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 sottoponiamo 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 gestisca 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 accettandone, 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 Statonazione 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 cosiddetti *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].
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 "cittadinanza 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 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 quest'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 probabilità 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 determinato 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 costantemente 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 tracce 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 *Decretolegge 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: poiché 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 può 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 é possibile ricavare i loro dati sensibili, cioé 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 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 aeroporti 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 territorio 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 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'appartenenza 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 prelevano 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 applicati 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 monitorare 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 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'attacco 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'intelligence 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 diciassette 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 (Bamford, 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 tortuose. 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 attacchi 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 dataimmagine, 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 digressione 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 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 assisteremmo 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.

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.
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 utilizzeranno 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 tracce 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 massmedia. 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 determinati 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 interfaccie 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 dispositivo 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 passaggio 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 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 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 nominativi 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'esclusione/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 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 metodi 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 improprio 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 cosiddetto "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 essenzialmente 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 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".