "spionaggio industriale". Per tutelarsi è

normale che esse cerchino di sviluppare strumenti di controllo in maniera tale da arginare i fenomeni. Castells a questo proposito evidenzia come circa il settantacinque per cento delle aziende negli U.S.A. monitori costantemente le e-mail dei dipendenti. Basta dotarsi di programmi come *Gatekeeper* che mostrano tutta l'attività del server e tutte le connessioni (Castells, 2001) e vengono sviluppati sistemi che permettono il controllo delle battute in maniera tale da saper quantificare il lavoro svolto (Lyon,1994). In tutti questi casi si può facilmente vedere come lo strumento di lavoro diventi esso stesso strumento di sorveglianza.

Un caso da evidenziare nel settore lavorativo è quello dei call-center. Uno studio svolto dalla Lankshear e dai suoi collaboratori in quest'area di lavoro ha condotto gli autori a sviluppare interessanti conclusioni. Loro evidenziano come nei call-center vengano attuati essenzialmemte due tipi di sistemi di sorveglianza: il primo attraverso un sistema automatico di gestione delle chiamate, il secondo con la possibilità di accesso remoto al telefono dell'operatore (Lankshear, Cook, Mason, Coates, Button, 2001).

L'*ACD* (*Automatic Call Dialling System*) nato per gestire le chiamate, riesce ad essere uno strumento in grado di quantificare il lavoro svolto registrando i tempi di chiamate e il periodo di inattività del sistema di ciascun operatore. Mentre la seconda pratica riguarda la registrazione o l'ascolto delle chiamate. La giustificazione aziendale è che questo rappresenti una protezione per l'azienda a livello legale, infatti avere le registrazioni di tutte le chiamate rende possibile

sapere sempre come ci si è comportati con un cliente. Questo però comporta la possibilità del *management* di ascoltare le chiamate e controllare così gli impiegati.

Quello che emerge dalla ricerca della Lankshear è che in molti casi la registrazione è stata usata per decidere chi dover riassumere o meno (Lankshear, Cook, Mason, Coates, Button,2001), ma l'aspetto più rilevante riguarda il tipo di controllo effettuato. A differenza della fabbrica dove i segni della sorveglianza sono quasi sempre visibili, all'interno dei call-center, come delle altre aziende che utilizzano strumenti informatici, la sorveglianza è attuata per mezzo di strumenti invisibili. L'impiegato non sa mai quando è controllato, non ha la possibilità di vedere il controllore. L'operatore telefonico non sa mai quando dall'altra parte il *management* sta ascoltando la sua chiamata, vive in un perenne stato d'incertezza. In questo caso il modello di sorveglianza ricalca a pieno il Panopticon benthamiano, e come questo, riesce ad essere un dispositivo autodisciplinante (Lankshear, Cook, Mason, Coates, Button,2001). Ma aldilà dei modelli, siano essi pan-ottici o meno, quello che viene evidenziato da più parti è l'aumento massiccio degli strumenti in grado di monitorare il lavoro.

I sistemi di video sorveglianza, giustificati nei grandi magazzini in quanto deterrenti ai furti, vengono utilizzati in tutte le aree lavorative siano esse aziende, fabbriche, università, garantendo da un lato la sicurezza del luogo e dall'altro un monitoraggio continuo del lavoratore (Froomkin, 2000; Lyon, 1994, 2001; Marx G.T., 2001,2002).

L'utilizzo di badge d'accesso a determinate aree piuttosto che altre garantisce al management di

sapere in ogni momento dove il singolo lavoratore si trova (Lyon, 1994, 2001).

Le aziende per tutelarsi utilizzano screening genetici ed analisi mediche per individuare la possibile insorgenza di malattie causate dal lavoro sull'operaio, ma questi strumenti da un altro lato si prestano ad essere ottimi strumenti di controllo sugli individui. Come evidenziano Lyon e Ball si è arrivati ad utilizzare particolari bagni che in maniera casuale analizzano le urine dei lavoratori per verificare che essi non siano dediti all'utilizzo di alcool o sostanze stupefacenti (Ball, 2003; Lyon, 2001).

La maggioranza degli autori fino a qui citati evidenzia come tutti questi strumenti di sorveglianza, monitorando costantemente il lavoratore, tendano a scoraggiare l'unione sindacale in tutti quei luoghi di lavoro in cui non viene gradita.

Un ulteriore aspetto da rilevare del controllo sui lavoratori è quello che riguarda le tecniche di *profiling*. All'interno delle aziende la *strategia dell'esclusione/inclusione* può risultare determinate per l'assunzione di un candidato rispetto ad un altro. Sapere con precisione quante più informazioni possibili su un lavoratore permette alle aziende di potersi tutelare notevolmente da possibili incidenti. Le aziende in sede di preselezione si rivolgono ad altre aziende per sapere se fra i suoi candidati ci sono "attivisti politici" o "hacker", o altre tipologie di lavoratori che risultino non gradite (Lyon,1994). È evidente anche in questo caso come la *data-image*, il *Sé virtuale* di un individuo, possa avere un potere discriminante sulla persona reale.

L'aspetto preoccupante di questa richiesta di informazioni da parte delle aziende appare maggiormente rilevante se lo mettiamo in correlazione con i dati biometrici. Negli ultimi tempi esse cercano di ottenere anche i dati sensibili, come le informazioni sullo stato di salute familiare, per tutelare se stesse. Le analisi fatte effettuare ai lavoratori possono portare a sapere se i candidati fanno uso di sostanze stupefacenti, se le donne sono incinte, inoltre l'analisi del Dna può dare importanti informazioni sulla mappatura genetica dell'individuo. Come abbiamo evidenziato in precedenza, le assicurazioni possono decidere di non assicurare determinati individui solo perché potenzialmente soggetti a determinate malattie. Il test genetico si presta ad essere uno strumento fortemente discriminante in sede di assunzione (Cockfield, 2004; Lyon, 2001; Parthasarathy, 2004; Rifkin, 1998).

Come avverte il Garante per la Protezione della Privacy Stefano Rodotà in un articolo su *La Repubblica*[18] i dati genetici rappresentano la nostra individualità più profonda, possono essere grandi strumenti predittivi per l'insorgere di nuove malattie e possono permettere di curare predisposizioni genetiche potenzialmente dannose. Ma nel momento in cui le aziende vanno alla ricerca di questi dati per tutelarsi il pericolo è quello di creare una "*sottoclasse*, una categoria di non assicurabili e di non assumibili". La legislazione europea fino ad ora è incentrata sulla tutela di queste informazioni, ma negli U.S.A. le compagnie di assicurazioni possono avere accesso a questi dati nel momento in cui devono concedere un

[18] *Se il mercato scheda la salute del cittadino*, in *La repubblica* del 14/07/2003.

mutuo ad una persona. Il pericolo di una schedatura di massa a livello genetico potrebbe comportare, continua Rodotà, la nascita di una "concorrenza genetica" e di una "eugenetica di mercato": coloro i quali possiedono una buona condizione genetica potrebbero chiedere particolari condizioni di vantaggio agli assicuratori, mentre gli altri verrebbero del tutto esclusi. In questo modo la *strategia dell'esclusione/inclusione* riuscirebbe ad affinare moltissimo le sue capacità. La nascita di profili genetici può comportare che

> le stesse nozioni di società e di giustizia potrebbero essere trasformate. La meritocrazia potrebbe lasciare spazio alla "genetocrazia", con individui, gruppi etnici e razze sempre più catalogati in base al genotipo, dando il via all'emergere di un "informale" sistema di caste biologiche nei Paesi di tutto il mondo (Rifkin,1998,p.28).

Casi in cui la discriminazione è avvenuta sono tutt'altro che irreali e Lyon ne riporta almeno cinque (Lyon,1994;2001), mentre Rifkin citando uno studio condotto da Lisa Gender del Dipartimento di Neurobiologia di Harvard afferma che su 917 individui esaminati, 455 avevano avuto esperienze di discriminazione basate sui profili genetici (Rifkin,1998).

In più Lyon sottolinea come le compagnie assicurative tendano a non assicurare i lavoratori che abitano in determinate aree, particolarmente svantaggiate, perché più facile venire aggrediti e simili. In questo modo si condanna un individuo a svolgere solo quelle mansioni più umili dove l'assicurazione non viene richiesta (Lyon,2001). In parole povere un nero

che abita ad Harlem potrebbe non riuscire mai ad ottenere un impiego buono, anche se ha studiato, se continuasse a vivere in quella zona, perché nessuna assicurazione lo tutelerebbe, e lo stesso se un individuo risultasse avere un “genotipo” non buono.

Inoltre è bene evidenziare che le legislazioni vigenti variano tantissimo da paese a paese. La Parthasarathy in un suo recente studio vede come negli U.S.A. il problema ha coinvolto una serie di organismi, esperti, commissioni, avvocati, che hanno concordato che il diritto individuale alla privacy è maggiore rispetto a quello delle compagnie assicurative di ottenere informazioni, mentre in Gran Bretagna il dibattito ha portato alla formulazione dell’idea che il diritto individuale deve essere controbilanciato a quello delle assicurazioni. Ed esse possono ottenere informazioni genetiche per tutte le polizze che superano i centomila dollari (Parthasarathy, 2004).

Alla luce della globalizzazione dei flussi informatici e dell’utilizzo di particolari software in dotazione ai settori pubblici, è lecito domandarsi fino a che punto la legislazione nazionale riesca ad arginare il fenomeno nel momento in cui le aziende si configurano come *attori* transnazionali, e riescano ad entrare i possesso di informazioni riservate semplicemente sfruttando questi software. Per usare una metafora di Lyon vediamo che i database che raccolgono i nostri dati sono “contenitori che perdono”.

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'implentazione, 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 verrano 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

[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.

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;

[20] L'informativa è visualizzabile all'indirizzo: http://www.skytv.it/Offerta/PopUp_Privacy.htm

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).

[21] Si veda nota precedente

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 e-mail. 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

[22] L'informativa sulla privacy della XBox Live è disponibile all'indirizzo: http://www.xbox.com/it-IT/live/privacystatement.htm

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

[23] Il documento è visionabile in lingua inglese all'indirizzo: http://www.interlex.it/testi/pdf/wd5035.pdf

concerne la Direttiva sulla Privacy (n. 95/46/CE), che prevede per tutti gli Stati non appartenti 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 costamente 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

[24] http://www.realnetworks.com/local/it/guids.html

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

[25] Fonte Logitech :http://www.logitech.com/index.cfm?page=utilities/home&contentid=4056&countryid=16&languageid=5

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 gratuitamentre 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 apllicativi 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.

[26] A questo proposto si veda l'articolo su *Punto Informatico* all'indirizzo http://punto-informatico.it/p.asp?i=47390b

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:

[27] L'indirizzo è: http://www.microsoft.com/windows/windowsmedia/IT/software/v7/privacy.asp#_What_personal_identifiable

> 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 inizialmemente 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

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

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'utiizzo 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.

[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

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

[31] Vedi nota ventinove

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 discipilna 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 trafficco. 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 effettuata possono sapere in ogni

zona quali classi socioecomiche 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 aereoporti, nelle università e nelle scuole, agli incroci dei semafori, lungo i varchi eletronici, 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:

[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

- 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.

[33] In Italia questo impiego non'è permesso.

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): "novita' - e' 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 impeghi 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 aereoporti 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.

[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

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 pre-esistente) 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 minaccie. 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 aereoporti 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 allontare le bande giovanili da quell'area e spostare così in un altro luogo la possibile criminalità (Lyon, 1994), mentre nelle metropolitane è utilizzato per allontare 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 esatezza 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

[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

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

[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

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 aereoporti 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 ricevere 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

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

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

[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.

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'ìdentificazione 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

[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://punto-informatico.it/archivio/trovato.asp?sel=0&sand=Viaggio%20nel%20mondo%20RFID

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 apllicazioni 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*

[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

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 forniglierle, come invece avviene per le carte di credito e quelle fedeltà.

[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

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

[48] Si veda Wacquant L., 1999.

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 incrocieranno 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 esatezza 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

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

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

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

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

[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

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

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

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).

[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 .

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 riguaradanti 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.

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

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 richiedavano 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 discrimazione 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 ampiamenti discussi precedentemente. Quello che deve essere sottolineato è la grande

[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

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 anti-globalizzazione. 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.

[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.

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 sacedorti, 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 democratrico, 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 soggiocati 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 verrano 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?idcontent=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/PaperProfiling.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_Position_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/may012000/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=454143 .
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 post-bipolare.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://punto-informatico.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 self-regulation*, 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/19eubiometric.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).