

## Filippo Domenicali

# ESISTE UNA “FILOSOFIA DELLA SORVEGLIANZA”?

### ABSTRACT

Prendendo spunto dal sottotitolo dell'edizione italiana di uno scritto di David Lyon, intendo porre la domanda: “dietro l'apparente eterogeneità delle pratiche di sorveglianza contemporanee, c'è una “filosofia della sorveglianza”? Pochi anni fa si era soliti definire queste pratiche “sorveglianza disorganizzata”, oggi, sotto la pressione del pericolo ubiquo, i dispositivi di controllo tendono a convergere in database centralizzati. Sosterrò che questa filosofia esiste, è il suo nocciolo è la simulazione, cioè l'anticipazione sistematica delle condotte rischiose.

### 1. SOCIETÀ DELL'INFORMAZIONE, SOCIETÀ DELLA SORVEGLIANZA

Da oltre vent'anni sentiamo ormai parlare di “società dell'informazione”<sup>1</sup> per caratterizzare uno dei tratti salienti delle società occidentali avanzate. Questa definizione, spesso elogiativa, è utile a caratterizzare la seconda natura assunta dal nostro presente, che ha sempre più bisogno delle tecnologie, di quella informatica in particolare, per adempiere alle funzioni principali della nostra vita quotidiana. Il computer è ormai diventato, anche in conseguenza dell'abbassamento dei costi, un oggetto d'uso domestico, parte integrante delle nostre case. Il telefonino è assurto al ruolo di status symbol e non saremmo quasi in grado di vivere senza. Se in un saggio di quarant'anni fa Thompson affermava che l'orologio è stato la tecnologia di definizione della modernità, oggi si può affermare senza tema di smentita che il computer ha la medesima funzione nel nostro mondo postmoderno<sup>2</sup>. Con un'importante differenza però: lo è ad un livello esponenzialmente maggiore. Con il termine “tecnologia di definizione” intendiamo quegli strumenti capaci di coordinare le nostre attività sociali, e permettere l'ordinato svolgimento delle funzioni della vita quotidiana. Indubbiamente questa esplosione dell'uso delle tecnologie della comunicazione ha apportato enormi vantaggi, vent'anni fa nemmeno immaginabili, consentendo il collegamento e la diffusione in tempo reale da una parte all'altra del pianeta di ogni tipo d'informazione, e costituendo in questo modo la piattaforma tecnologica di base del nostro mondo globalizzato.

---

<sup>1</sup> Cfr. tra le tante analisi in particolare quelle di J. BENIGER, *Le origini della società dell'informazione. La rivoluzione del controllo*, UTET, Torino, 1995, D. LYON, *La società dell'informazione*, Il Mulino, Bologna, 1991, M. CASTELLS, *La nascita della società in rete*, Università Bocconi Editore, Milano, 2002.

<sup>2</sup> E. P. THOMPSON, *Time, Work-discipline and Industrial Capitalism*, in “Past and Present”, n. 38, 1967.

In questo saggio vorrei però soffermarmi sul lato oscuro della globalizzazione dell'informazione, per mettere in risalto quello che si potrebbe chiamare il "rischio elettronico" connesso a questa capillare estensione delle tecnologie informatiche. Non bisogna infatti dimenticare, come ammonisce il sociologo canadese David Lyon, che la società dell'informazione è, per sua stessa natura, una società sorvegliata<sup>3</sup>. La domanda alla quale vorrei rispondere, prendendo come riferimento temporale una periodizzazione senz'altro controversa (moderno/postmoderno)<sup>4</sup>, è se nel passaggio dalla modernità alla postmodernità vi sia stata una mutazione qualitativa da parte dei criteri stessi che organizzano le pratiche di sorveglianza, ovvero se possiamo affermare di essere oggi di fronte ad una nuova "logica" e ad una nuova "filosofia" della sorveglianza. Con il termine "logica" o "filosofia" intendo indicare quei criteri di selezione e quelle direttrici di sviluppo verso le quali ci stiamo impercettibilmente muovendo, un nuovo orizzonte verso il quale siamo protesi, e che al momento non abbiamo ancora definitivamente raggiunto. Mettere in guardia contro i nuovi rischi elettronici ha dunque il significato di concettualizzare una tendenza, per poterla affrontare in maniera responsabile. Non è infatti mia intenzione biasimare o sottovalutare gli enormi benefici, in termini di risparmio di tempo e diffusione delle conoscenze, consentiti dai mezzi di comunicazione elettronica. Si tratta piuttosto di raggiungere una nuova consapevolezza che ci consenta di valutarli in modo critico.

Lo scambio elettronico globale di informazioni è quindi mediato da elaboratori elettronici che le diffondono, lavorano, archiviano. Una prima differenza fondamentale che sussiste tra la sorveglianza tradizionale "a vista" e quella attuale è data dal fatto che siamo entrati nell'era della "dataveglia"<sup>5</sup>. Non è infatti più necessario disporre di un mezzo oculare per tenere sotto controllo gli individui, ma questo può essere ottenuto in modo diretto attraverso il raffronto in tempo reale dei dati, cioè delle scie o tracce elettroniche che ogni individuo si lascia alle spalle in ogni momento della sua vita quotidiana. È d'obbligo infatti notare l'attuale proliferazione dei sistemi che funzionano attraverso le *smart card* o i *badge*, schede plastificate provviste di microchip

---

<sup>3</sup> «Le società che per le loro procedure amministrative e di controllo dipendono dalle tecnologie della comunicazione e dell'informazione sono società sorvegliate. Gli effetti di ciò sono percepibili nella vita quotidiana, la quale è strettamente monitorata come mai prima era successo nella storia». D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002 p. 1.

<sup>4</sup> L'opposizione "moderno/postmoderno" in questa sede vuole avere un senso prima di tutto esplicativo. Se in campi come la filosofia, la sociologia o la storia questa definizione non ha ancora conquistato un pieno diritto di cittadinanza, negli studi sulla sorveglianza può essere invece sicuramente d'aiuto per concettualizzare la sostanziale differenza esistente tra una modernità ed un postmoderno fatti di pratiche qualitativamente e tecnologicamente differenti. Approfondiremo meglio questo aspetto più avanti.

<sup>5</sup> La dataveglia viene messa in atto concretamente con tecniche come il *data-mining* e il *computer-matching*, che permettono di incrociare e raffrontare istantaneamente i dati riguardanti un singolo soggetto. Queste tecniche consentono, senza arrivare alla visione diretta, di monitorare ugualmente il comportamento, gli spostamenti e le transazioni dell'individuo controllato, fornendo un'immagine straordinariamente precisa della sua vita reale.

o banda magnetica in grado di memorizzare tutte le nostre transazioni, in numerosi ambiti della vita quotidiana (carte fedeltà, telepass, tessera della biblioteca, carta di credito, tessera sanitaria, patente, carta d'identità elettronica...). Ci stiamo muovendo verso quella che può essere definita una "badge-generation" per cui ogni spostamento richiederà sempre più spesso un pass in grado di garantire l'accesso a determinate strutture o a determinati servizi. Un mondo apparentemente più libero e che offre maggiori possibilità, ma irto di barriere. Il nostro tempo è stato definito, e a ragione, un'era dell'accesso<sup>6</sup>, un tempo cioè in cui è il guardiano virtuale, il database, a farla da padrone. La disciplina non ha più bisogno di essere impartita attraverso coercizioni evidenti, ma si attua istantaneamente attraverso codici d'accesso che decidono chi può entrare nell'era globale e chi deve invece rimanere ai margini. La dataveglianza, il controllo in tempo reale dell'informazione, costituisce quindi il *modus operandi* degli attuali sistemi di sicurezza. All'occhio umano si sostituiscono le capacità di elaborazione del computer, che ne moltiplicano la potenza e l'efficacia.

## 2. IL PERICOLO UBIQUO

Il secondo punto da tenere in considerazione riguarda le cause di questa formidabile estensione del controllo. Le società contemporanee, come aveva già notato Michel Foucault nel corso degli anni '70, devono far fronte ad una vera e propria "cultura politica del pericolo":

«Il liberalismo si impegna in un meccanismo in cui sarà tenuto, in ogni istante, ad arbitrare la libertà e la sicurezza degli individui attorno alla nozione di pericolo. [...] Pericoli continuamente suscitati, riattualizzati, messi in circolazione da quella che potremmo chiamare la *cultura politica del pericolo*. [...] La seconda conseguenza del liberalismo e dell'arte liberale di governare, è la formidabile estensione delle procedure di controllo, di costrizione e coercizione, destinate a costituire una sorta di contropartita e di contrappeso delle libertà. [...] Terza conseguenza è la comparsa, in questa nuova arte di governo, di meccanismi che hanno la funzione di produrre, ispirare ed accrescere la libertà, introducendo un sovrappiù di controllo e di intervento. Vale a dire che il controllo non funge più, in questo caso, da contrappeso necessario alla libertà, [...] diventa piuttosto il principio motore della libertà».<sup>7</sup>

Si tratta quindi di "società del rischio"<sup>8</sup> poiché le tecnologie di sorveglianza elettronica intendono rispondere ad una domanda di sicurezza crescente. È utile infatti notare che i regimi politici cosiddetti liberali o neoliberali, con la loro rivendicazione di una maggiore libertà per il maggior numero di individui si trovano perennemente in una situazione di "impasse" che ne condiziona il funzionamento. Ogni libertà garantita ha infatti costantemente bisogno di essere protetta, e questa protezione costituisce sovente l'antitesi della libertà stessa, in quanto richiede un controllo sempre

---

<sup>6</sup> J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, Mondadori, Milano, 2000.

<sup>7</sup> M. FOUCAULT, *Nascita della biopolitica. Corso al Collège de France (1978-1979)*, Feltrinelli, Milano, 2005, pp. 68-70 (corsivo mio).

<sup>8</sup> U. BECK, *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2000.

più capillare del corpo sociale nel suo insieme. È la nota antitesi tra libertà e sicurezza, croce e delizia dei nostri politologi. Più cerchiamo di allargare il campo della libertà di circolazione e della libertà d'azione degli individui più siamo costretti a quadrettare questo campo e ad intensificare i meccanismi di sicurezza che hanno il compito di garantire questi stessi movimenti e azioni. Nel momento in cui diviene tecnologicamente possibile tenere sotto controllo un numero sempre maggiore di individui attraverso le tecnologie elettroniche ed informatiche ecco che la libertà comincia a dileguare. Per la politica si tratta dunque di ricercare continuamente la quadratura del cerchio, cioè l'equazione aurea capace di garantire un maximum di libertà gravata da un minimo sufficiente di controllo. C'è da chiedersi se questo obiettivo, dal punto di vista del potere, sia davvero auspicabile, o se invece queste tecnologie non vengano utilizzate per indurre, provocare alcuni tipi di comportamento che, certo, hanno importanti effetti economici. Sarei quindi tentato di raffigurare il campo della sicurezza contemporanea come un mercato, in cui, ad una richiesta globale di sicurezza, in parte indotta da quella cultura generalizzata del pericolo di cui parlavo prima, fa riscontro una risposta da parte dello Stato, o da chi è incaricato di esercitare il potere nel proprio ambito di pertinenza, che è tesa non alla soppressione completa del pericolo, ma alla selezione continua di un certo tipo di pericoli, che inducono determinati comportamenti, che a loro volta hanno determinati effetti. Questa specie di circolo vizioso consente infatti lo svolgimento e il perdurare di una società ben ordinata, che necessita sempre, come in un sistema immunitario sano<sup>9</sup>, di una certa quantità del suo opposto: caos, disordine, delinquenza, pericolo.

La parola d'ordine, quando si tratta di questo genere di problemi, potrebbe sicuramente essere "privacy". Ma occorre individuare, prima di tutto, "chi" attenta all'integrità di questa privacy? C'è stato un cambiamento fondamentale proprio in questi ultimi anni, notato da Lyon: se infatti nel suo importante saggio del 1994 (*L'occhio elettronico*) aveva messo in guardia i lettori dalla sempre maggiore invadenza della società dei consumi nella nostra vita quotidiana, ed aveva trattato soprattutto dei pericoli delle intrusioni pubblicitarie nella vita degli individui abitanti nel ricco Occidente, a partire dall'11 settembre 2001 c'è da registrare una brusca inversione di rotta. Nel suo ultimo saggio (*Massima sicurezza*)<sup>10</sup> la prospettiva è cambiata diametralmente; egli afferma infatti che dopo gli attacchi alle Twin Towers quella che bisogna temere in primo luogo è diventata l'intrusione da parte dello Stato nella vita dei cittadini, che in nome della sicurezza nazionale è

---

<sup>9</sup> Faccio qui riferimento al modello avanzato dal filosofo Roberto Esposito per spiegare il funzionamento dell'attuale paradigma biopolitico, che presiede al funzionamento delle società liberali. A proposito dell'"ipertrofia degli apparati di sicurezza" che caratterizzano sempre più diffusamente le società contemporanee, egli afferma: «Si può vedere in essa il punto cieco cui sembra pervenire il loro sviluppo: dal momento che tale sindrome autoprotettiva non soltanto finisce per relegare sullo sfondo ogni altro interesse – e anzi l'"interesse" stesso come forma di vita-in-comune – ma produce l'effetto opposto rispetto a quello desiderato. Anziché adeguare la protezione all'effettivo livello di rischio, tende ad adeguare la percezione del rischio al crescente bisogno di protezione – facendo così della stessa protezione uno dei maggiori rischi». R. ESPOSITO, *Immunitas. Protezione e negazione della vita*, Einaudi, Torino, 2001, p. 19.

<sup>10</sup> Il titolo originale è, significativamente, *Surveillance after September 11*.

arrivato a varare leggi sempre più restrittive che consentono maggiori poteri di controllo ai governi nazionali, e a quello degli Stati Uniti in particolare. La legislazione americana che ha fatto seguito ai terribili fatti dell'11 Settembre, segnatamente il "Patriot act"<sup>11</sup>, ha infatti ristretto i limiti della libertà dei cittadini consentendo al governo di intervenire sempre più spesso e anche in modo indiscriminato nella vita privata degli stessi, attentando alla sicurezza dei dati personali, che possono venire passati al setaccio anche in base ad un semplice sospetto. L'area del "sospetto categoriale" si è così notevolmente estesa ed allargata a tutti coloro che, per un motivo o per l'altro, possono essere considerati "individui a rischio" e che così vedono minata sia la loro privacy che la loro libertà d'azione e di movimento. Con queste misure estreme entriamo dunque in un orizzonte probabilistico all'interno del quale lo Stato si fa carico della catalogazione e della suddivisione in categorie di rischio delle "data-immagini" degli individui che compongono una popolazione. La data-immagine rappresenta infatti il doppio virtuale della nostra identità reale, ed è ottenuta facendo la somma di tutte le tracce elettroniche che inevitabilmente rimangono memorizzate all'interno dei diversi database con i quali abbiamo abitualmente a che fare. Se all'inizio dell'era informatica questi archivi elettronici erano in qualche modo disorganizzati e disomogenei, la tendenza attuale, favorita dalla globalizzazione dei mercati, è quella ad una convergenza sempre più massiccia in grandi database collegati da un linguaggio e da codici comuni. In questo modo diviene possibile ottenere la tracciabilità completa delle attività degli individui, che costituisce un quadro esauriente della loro personalità e delle loro attitudini (siti Internet visitati, transazioni effettuate, movimenti compiuti, ma anche e-mail o messaggi elettronici inviati, idee espresse, ecc. ecc.). Sotto la pressione di un pericolo ubiquo ogni intrusione finisce per diventare tollerabile, poiché ne va della sicurezza nazionale. Questo tipo di sicurezza implica anche la necessità da parte dei governi di conservare il più possibile il segreto e di filtrare continuamente l'informazione diffusa, un sistema che non permette ai comuni cittadini di rendersi conto dell'effettiva gravità del pericolo, e quindi di farsi un'idea sulla realtà o meno dei rischi che vengono loro paventati. Così ci troviamo di fronte ad una vistosa asimmetria, che ha poco a che fare con un regime democratico: da una parte i governi, per ragioni di sicurezza, non descrivono chiaramente il livello del rischio; dall'altra i comuni cittadini, non disponendo di informazioni precise, non possono far altro che accettare ciecamente le misure che vengono loro imposte.

---

<sup>11</sup> Cfr. l'articolo di Guido Olimpio apparso sul "Corriere della sera" del 16 Giugno 2005, dal titolo: *Usa, poteri speciali dopo l'11 settembre. Il Patriot Act*, nel quale l'autore afferma che «L'Fbi, con l'appoggio della Casa Bianca, da agenzia di polizia si trasforma in corpo spionistico. I federali chiedono di poter acquisire dati (conti bancari, Internet, cartelle cliniche) senza dover richiedere l'autorizzazione di un magistrato a patto che esista "un ragionevole sospetto" nei confronti di un cittadino [...] In alcuni casi l'Fbi non deve neppure faticare. Grandi gruppi hanno messo a disposizione delle autorità federali i loro database. Numeri di carte di credito usate per pagare una spedizione, contenuto del pacco, riferimenti personali sono stati passati alla polizia. I servizi di sicurezza di alcune società hanno creato uffici di collegamento con l'Fbi organizzando una propria polizia. Conseguenza: il fattorino che ti recapita un pacco è incoraggiato a segnalare qualsiasi cosa "sospetta"».

Un'efficace metafora utilizzata per schematizzare il funzionamento delle attuali forme di sorveglianza è quella del Panopticon. Sappiamo infatti che il progetto del Panopticon (elaborato per la prima volta da Jeremy Bentham nel 1791)<sup>12</sup> è stato usato da Foucault per indicare i metodi di funzionamento della sorveglianza e della disciplina degli individui durante tutta l'età moderna: fabbriche, caserme, scuole, ospedali, prigionie hanno utilizzato questa elementare forma di controllo costituita dalla disposizione architettonica degli spazi per la produzione di forza lavoro ben addestrata, la base di una società ordinata<sup>13</sup>. In tempi più recenti, altri autori, penso in particolare al sociologo americano Mark Poster, hanno ripreso questa metafora per descrivere l'attuale funzionamento delle società dell'informazione (sorvegliate)<sup>14</sup>. Poster ha messo in evidenza come il Panopticon contemporaneo sia oggi costituito dal database, che egli definisce un Superpanopticon, in quanto, da un solo punto d'osservazione, è in grado di catalogare e di vedere un numero altissimo di data-immagini, cioè di profili virtuali degli individui. Se il biopotere studiato da Foucault è costituito da due assi, uno individualizzante rivolto al controllo dell'individuo, ed uno massificante rivolto alla gestione delle popolazioni prese in massa<sup>15</sup>, è chiaro che il Superpanopticon elettronico racchiude entrambe le funzioni all'interno di un solo dispositivo, divenendo una tecnologia di controllo indispensabile al funzionamento del biopotere. La metafora del Panopticon mi sembra utile anche a caratterizzare le differenze tra i sistemi di sorveglianza conosciuti dalla modernità e quelli in voga nel nostro tempo, che per chiarezza ho definito postmoderno. So bene che la definizione è molto spesso osteggiata e messa in dubbio dai filosofi e dai sociologi, ma vorrei sottolineare come in questo campo si sia di fronte ad una vera e propria differenza qualitativa: il Panopticon benthamiano funzionava soprattutto attraverso una calcolata economia della distribuzione degli spazi, tesa alla visibilità totale, anche se si trattava di un sistema oculare che poteva esercitarsi soltanto all'interno di spazi chiusi (istituzioni totali) e quadrettati; il Superpanopticon elettronico invece funziona attraverso lo spionaggio automatizzato delle data-immagini, una modalità di controllo che si effettua attraverso la raccolta, la selezione e l'incrocio dei dati personali, e che prosegue ben oltre le istituzioni chiuse, prolungandosi fin all'interno delle mura domestiche, e, per così dire, non molla mai la presa<sup>16</sup>. Pensiamo all'esempio del telefonino,

---

<sup>12</sup> J. BENTHAM, *Panopticon. Ovvero la casa d'ispezione*, a cura di M. Foucault e M. Perrot, Marsilio, Venezia, 1983.

<sup>13</sup> M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino, 1977, pp. 213-247.

<sup>14</sup> M. POSTER, *Foucault, Marxism and History. Mode of Production versus Mode of Information*, Polity Press, Cambridge, 1984, pp. 102-104, e anche *The Mode of Information. Poststructuralism and Social Context*, Polity Press, Cambridge, 1990, pp. 93-103.

<sup>15</sup> M. FOUCAULT, *La volontà di sapere. Storia della sessualità I*, Feltrinelli, Milano, 1978, pp. 119-128 (in particolare p. 123).

<sup>16</sup> Su queste importanti trasformazioni delle funzioni panottiche, che qui mi limito ad accennare, mi permetto di rinviare al mio *Dal panopticon architettonico al panopticon elettronico. Prospettive foucaultiane*, in "I castelli di Yale", n.7, 2004, pp. 83-97.

del controllo dei tabulati e del segnale microcella che viene emesso anche a telefono spento<sup>17</sup>. In breve, non c'è più un "fuori".

### 3. IL POTERE DI Google

Oggi il Superpanopticon è Google. Questo motore di ricerca, divenuto in breve tempo il più usato al mondo, ha una capacità di penetrazione e di controllo fino a ieri impensabile, grazie alla tecnologia "double click" è in grado di memorizzare la serie completa degli spostamenti degli utenti, registrando i siti visitati e le preferenze di ciascuno. "Sapere è potere" diceva Bacone, ed oggi è più vero che mai. L'immensa memoria dei database di Google, capace di contenere i dati personali di miliardi di utenti diffusi su tutta la superficie del globo, database sottoposti a controlli praticamente inesistenti, suscita importanti interrogativi etici che non possiamo sottovalutare: è giusto che un'azienda privata possa diventare "l'ecosistema dell'informazione del mondo" rimanendo senza obblighi né responsabilità, e capace di trattare alla pari, molto spesso addirittura in posizione di preminenza, con i governi nazionali? Non bisogna dimenticare, e i fatti degli ultimi mesi sembrano darci ragione, visto che queste poderose banche dati hanno suscitato le attenzioni e le mire del governo degli Stati Uniti, che si è prodigato parecchio per avervi accesso<sup>18</sup>. La tecnologia di Internet, inizialmente nata per scopi militari, è stata infatti messa a punto dallo stesso governo americano, che vorrebbe ora esercitare una specie di "diritto di paternità" che gli permettesse di accedere, per motivi di sicurezza, al controllo mondiale degli utenti. A questo tipo di ingerenza gli ideatori del motore di ricerca, Larry Page e Sergey Brin, hanno finora opposto un netto rifiuto motivato dai loro sogni visionari e intrisi di messianesimo liberale. Essi infatti si autorappresentano come benefattori dell'umanità mossi da un anticonformismo liberal; ma le recenti trattative con il governo cinese, in seguito alle quali hanno accettato di censurare il proprio motore di ricerca togliendo termini come "diritti umani" e "democrazia" pur di penetrare in questo immenso mercato in estensione, hanno motivo di suscitare nuovi dubbi e nuove paure sull'effettiva sicurezza del sistema<sup>19</sup>. La sorveglianza elettronica può

---

<sup>17</sup> Per definire la gravità del problema è utile far riferimento ad alcuni articoli apparsi sul "Corriere della sera" nel Febbraio 2005, che mettevano in guardia rispetto alla proliferazione delle intercettazioni telefoniche. Particolarmente interessanti sono quelli di Lorenzo Salvia: *Troppi cellulari intercettati. La Tim: Esaurite le linee*, del 20 Febbraio e *Cellulari, aumentano le intercettazioni illegali*, del 25, in cui l'autore espone importanti considerazioni riguardanti l'uso e l'abuso delle intercettazioni per prevenire e sanzionare i reati, che ha portato in breve tempo al raggiungimento del massimo delle linee intercettate. Sull'importanza del telefonino e sulla tendenza all'accentramento "palmare" delle funzioni dei computer rimando al bel saggio di M. FERRARIS, *Dove sei? Ontologia del telefonino*, Bompiani, Milano, 2005, che offre all'autore l'occasione per esporre brillanti considerazioni su questo nostro presente *hi-tech*.

<sup>18</sup> Faccio riferimento a quanto scritto da Ennio Caretto sul "Corriere della sera" del 21 Gennaio 2006 in un articolo intitolato. *Google a Bush: i dati restano segreti*, a proposito del rifiuto opposto dal motore di ricerca al governo americano che tentava di appropriarsi delle sue banche dati: «L'amministrazione Bush vuole che Google, il re dei motori di ricerca su Internet, diventi uno "sceriffo elettronico". Per la precisione che le consegni milioni di pagine della sua banca dati, le più cliccate dagli utenti, e i tabulati di una settimana campione delle visite dei navigatori».

<sup>19</sup> Si veda il medesimo articolo di Caretto del 21 Gennaio.

quindi essere descritta secondo il modello della rete aperta, progettata per creare continuamente nuovi nodi e nuove ramificazioni. Un potere reticolare diffuso e onnipresente, che colonizza di continuo nuovi territori e nuovi spazi virtuali, che hanno però significative ricadute e significativi effetti concreti sulla vita reale dei cittadini, sempre più sottoposta a nuovi obblighi e nuovi controlli<sup>20</sup>.

#### 4. LA NUOVA “FILOSOFIA DELLA SORVEGLIANZA”

A questo punto possiamo cominciare ad affrontare il tema centrale di questo saggio. Prendendo a prestito il sottotitolo dell'edizione italiana di un importante volume di David Lyon, ho intenzione di porre la domanda: “è possibile definire l'attuale filosofia della sorveglianza?”<sup>21</sup> Mi sembra che occorra fare alcune osservazioni preliminari. Nel campo di studi sulla sorveglianza, campo di nascita recente del resto<sup>22</sup>, si è parlato a lungo delle pratiche di controllo contemporanee nei termini di una “sorveglianza disorganizzata” in quanto le diverse agenzie incaricate di monitorare i dati degli utenti fanno generalmente capo ad enti o ad imprese diverse e quindi rendono frammentata la raccolta dei dati che sono suddivisi in campi e finalità molto diversificate tra loro (agenzie di marketing mirato, enti statali, istituzioni, luoghi di lavoro, ecc.). La pressione del pericolo ubiquo, abbiamo detto, ha invertito questa tendenza alla frammentazione, facendo sì al contrario che questa immensa mole di dati transiti, oppure divenga sempre più accessibile, per database centralizzati che hanno la capacità di raccogliere ed elaborare i dati dispersi al fine di costruire una data-immagine sufficientemente precisa dei singoli individui. È inutile notare che questa volontà di precisione deve necessariamente scontrarsi con delle necessità di approssimazione dovute alla staticità forzata dei codici cataloganti, la quale fa sì che la data-immagine in realtà differisca dalla personalità reale del soggetto analizzato, in quanto è in ogni caso una “caricatura”, ma una caricatura che viene presa dannatamente sul serio<sup>23</sup>. Non possiamo fare a meno di notare<sup>23</sup> che la personalità umana, per fortuna,

---

<sup>20</sup> Cfr. l'interessante articolo di J. E. CAMPBELL e M. CARLSON, *Panopticon.com. Online Surveillance and the Commodification of Privacy*, in “Journal of Broadcasting & Electronic Media”, December 2002, pp. 586-606.

<sup>21</sup> Il volume in questione è *The Electronic Eye. The Rise of Surveillance Society*, 1994 (trad. It: *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Feltrinelli, Milano, 1997).

<sup>22</sup> David Lyon, il massimo esperto mondiale di questo genere di studi, lavora da oltre un decennio alla fondazione di uno speciale sottosettore di studi sulla sorveglianza, i cosiddetti *Surveillance Studies*. La nascita di questo sottosettore, secondo lo stesso Lyon, è resa possibile «sia dalla proliferazione della sorveglianza informatizzata, sia dalla riconosciuta importanza che Michel Foucault aveva dedicato al nesso potere-sapere», D. LYON, *La società sorvegliata*, cit., p. 152. In questa direzione si muovono anche le sue ricerche accademiche, egli infatti è uno dei promotori del *The Surveillance Project* (<http://www.queensu.ca/sociology/Surveillance/intro.htm>) attivato presso il Dipartimento di Sociologia della Queen's University di Kingston, Ontario.

<sup>23</sup> Come ha giustamente osservato Mark Poster, il linguaggio elettronico opera attraverso una serie di “griglie di specificazione”, provviste di un numero limitato di categorie e di campi. I database impiegano categorie linguistiche per classificare e schedare i dati che riguardano gli individui. Durante questo processo, avvengono però delle distorsioni: «La codificazione digitale impone la sua griglia limitativa e cambia il suo materiale nel farlo. La sorveglianza tramite

è sempre più ricca e più varia, contiene un numero di sfumature più alto di quanto potrà mai descriverla una macchina elettronica, anche se provvista di programmi intelligenti incaricati di manovrarla. Dicevamo, lo scambio e la circolazione di queste data-immagini è divenuto sempre più esteso e massiccio, ed ha portato a superare quella disorganizzazione iniziale, creando un sistema mondiale sempre più accentrato e convergente.

Oltre alle finalità di *intelligence* legate all'emergenza del terrorismo internazionale e alla pubblica sicurezza bisogna infatti considerare le tendenze all'informatizzazione dei registri nel campo della burocrazia e della pubblica amministrazione. Quella che Max Weber aveva definito una "gabbia d'acciaio" potrebbe divenire oggi una "gabbia elettronica" non appena si sia terminato di ristrutturare l'amministrazione dello Stato su base informatica. A quel punto sarà possibile, da un solo terminale, ottenere la fotografia esaustiva degli individui suddivisa nei diversi settori che costituiscono la loro vita pubblica, e privata. Vista la perenne situazione di indigenza in cui si ritrovano le pubbliche amministrazioni, i tagli di personale e di fondi, sembra naturale aspettarsi un'amministrazione sempre più leggera, che delega ai computer gran parte del lavoro cartaceo precedentemente svolto all'interno degli uffici pubblici e che porterà infine alla sostituzione dei *dossier* personalizzati con archivi elettronici, facendo intravedere scenari anche abbastanza inquietanti. Sarà allora possibile controllare in modo automatico, per esempio i mancati pagamenti delle bollette, o qualunque tipo di irregolarità fiscale, che porteranno alla conoscenza, sebbene attraverso dati in qualche modo indiretti, della personalità degli individui schedati e dei dettagli personali della loro vita quotidiana. Se gli Stati moderni hanno raggiunto la stabilità interna del loro ordine pubblico attraverso un lungo processo di educazione e disciplinamento della popolazione, che si è compiuto in un arco temporale molto esteso, e che conveniamo di chiamare "modernità", potrebbe affacciarsi la possibilità di un disciplinamento di tipo diverso, attraverso il controllo degli individui mediato dall'informatica. Stabilire in tempo reale il "normale" e il "deviante" non è più pura fantasia.

Se infatti consideriamo quell'immenso sapere, immenso per il suo valore, che può essere raccolto dai database, un sapere che riguarda i cittadini, e a questo sapere aggiungiamo l'uso di una serie di *cliché* derivati dalla psicologia, modelli di comportamento e tipi di reazione elaborati in modo statistico, ecco che diviene possibile "prevedere" in base al comportamento passato, ciò che un singolo individuo può essere in grado di fare, e quindi la "quantità di rischio" di cui è portatore. Dal punto di vista del potere che sorveglia potrebbe diventare auspicabile una specie di stima del

---

mezzi di informazione codificata digitalmente costituisce nuovi soggetti con il linguaggio impiegato nei database». Secondo Poster bisogna quindi attribuire un ruolo produttivo al linguaggio elettronico. Il database infatti «impone un nuovo linguaggio sopra quelli già esistenti che è un linguaggio impoverito e limitato, che usa la norma per costruire gli individui e definire i devianti [...] la struttura o la grammatica dei database crea rapporti tra pezzi di informazioni che non esistono in quei rapporti fuori dai database». M. POSTER, *The Mode of Information*, cit., pp. 94-96 (trad. mia).

rischio connesso all'esistenza di una certa categoria di individui, rischio che si tratterebbe poi di neutralizzare o controllare sempre più da vicino. Quella attuale, come l'ha definita il sociologo Zygmunt Bauman, è realmente una "società dell'incertezza"<sup>24</sup>, come ho cercato di dimostrare, si tratta sempre più di un'incertezza che va gestita, che non può essere annullata del tutto ma che ci porta in un orizzonte probabilistico all'interno del quale i fatti sociali fluttuano in un certo senso tra un massimo ed un minimo, e devono essere tenuti all'interno dei valori che volta per volta vengono definiti normali da una serie di interventi e di mosse da parte delle istanze incaricate di esercitare il potere, lo Stato e la polizia. Vi è tutta una serie di fenomeni che costituiscono quello che ho definito il "disordine" che è chiaramente impossibile debellare del tutto, e che dal punto di vista del governo vanno inseriti in campi d'utilità. Un governo economico, uno Stato leggero e liberale come quelli delle società Occidentali avanzate non possono infatti permettersi di utilizzare sistemi totalitari da Stato di polizia, che hanno alti costi, sia monetari che d'immagine politica; l'opinione pubblica è sempre più sensibile, in tempi di crisi, ai temi del risparmio e dell'economia, e non accetterebbe il controllo poliziesco per nessuna ragione. I governi attuali sono dunque in un certo senso costretti a muoversi attraverso meccanismi indiretti, che agiscono in modo silenzioso e invisibile all'interno del corpo sociale, poco appariscenti, in modo da non dover pagare, o pagare il meno possibile, il costo politico dell'intensificazione della stretta sui cittadini. Così è utile valutare la portata delle campagne stampa pro- o contro- determinate misure di intervento o determinati provvedimenti, ed è qui che la diffusione delle informazioni assume una portata politica e il loro controllo diventa una posta in gioco fondamentale. Si tratta quindi non di imporre una condotta, ma d'agire per mezzo di dispositivi<sup>25</sup> che inducono surrettiziamente un certo tipo di comportamento, che nelle menti dei cittadini devono poter prevalere in quanto legati al metro dell'interesse e del vantaggio personale. La consapevolezza di poter essere osservati in qualunque momento della nostra vita pubblica, e in parecchi di quella privata, la sola possibilità concreta di poter essere scoperti mentre si commette un illecito deve bilanciare la volontà o l'utilità del compierlo, modificando in modo decisivo l'interesse dei cittadini verso comportamenti trasgressivi e incentivando al contrario le condotte virtuose. È la

---

<sup>24</sup> Z. BAUMAN, *La società dell'incertezza*, Il Mulino, Bologna, 1999.

<sup>25</sup> Per la definizione del significato del termine "dispositivo", fondamentale nel lessico foucaultiano, rinvio alla bella, anche se un po' complessa, lettura data da G. Deleuze: «Ma che cos'è un dispositivo? È innanzi tutto un groviglio, un insieme multilineare. È composto da linee di diversa natura [...] Sbrogliare le linee di un dispositivo, in ogni caso, è tracciare una mappa, cartografare, percorrere terre sconosciute, ed è ciò che egli chiama "lavoro sul campo" [...] Le due prime dimensioni di un dispositivo, o quelle che Foucault districa per prime, sono curve di visibilità e curve di enunciazione». G. DELEUZE, *Che cos'è un dispositivo?*, in *Divenire molteplice. Nietzsche, Foucault ed altri intercessori*, Ombre Corte, Verona, 1999, pp. 64-65. Il Panopticon di Bentham è un perfetto esempio di dispositivo di sorveglianza, in quanto combina delle linee di visibilità, garantite dallo sfruttamento degli spazi architettonici, e linee di enunciazione costituite dai regolamenti disciplinari in vigore al suo interno. A queste due linee principali, che concernono il visibile e l'enunciabile (le parole e le cose), va aggiunta una terza linea, di *soggettivazione*, in quanto da questi spazi e da questi regolamenti viene prodotto un nuovo tipo di soggetto, "disciplinato" e obbediente. È un vero e proprio dispositivo per la trasformazione degli individui.

stessa meccanica degli interessi a funzionare da deterrente, ed è questa meccanica l'obiettivo del potere più invisibile ed economico, che si radica direttamente nelle menti e nelle rappresentazioni dei soggetti.

## 5. LA SIMULAZIONE CHE SORVEGLIA

Viviamo sempre più immersi nell'iperreale. Il termine coniato dal sociologo francese J. Baudrillard trent'anni or sono mi sembra oggi di stretta attualità<sup>26</sup>. L'iperreale è un luogo, anzi un non-luogo, fatto di simulacri, di previsioni, di stime, di calcoli statistici, e costituisce il nostro futuro prossimo. Non si tratta più di analizzare i dati oggettivi attuali, ma di concettualizzare delle tendenze di sviluppo. Lo schema temporale di questa nuova logica della sorveglianza è aperto verso il futuro, tanto che si potrebbe sostenere che in questo tipo di razionalità non è più il presente o il passato ad essere centrale, quanto piuttosto tutta quella serie aperta di eventi, soltanto probabili, che dallo stato di cose attuali potrebbero scaturire (una possibilità fissata in grafici e percentuali). L'incertezza del presente genera l'ansia e la paura del futuro, alla quale rispondiamo cercando di prevedere continuamente ciò che si staglia all'orizzonte. Le forme di sapere che assumono importanza sono quelle che ci permettono di individuare i pericoli prima che possano giungere a costituire una reale minaccia. È per questo motivo che diventa fondamentale comprendere la "filosofia" delle attuali pratiche di sorveglianza, una filosofia costituita da un nocciolo di razionalità che si estende allargando le proprie maglie e stabilendo sempre nuove connessioni tra i punti della rete. Secondo Gilles Deleuze non si tratta più di una forma di controllo che si presenta come "stampo", esprimendosi nelle istituzioni chiuse che impartiscono a tutti lo stesso addestramento, ma piuttosto di un sistema capace di integrare le differenze individuali, e che porta ad estenderle a dismisura: più siamo "globali" e, cittadini delle società occidentali avanzate, lasciamo dietro di noi un numero maggiore di tracce e di scie elettroniche, più esse permettono di approfondire la conoscenza della nostra personalità; più ci muoviamo, più lasciamo tracce. Per questo la nuova sorveglianza lavora in un assetto a "geometria variabile" in grado di adattarsi al potenziale differenziale degli individui<sup>27</sup>.

---

<sup>26</sup> Cfr. J. BAUDRILLARD, *Simulacri e impostura. Bestie, Beaubourg, apparenze e altri oggetti*, Cappelli Editore, Bologna, 1980, pp. 45-95.

<sup>27</sup> In un importante saggio scritto negli ultimi anni della sua vita Gilles Deleuze cerca di concettualizzare la differenza tra le forme di potere della modernità, costituite dal modello dell'internamento, e quelle nuove forme di controllo che si affacciano al nostro presente. In questo modo egli stabilisce un'opposizione tra internamento e controllo, che si ripercuote su quella tra società disciplinari e società di controllo: «I diversi internati o ambienti di internamento attraverso cui passa l'individuo sono variabili indipendenti: si presume che ogni volta si ricominci da zero, ed un linguaggio comune a tutti questi ambienti esiste, ma è *analogico*. Mentre i diversi controllati sono variazioni inseparabili, che formano un sistema a geometria variabile il cui linguaggio è *numerico* (che non vuol dire necessariamente binario). Gli internamenti sono *stampi*, dei calchi distinti, ma i controlli sono una *modulazione*, qualcosa come un calco autodeformante che cambia continuamente, da un istante all'altro, o qualcosa come un setaccio le cui maglie divergono da una zona all'altra [...] Non c'è bisogno di ricorrere alla fantascienza per concepire un

L'iperreale è il campo della *simulazione*<sup>28</sup>, vera parola chiave per comprendere l'evoluzione dei sistemi di sorveglianza informatizzati. I sistemi di sicurezza sono mossi sempre più dalla volontà di anticipare i comportamenti umani, cogliendoli ancor prima che si verifichino, al fine di scongiurare il maggior numero possibile di pericoli. Questa tendenza, proprio perché mira ad ottenere degli effetti sugli individui, si lega necessariamente alle cosiddette "scienze umane", e alla psicologia in particolare.

La psicologia del comportamento umano permette infatti di suddividere gli individui in categorie legate alle loro singole particolarità, ed in questo senso può fornire agli ingegneri informatici un aiuto concreto nello stabilire i criteri delle macchine automatizzate per la sorveglianza. Questi sistemi non sono fantascienza, ma vengono già utilizzati da alcuni anni nelle parti più avanzate del pianeta. È noto che nella metropolitana di Londra è stato installato un sistema di telecamere intelligenti, chiamato *Cromatica*, in grado di prevedere i comportamenti suicidi<sup>29</sup>. Vediamo come funziona: da una parte vi sono delle telecamere puntate sui binari della metro, che scannerizzano uno ad uno i passeggeri pronti per l'imbarco; dall'altra questa tecnologia di riconoscimento viene associata a degli schemi di comportamento derivati dalla psicologia e dalla statistica, che ci dicono che un individuo prima di gettarsi sui binari attende il passaggio di un certo numero di convogli. La telecamera che l'osserva, tenendo conto di quanto tempo l'individuo aspetta sulla linea gialla, dopo un certo numero di minuti allerta direttamente la polizia, che provvede a controllare il soggetto dal comportamento sospetto, ed eventualmente a dissuaderlo dal folle gesto. *Cromatica* è un perfetto esempio di tecnologia di sorveglianza preventiva, che segue una logica della simulazione e dell'anticipazione del comportamento futuro. Se questa razionalità sorvegliante dovesse affermarsi appieno, è chiaro che vi sarebbe una forte contraddizione con i principi dei diritti civili dei cittadini. Pensiamo infatti che difficilmente sistemi di questo tipo potrebbero essere accettati in modo acritico all'interno di una democrazia. Non può essere che un reato venga sanzionato *prima* di essere compiuto! Si dice: "prevenire è meglio che curare"; verissimo. Bisogna però comprendere se questa prevenzione generalizzata sia effettivamente efficace, e se questa estensione in realtà poi non costi

---

meccanismo di controllo che ad ogni istante dia la posizione di un elemento in ambiente aperto, animale in una riserva, uomo in un'impresa (collare elettronico). Félix Guattari immaginava una città in cui ciascuno potesse lasciare il proprio appartamento, la propria via, il proprio quartiere grazie a una personale carta elettronica (dividuale) capace di rimuovere questa o quella barriera; ma, d'altro lato, che la carta potesse essere respinta il tale giorno, o a una tale ora; quello che conta non è la barriera, ma il computer che individua la posizione di ciascuno, lecita o illecita, e opera una modulazione universale». G. DELEUZE, *Poscritto sulle società di controllo*, in *Pourparler. 1972-1990*, Quodlibet, Macerata, 2000, pp. 235-240.

<sup>28</sup> Il testo di riferimento per questo genere di considerazioni è indubbiamente quello di W. BOGARD, *The Simulation of Surveillance. Hypercontrol in Telematic Societies*, Cambridge University Press, Cambridge, 1996.

<sup>29</sup> Cfr. D. LYON, *La società sorvegliata*, cit., pp. 77-82.

in termini di erosione dei diritti civili più di quanto possa realmente offrire in termini di incremento della sicurezza.

Lo stesso discorso vale per quei sistemi di sorveglianza “algoritmica” e automatizzata che si basano sull’uso di speciali “dizionari” sull’esempio del sistema Echelon<sup>30</sup>. Anche in questo caso abbiamo a che fare con un orecchio globale che, dallo spazio, ascolta tutte le comunicazioni che avvengono sulla terra. Questo sistema, in orbita da anni, tanto da essere divenuto ormai leggendario, si attiva in base al rilevamento di “parole chiave” contenute in uno speciale dizionario. È sufficiente proferire o digitare una certa parola considerata sospetta per essere immediatamente ed automaticamente soggetti a controllo.

È inutile dire che queste misure, intrise di una furia tecnologica senza pari, lasciano il tempo che trovano. Quella che invece è necessaria, è una nuova consapevolezza dei cittadini che porti ad una presa di coscienza critica del nostro rapporto con le tecnologie. Viviamo nel sogno che sia possibile risolvere tutti i problemi attraverso l’uso massiccio della tecnica. In questo mondo esisterebbero solo problemi tecnici e nessun problema morale, tutto sarebbe risolvibile col metodo dello schiaccianoci. Il rispetto per l’integrità della persona deve invece essere proclamato a voce alta. Per definire questo rispetto occorre però un nuovo vocabolario, che si confronti con i problemi del presente e sia all’altezza di affrontarli. Occorre una nuova tavola dei diritti civili, al cui interno siano ponderate la protezione dei dati personali e il diritto alla riservatezza in alcuni campi che riguardano la vita privata. Il concetto di privacy non è che l’inizio<sup>31</sup>. È importante comprendere che non si può pensare di risolvere i problemi della sicurezza dei cittadini esclusivamente attraverso l’introduzione di nuovi controlli, perché questo fa sì che inevitabilmente l’antinomia libertà/sicurezza continui a rovesciarsi nel proprio opposto non appena si modificano i dati iniziali. Si tratta di un equilibrio

---

<sup>30</sup> Cfr. D. CAMPBELL, *Il mondo sotto sorveglianza: ‘Echelon’ e lo spionaggio elettronico globale*, Eleuthera, Milano, 2002.

<sup>31</sup> Esso rappresenta un punto di partenza, che merita di essere esteso ed integrato il più possibile. Secondo Stefano Rodotà dobbiamo puntare al pieno raggiungimento di quattro “diritti” civili fondamentali nell’era della sorveglianza elettronica: «- deve divenire componente essenziale della privacy, e dunque essere rafforzato ed esteso, il ‘diritto di opposizione’ a determinate forme di raccolta e di circolazione delle informazioni personali [...] - la stessa logica dev’essere seguita per rendere effettivo il ‘diritto di non sapere’, che può essere considerato come una specificazione del diritto di opposizione. [...] - dev’essere reso più netto e stringente il ‘principio di finalità’, che condiziona la legittimità della raccolta delle informazioni personali alla preventiva comunicazione all’interessato dei modi in cui verranno utilizzate le informazioni raccolte; [...] - deve assumere maggior rilievo il ‘diritto all’oblio’ prevedendo che talune categorie di informazioni debbano essere distrutte, o conservate solo in forma aggregata e anonima, una volta che sia stata raggiunta la finalità per la quale erano state raccolte o dopo che sia trascorso un determinato periodo di tempo». S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, pp. 156-158 (corsivo mio).

delicato. Ciò che manca, è dunque una nuova “etica della sorveglianza”<sup>32</sup> capace di far fronte alle nuove forme di discriminazione digitale che sempre si producono.

Vorrei concludere citando un passaggio della relazione annuale tenuta dallo stesso Stefano Rodotà nelle vesti di Presidente dell’Authority per la privacy:

«Non dimentichiamo che la rivoluzione elettronica è una rivoluzione giovane e, come tutti i grandi cambiamenti tecnologici del passato, è entrata nella società civile con una certa prepotenza, con possibili effetti di inquinamento. Da anni si lavora per liberare l’ambiente dalle emissioni nocive, dai rumori insopportabili, dalle aggressioni alla natura, che sono state conseguenze pesanti della prima rivoluzione industriale. È tempo che strategie analoghe vengano intraprese per cancellare le diverse forme d’inquinamento dell’ambiente informativo e delle libertà civili. Diventa così evidente che non v’è contraddizione tra tecnologia e *privacy*, ma che, al contrario, vi sono forme benefiche di alleanza da incentivare in ogni modo»<sup>33</sup>.

---

<sup>32</sup> Sui problemi dell’etica nella società della tecnica rimane fondamentale, a mio avviso, il contributo di Hans Jonas che riflette sull’attuale “vuoto etico”, uno spazio bianco che è necessario colmare al più presto, attraverso una più approfondita conoscenza dei rischi per l’individuo e la sua vita privata, generati dall’enorme estensione delle tecnologie in tutti i settori della vita quotidiana. Cfr. H. JONAS, *Il principio responsabilità. Un’etica per la civiltà tecnologica*, Einaudi, Torino, 1990, pp. 3-32.

<sup>33</sup> Si tratta di un passaggio preso dalla relazione annuale tenuta il 9 Febbraio 2005, l’ultima tenuta da Rodotà in veste di Presidente dell’Authority, reperibile al sito <http://www.garanteprivacy.it/garante/doc.jsp?ID=1093776>.