# Tecnologie della visibilità

## Annotazioni sulle pratiche di sorveglianza

**Andrea Mubi Brighenti**

**Abstract** La sorveglianza si costituisce come un insieme di relazioni socio-tecniche che danno forma a relazioni di visibilità e intervisibilità. Il testo presenta brevemente alcuni nessi ritenuti centrali per meglio comprendere il rapporto tra lo sviluppo e l'applicazione di tecnologie che riconfigurano le relazioni di visibilità tra soggetti, siti ed eventi sociali. In particolare, si focalizza su come il corpo individuale e il corpo della popolazione formino due poli o due campi di azione del controllo, e su come i fattori di docilità, partecipazione e "sociabilità" vengano mobilizzati nelle nuove formazioni di sorveglianza.

**Keywords** sorveglianza; visibilità; anatomopolitica; biopolitica; tecniche di gestione dell'informazione

### 1. L'istituzione socio-tecnica dei regimi di visibilità

Alle pratiche di sorveglianza viene spesso associato un significato sociale ambiguo, oscillante tra controllo e cura. Osservatori e commentatori diversi sono proni a sottolineare alternativamente l'uno o altro aspetto, ma è evidente che i due procedono insieme. Tuttavia, per comprendere più accuratamente come le misure di sorveglianza odierne possano modificare la vita sociale, politica, culturale e istituzionale, oltre che le relazioni interpersonali, non è sufficiente limitarsi a queste caratterizzazioni generali, per così dire "di massima", bensì è necessario analizzare le forme della sorveglianza come un insieme di relazioni socio-tecniche che gestiscono, distribuiscono e modificano relazioni di visibilità e intervisibilità tra le parti.

In questo momento storico ci troviamo di fronte a una molteplicità dei luoghi sociali di sorveglianza (Lyon 2007, §2), dato che essa viene oggi condotta in una pluralità di situazioni da parte di organizzazioni di tipo molto diverso (ad esempio organizzazioni militari, di polizia, di intelligence, mediche, commerciali, assicurative) per finalità altrettanto diverse (ad esempio il controllo dei propri impiegati, dei propri concorrenti, e in generale dei "clienti" della propria organizzazione – intendendo il termine in senso ampio, tale che ad esempio i devianti possono venire

TECNOSCIENZA
Italian Journal of Science & Technology Studies
Volume 2(2) pp. 85-101 - ISSN 2038-3460
http://www.tecnoscienza.net



T/S TECNOSCIENZA
Italian Journal of Science & Technology Studies

considerati come "clienti" delle agenzie di polizia, e così via).

Nella maggior parte di simili casi, l'introduzione di sistemi e misure di sorveglianza è guidata da una ragione tecnocratica, anche quando la finalità della sorveglianza sia di altro tipo (politica, economica, personale etc.), ovvero dalla fiducia che la disponibilità di informazioni e di dati raccolti migliorerà l'efficienza di prestazione dell'organizzazione nel raggiungimento delle sue finalità. Perlomeno, questa è la razionalizzazione più facile da produrre, dato che in effetti tale efficacia è molto difficile da dimostrare a causa dell'ampio numero di variabili presenti in ciascuna situazione; in effetti, molto spesso l'efficacia si rivela essere un presupposto più che una vera e propria dimostrazione – o, se si vuole, una retorica di cui certi attori e certe istituzioni si servono per finalità di comunicazione pubblica e di costruzione della propria immagine. Andrebbe però anche approfondita e valutata l'ipotesi che la sorveglianza possa essere una strategia in cui entrano in gioco fattori diversi da quelli di un semplice calcolo dei costi e dei benefici, o in alternativa nel cui calcolo dei costi e dei benefici rientrano fattori diversi da quelli pubblicamente dichiarati. Va inoltre considerato un aspetto che si potrebbe chiamare di "supererogazione", rilevato per primo da Jacques Ellul (1965): secondo Ellul, a causa della natura auto-accrescitiva e monista della tecnica, lo strumento tecnico tende a venire applicato dappertutto per il solo fatto che è possibile applicarlo. Questa sorta di logica espansionista della sorveglianza è stata in seguito rimarcata da numerosi altri osservatori. La riflessione sulle finalità per cui si cerca di manipolare la visibilità non può però condurre lontano qualora non si considerino le modalità concrete e le strutture attraverso le quali tale manipolazione viene condotta.

Può essere interessante rilevare che, essendo la sorveglianza una pratica organizzata – e dunque anche una pratica organizzativa – essa opera attraverso l'istituzione di *regimi* di visibilità. Un regime di visibilità è un'architettura sistematica di dispositivi e norme – anche se, occorre precisare, tale sistematicità non esclude affatto la presenza di elementi e attività discrezionali o persino arbitrarie e discriminatorie. Quel che accade all'interno di ogni regime di visibilità è il delinearsi di un asse pubblicità–privatezza, o divulgazione–segreto, sul quale, come rilevato inizialmente da Simmel (1908, trad. it. 1998, §5) (a cui da questo punto di vista va attribuito il riconoscimento di ispiratore della sociologia della sorveglianza) la distribuzione delle informazioni e delle conoscenze è differenziale e selettiva, creatrice tanto di legame sociale quanto di effetti di potere (o, più precisamente, di ciò che in seguito si è designato con il termine dominazione). Il concetto stesso di segreto, secondo Simmel, amplia la vita sociale in quanto vi introduce l'idea che, accanto al mondo sociale evidente, esista un intero altro mondo potenzialmente conoscibile ma non conosciuto. Attraverso l'idea di segreto, la sorveglianza trasforma la gestione di informazioni disposte lungo l'asse divulgazione–segreto in effetti di potere. Come più recentemente ha notato Gary Marx (2005), essa implica una gestione di confini in un doppio senso: da un lato, la sorveglianza istituisce e rafforza confini creando "profili" (di sospetti, clienti, lavoratori, abitudini di consumo, voto e così via) funzionali a un trattamento differenziale dei soggetti; dall'altro lato, essa scavalca o elimina confini, consistendo in una violazione sistematica di informazioni inizialmente intese come private o segrete.

## 2. Sorveglianza, docilità e partecipazione

Ora, è evidente che tali manipolazioni della visibilità non si riducono semplicemente a dati visuali, ma includono un più ampio campo delle percettibilità sociali che definiscono il *plenum* del qui-ed-ora (Brighenti 2010). È stato fatto notare che nella società contemporanea un aspetto sempre più centrale delle pratiche di sorveglianza è quello di poter tracciare e controllare informazioni e flussi di dati in formato digitale. Si tratta di informazioni non necessariamente visuali ma che in ogni caso, perché vi sia sorveglianza, devono venire *visibilizzate*. Secondo gli studiosi, l'intero processo passa in questo modo dall'essere imperniato sulle persone e sui loro corpi fisici all'esserlo su codici e dati numerici informatizzati (Ericson e Haggerty 2000; Lyon 2001, 2003). Al fine di valutare meglio questa tesi, può comunque essere utile esaminarla in un contesto storico e concettuale più ampio, ad esempio risalendo all'opera incomparabile di Michel Foucault. Per Foucault (1975), come è noto, la razionalità originaria della sorveglianza in quanto tecnologia di potere consisteva nel collocare l'individuo all'interno di un diagramma fisico e di rapporti di forze (in altri termini, in una istituzione chiusa) al fine di indurlo ad assumere una serie di atteggiamenti calcolati in anticipo. In rapporto a questa definizione, è innegabile che simili pratiche di sorveglianza esistano ancora.

Si consideri ad esempio il caso dei check-in agli aeroporti: il fatto di sapere che si dovrà passare attraverso un sistema di sicurezza e un metal detector – e che si sarà dunque, a tutti gli effetti, visibilizzati – induce la maggior parte delle persone a "docilizzare" il proprio corpo, non solo sottomettendosi a un certosino rituale di ispezione ma anche predisponendosi a rendere tale ispezione la più facile e fluida possibile per gli ispettori. Tutta la situazione è strutturata come un dispositivo che attraversa un insieme socio-tecnico e che lo "lavora"; sicché, se la situazione non viene contestata nel suo complesso, eventuali atti di resistenza plateali non verranno interpretati come orgogliose affermazioni di libertà ma solo come semplici intralci alla circolazione generale. Gli studi sull'introduzione di scanner a raggi X di tipo Backscatter negli aeroporti (Amoore e Hall 2009) ci ricordano inoltre come le modalità di visibilizzazione dei corpi dei passeggeri potrebbero in breve tempo raggiungere livelli di imbarazzante precisione – anche se simili riflessioni, che sicuramente catturano l'immaginazione pubblica e suscitano vociferanti reazioni da parte dei commentatori, risultano naif laddove non si consideri l'intero regime di visibilità in questione. Nel senso foucaultiano, la sorveglianza non dipende che in parte dal fatto che il passaggio attraverso il rettangolo del metal detector o dello scanner modello Backscatter produca dei dati su di noi, bensì dal fatto che tale consapevolezza della visibilizzazione si trasforma nella disposizione che ciascuno di noi adotta mettendosi in fila dietro gli altri, controllando il proprio corpo per rimuovere oggetti di metallo, predisponendosi a venire ispezionato e così via.

Effetti di sorveglianza di questo tipo sono riscontrabili anche in altri casi. Ad esempio, in alcuni comuni inglesi (il Regno Unito essendo uno dei paesi più videosorvegliati al mondo) le telecamere di sorveglianza a circuito chiuso installate ufficialmente per finalità di controllo della devianza e di sicurezza della proprietà privata sono state impiegate per punire un insieme di illegalità minori, o anche sem-

plici irregolarità, tra le quali il non rimuovere gli escrementi del proprio cane, il non eseguire la raccolta differenziata nel modo corretto, l'affiggere volantini senza permesso, il fumare o bere in luoghi non consentiti e così via. Evidentemente, il fatto di rendere pubblicamente noti simili utilizzi delle telecamere di sorveglianza mira a indurre un effetto di auto-normazione negli abitanti. Se è pur possibile che qualche ammenda sia stata emessa sulla base di informazioni raccolte attraverso questi strumenti di sorveglianza, non si comprenderebbe davvero il funzionamento di tale diagramma di visibilità se non si includesse il fattore della esemplarità. Il discorso implicito in questi esempi di sorveglianza si può così esplicitare: "In questo momento potreste essere osservati dalle nostre telecamere, anche se non potete sapere esattamente se lo siete davvero; dunque comportatevi come sapete che noi vorremmo che vi comportaste se vi stessimo effettivamente osservando".

In un'ottica foucaultiana, il cartello che avvisa che in un dato angolo si sta venendo ripresi da telecamere non è affatto un elemento accidentale superaddito al sistema, reso necessario ad esempio da qualche norma giuridica sulla privacy o sul diritto alla notifica, ma è al contrario parte essenziale della tecnologia di sorveglianza stessa. Di nuovo in un senso foucaultiano molto preciso, riprendere qualcuno senza dirglielo o farglielo in qualche modo sapere non costituisce un caso di sorveglianza, poiché non crea effetti di disciplinamento. La tecnologia di sorveglianza infatti non si limita ad una attrezzatura, ad esempio una telecamera a circuito chiuso o un metal detector o uno scanner, ma include l'insieme delle relazioni materiali e immateriali che si vengono a stabilire tra uomini e cose all'interno di un dispositivo sorvegliante. In breve, nell'accezione di Foucault la sorveglianza è sempre un processo partecipativo e collaborativo. Più recentemente, la persistenza di processi cooperativi di sorveglianza è stata sottolineata ad esempio da Gary Marx (2006), secondo il quale sono oggi dilaganti forme "morbide" di sorveglianza che mirano da un lato a presentarla attraverso una (pseudo-)forma di diritto contrattuale (ad esempio: "I passeggeri non sono obbligati a sottoporsi alla perquisizione personale se decidono di non imbarcarsi"), dall'altro a instillare e premiare la volontà collaborazionista attraverso forme di sollecitazione alla sottomissione di tipo informale e gratificante (così, per "collaborare" alla soluzione di un caso di omicidio tutti gli abitanti maschi di una certa età di una cittadina vengono invitati a dimostrare il loro senso di "comunità e responsabilità" fornendo un prelievo del loro DNA attraverso la saliva).

## 3. Trattamenti *ad hoc* e trattamenti aggregati

Occorre però interrogarsi sulla questione: la sorveglianza possiede solo un valore "performativo" (per utilizzare un termine che non era del filosofo francese ma che può rendere l'idea) o possiede anche un valore predittivo, ovvero persino un valore retrodittivo? Porsi questa domanda significa rilevare che un dispositivo di sorveglianza può in effetti sempre subire un processo di eterogenesi dei fini: attraverso la pratica di osservazione sistematica di comportamenti empirici si produce una trasformazione degli stessi standard previsti per l'accettabilità dei comporta-

menti, standard che possono venire poi applicati *ad hoc*, o persino retrospettivamente *ad hominem*. Questo problema ci ricorda che oggi registriamo uno scollamento sempre più sensibile tra la mole dei dati raccolti e delle informazioni prodotte attraverso i processi di sorveglianza da un lato, e il loro possibile utilizzo dall'altro.

Simile scollamento va immaginato concretizzarsi in diversi possibili scenari: vuoi uno scenario di repressione politica di tipo autoritario, vuoi uno scenario di banale, ma potenzialmente illimitato, sfruttamento economico-commerciale. Ad esempio, rispetto al primo scenario, l'estensione degli strumenti di sorveglianza predisposti e resi possibili dalle legislazioni antiterrorismo dell'ultimo decennio ha consentito un utilizzo pervasivo di strumenti di sorveglianza spesso attraverso razionalizzazioni e giustificazioni ex-post. Nel cosiddetto "affaire Tarnac" in Francia – paese che rappresenta, per utilizzare un epiteto a cui siamo ormai familiari, una delle più mature democrazie occidentali – la corte d'appello giudicante ha consentito l'utilizzo nel procedimento penale di dati sull'anarco-situazionista Julien Coupat che erano stati raccolti al di fuori di qualsiasi procedura regolare e persino molto tempo prima dei fatti a lui imputati (il che fa supporre che Coupat fosse già un "cliente" della polizia investigativa quando non si era ancora prodotta alcuna illegalità). Rispetto al secondo scenario, poi, è banale ma per nulla raro che informazioni su clienti e utenti acquisite da ditte e società commerciali vengano spregiudicatamente utilizzate per finalità completamente differenti da quelle per cui sono state raccolte, e in generale per finalità di profitto. Abbiamo qui in sostanza due esempi che mostrano come un regime di visibilità non sia affatto un'istituzione completa che funziona in un'unica direzione definita a priori, ma sia piuttosto un insieme composito, eterogeneo e multidirezionale che si modifica e si direziona attraverso il proprio stesso funzionamento pratico.

Autori come Dandeker (1990), Whitaker (1999) e Lyon (2001) hanno sostenuto che, mentre storicamente dal diciottesimo al ventesimo secolo l'attore principe della sorveglianza è lo stato nazione, oggi assistiamo a un proliferare dei nuclei e delle agenzie di sorveglianza. Rispetto a questa tesi, il grande vantaggio di una epistemologia foucaultiana risiede nel non riservare alcuna posizione privilegiata particolare allo stato in quanto istituzione, bensì di andare ad osservare delle forme di razionalità, ad esempio razionalità disciplinare o governativa, nel momento del loro comporsi in dispositivi. Nei termini di Foucault, non è tanto lo stato che sorveglia, disciplina o governa, quanto piuttosto la razionalità e i dispositivi di sorveglianza, disciplina e governo che infiltrano il funzionamento di istituzioni come quella statale, la quale è lungi dall'essere l'unica coinvolta, dall'esserlo in modo specifico o anche semplicemente diverso dalle altre. Ora, riconoscere l'esistenza di una pluralità di attori e di pratiche socio-tecniche di sorveglianza significa anche riconoscere una pluralità di saperi che agiscono nei sistemi socio-tecnici, i quali non risultano pertanto determinati a priori e insediati stabilmente una volte per tutte, bensì sempre *in the making*. Ad esempio, la ricerca condotta da Klauser (2009) sull' installazione di un sistema di CCTV in un aeroporto internazionale come quello Ginevra mostra sia il coinvolgimento di forme di expertise diverse – che includono polizia, management aeroportuale, informatici e gestori tecnici del sistema – sia il fatto che

lo stesso sistema tecnico possa di conseguenza venire situazionalmente e selettivamente impiegato per usi differenti, quali il controllo dell'accesso alle diverse aree dell'aeroporto, il controllo statistico dei flussi di popolazione, il controllo dei comportamenti individuali, il pedinamento di sospetti e in ultimo anche la registrazione generica e indistinta di "tutto quel che succede".

Si vede inoltre come la dimensione collaborativa possa essere del tutto assente da alcune pratiche che pure, intuitivamente, sembrano presentarsi ai nostri occhi quali pratiche di sorveglianza. In modo persino più cruciale, si intravede come in realtà i trattamenti *ad hoc* e *ad hominem* siano sempre complementari – per non dire che i trattamenti individualizzati sono resi possibili dal trattamento statistico aggregato, che è per eccellenza non-disciplinante. Michel Foucault (2004 [1977-1978]) riconduceva quest'ultimo tipo di trattamento ai "dispositivi di sicurezza", che caratterizzava come "biopolitici", in quanto essi non si riferiscono a un singolo corpo individuale ma ineriscono complessivamente a una "popolazione". Tecniche di sorveglianza come quelle di *data mining* e *pattern recognition*, oggi ampiamente utilizzate, configurano dei regimi di visibilità il cui punto di applicazione non è, in prima istanza, il singolo individuo. Ad esempio, la NSA, l'agenzia per la sicurezza nazionale statunitense – comprensibilmente, una delle organizzazioni più attrezzate e attive nel campo della sorveglianza – analizza di routine una mole, si dice, dell'ordine degli yottabyte ($10^{24}$) di conversazioni telefoniche ed e-mail (Aid 2009). A differenza della sorveglianza disciplinare, i dispositivi di sicurezza hanno natura statistica: essi possono "solo" calcolare dei margini accettabili e delle soglie inaccettabili di rischio; all'opposto di una pratica tangibile e concreta come quella dell' ispezione, la nozione di sicurezza rimane di natura intangibile, fondata unicamente su un calcolo di natura probabilistica riferita a una gamma di eventi possibili.

Al di là del lessico foucaultiano stretto, su si è basato il ragionamento condotto nel paragrafo precedente, sembra dunque difficilmente negabile che alcune delle pratiche di sicurezza contemporanee implichino processi che intuitivamente sentiamo come legati alla sorveglianza. Pensiamo ad esempio al caso di banche e istituti assicurativi che determinano se erogare prestiti o stipulare assicurazioni sulla base della provenienza geografica dei postulanti, o di profili di rischio degli stessi. Nel 2007 fece notizia il caso dell'istituto di credito canadese Laurentian Bank, che rifiutò una richiesta di prestito per acquisto di un autoveicolo pick-up a un residente della Kitigan Zibi First Nation, una comunità autoctona Algonquin. Nonostante il curriculum della persona in questione fosse impeccabile, la *policy* della banca in questione era – e, a quanto consta, è tutt'ora – quella di rifiutare prestiti ai residenti in una serie di codici postali, molti dei quali guarda caso si trovano nelle riserve delle *first nations*. Simili pratiche, spesso odiose e discriminatorie, sono in effetti dispositivi di sicurezza basati su dati aggregati, che producono dei "punteggi di fiducia" (*trust scores*) attraverso i quali i singoli vengono allocati a categorie di rischio precostituite.

Nei manuali degli assicuratori – e a partire dagli anni Ottanta anche nei manuali di criminologia – simili calcoli sono noti come "strategie attuariali", ovvero strategie basate sulla probabilità statistica di realizzazione di dati eventi. Il *triage* sociale securitario che ne risulta è reso possibile dall'acquisizione di dati individuali attra-

verso tecniche di sorveglianza "di basso profilo", ovvero recuperando all'occorrenza informazioni che il singolo individuo da giudicare ha inavvertitamente – ma spesso inevitabilmente – sparpagliato in giro e confrontandoli alle tendenze medie e alle soglie che in relazione a quelle tendenze medie si sono introdotte. Questo tipo di *social sorting*, si è detto, ha effetti socialmente, giuridicamente e politicamente problematici (Lyon 2007). L'introduzione dei profili di rischio crea infatti un effetto domino noto come *path dependency*, in cui il campo delle effettive possibilità successive accordate a un individuo viene progressivamente ristretto sulla base delle categorizzazioni puramente probabilistiche alle quali è stato in precedenza sottoposto. Il risultato è quello che viene chiamato uno svantaggio cumulativo (*cumulative disadvantage*). Ad esempio, in Gran Bretagna la polizia ha elaborato database di potenziali criminali sulla base delle statistiche di criminalità associate all'incidenza di comportamenti anti-sociali a scuola, abbandoni scolastici precoci e segnalazione di casi problematici da parte degli assistenti sociali. Questi profili di candidati criminali vengono poi applicati al resto della popolazione giovane. Sono già assegnati a questa categoria degli aventi profilo di potenziali criminali dei bambini di tre anni, le cui possibilità future non solo di accedere a un prestito bancario ma anche di camminare liberamente per la strada non sono, purtroppo per loro, esaltanti.

In senso stretto, nei dispositivi di sicurezza non si tratta di compiere, come invece nelle pratiche di disciplinamento, una presa in carico del singolo nella sua interezza, al fine di costituirne internamente le tendenze attraverso una "ortopedia morale" delle disposizioni; si tratta invece di controllare dei tassi e delle tendenze complessive che ineriscono a una popolazione. Nei casi riportati sopra, la selezione viene compiuta non cercando di sapere tutto, o il più possibile, su un singolo individuo (come nello scenario totalitario) ma invece riuscendo a posizionare il singolo individuo in un quadro complessivo noto, dunque conoscendo la media di tutti gli altri e determinando le soglie generali che separano l'inclusione dall'esclusione. Certamente, come si è detto sopra, Foucault stesso aveva esplicitamente contemplato il fatto che la sorveglianza discontinua funzionasse rendendo i propri effetti continui. Ora però ci troviamo in uno scenario in cui la raccolta dei dati è *effettivamente continua*. Se dunque sotto l'etichetta della "sorveglianza" i *Surveillance Studies* si occupano in effetti sia di pratiche di sorveglianza sia di pratiche di sicurezza, ciò accade per il buon motivo che per quanto, come ha mostrato Foucault, si tratti di due dispositivi socio-tecnici differenti, la loro interazione in contesti concreti è evidente. La complementarietà fra trattamento *ad hoc* e trattamento aggregato è dunque un aspetto rimarchevole delle tecnologie di sorveglianza attuali.

## 4. Passare per il corpo

Il corpo è il punto di applicazione privilegiato della sorveglianza, non fosse altro per il fatto che esso è eminentemente visibile, "apprensibile" e afferrabile. Tuttavia il corpo stesso può venire concettualizzato in modi diversi all'interno di diverse pratiche di sorveglianza. Si può pensare ad esempio a un corpo che agisce e che

pertanto può venire influenzato nelle sue disposizioni, giungendo a conformarsi a una norma (ovvero fallendo e diventando "anormale"); ma si può anche pensare a un corpo che *testimonia*, lasciando intorno impronte e tracce di sé che permettono di ritrovare e ricostruire la sua rotta attraverso uno spazio; ovvero ancora si può pensare a un corpo da sezionare analiticamente attraverso un insieme di variabili fisiche (come peso, altezza, temperatura, ecc.).

Mentre la sorveglianza disciplinare descritta da Foucault si propone di agire su delle condotte, di agire su un agente e sulla sua azione modificandola "geneticamente", si è già sopra constatata l'esistenza di altri regimi di visibilità nei quali il corpo viene reso pertinente in modo per così dire anatomico, cioè solo in quanto evidenza testimoniaria. In altri termini, il corpo si presenta come un territorio visibile a uno sguardo inquirente. Da questo punto di vista, i sistemi biometrici vengono utilizzati in primo luogo per operare un riconoscimento individuale biunivoco, verificando che la persona sia chi dichiara di essere e distinguendola da altri possibili "concorrenti" a quella stessa identità (*authentication*), ovvero per identificare la persona in questione anche se essa non avanza alcuna dichiarazione di identità (*recognition*). In relazione alla discussione del paragrafo precedente, si comprende come simili operazioni richiedano necessariamente un trattamento aggregato e omogeneo dei dati riguardanti un'intera popolazione. La storia classica della biometria inizia infatti con la medicina legale e la criminologia positivista italiana di metà Ottocento, entrambe ossessionate dalla fisiognomica dell'*homo criminalis*; ma dall'antropometria del singolo deviante si arriva in breve alla schedatura sistematica di gruppi sociali attraverso impronte digitali e fotografie segnaletiche (Gilardi 2003). Nelle pratiche sanitarie di base, poi, è l'intera popolazione (inizialmente l'intera popolazione urbana, per giungere infine, come si dice anche nel caso dei telefoni mobili, alla "copertura del territorio") a venire misurata e registrata. Il caso delle schedature "razziali" nei regimi totalitari fascisti e in quelli di apartheid (ad esempio, rispettivamente, Aly e Roth 2004; Bowker e Star 1999) può servire a ricordare alcuni punti di approdo di questo vasto movimento.

Non solo la fotografia sul passaporto, ma anche la firma, si può dire, è uno strumento biometrico, in senso forse attenuato ma pur sempre territoriale del termine. Se comunque la firma deriva da una estroflessione di uno schema motorio acquisito che può venire replicata entro un margine di variazione tollerato, il corpo nella sua materialità immediata fornisce una firma ancor più netta, in quanto la conformazione morfologica di ciascun corpo è differente dalle altre in un numero amplissimo di dettagli del viso e delle membra. I sistemi biometrici si applicano direttamente al corpo non per agire sulla sua azione bensì per cercare – forse peraltro, va detto, in modo illusorio – di distinguere univocamente ciascun corpo da un altro e ricongiungere biunivocamente ogni corpo all'opportuno record di un database. I sostenitori di questi sistemi affermano che, a differenza dei sistemi di autenticazione attraverso password o documenti cartacei, gli strumenti biometrici attuali sono più robusti nei confronti dei tentativi di effrazione e falsificazione, mentre i detrattori dicono che questi sistemi sono ancora molto inaffidabili o, al contrario, troppo pericolosi (ad esempio, sui passaporti biometrici, Bennett e Lyon, a cura di, 2008). Al di là delle valutazioni che se ne vogliano dare, quel che più interessa rile-

vare è che tutti i sistemi biometrici implicano una codifica e, in questo senso, un'astrazione dei dati corporei rilevati. Tali dati infatti vengono trascritti in una matrice matematica più o meno sofisticata, alla quale è possibile poi applicare algoritmi che rilevano correlazioni statistiche tra elementi, configurazioni formali di pattern e così via. Ciascun passaggio di queste "trascrizioni" dal corpo ai dati e viceversa implica, come è comprensibile, un insieme estremamente complesso di fattori: si tratta di veri e propri esercizi di traduzione che i sofisticati sistemi biometrici attuali svolgono in una varietà di modi, spesso attraverso sistemi autocorrettivi in grado di affinarsi progressivamente (vedi ad esempio Jain, Bolle e Pankanti, a cura di, 1999; Gray 2003; Tistarelli e Nixon, a cura di, 2009).

Anche in questo caso ci troviamo dunque di fronte a una configurazione sociotecnica ampliata ed eterogenea, in cui ciò che conta sono precisamente le articolazioni e i passaggi tra gli stadi intermedi, tra materie eterogenee e tra processi di "messa in forma" differenti. Importante rimane, in ogni caso, ricordare l'esistenza di questo momento del "passaggio per il corpo" utilizzato in alcuni dispositivi di sorveglianza. Il corpo viene sottoposto a misurazioni, scansioni, prelievi condotti con diverse modalità, che sono naturalmente e legittimamente aperte a contestazioni e preoccupazioni. Al centro del dibattito attuale sulla sorveglianza biometrica è infatti sia l'estensione di tali pratiche di controllo per un insieme di nuove funzioni, sia l'estensione delle dimensioni corporee prese in carico: la retina, iride, il viso (modellizzato tridimensionalmente), la modulazione vocale, le impronte palmari, l'andatura, l'odore corporeo, il DNA rilevato attraverso saliva o capelli, dimensioni spesso poi combinate in sistemi multi-biometrici.

## 5. Tracciamenti

A causa della pluralità sociale dei luoghi di sorveglianza già richiamata in apertura, le odierne pratiche di sorveglianza e di controllo risultano spesso separate tra loro, condotte per obiettivi diversi e utilizzando dispositivi e saperi eterogenei. Per questo motivo Lyon (2007) ha insistito sulla natura "post-panottica" della sorveglianza contemporanea: essa sarebbe composta non tanto da un unico apparato centrale di sorveglianza, come negli scenari totalitari "big-brotheristici", quanto da un patchwork di sistemi locali, ciascuno dei quali dotato di proprie finalità e modalità di funzionamento. Anche se la terminologia di Lyon non rende molta giustizia al pensiero di Foucault – il quale in realtà fu il primo ad analizzare la crisi delle società disciplinari, e il cui concetto di panottico è in ultima analisi meglio inteso come un dispositivo analitico di potere piuttosto che come un modello sociale complessivo che caratterizzerebbe un'epoca storica determinata – la questione perdura sostanziale. Al momento presente, non è scontato se l'interconnessione tra diversi dispositivi di sorveglianza sia destinata a risultare in un *patchwork*, o se invece possa produrre un "continuo" coerente di sorveglianza, come hanno paventato altri osservatori; o, ancora, se essa non prefiguri persino un quadro di sovrapposizioni, interferenze e incastri dagli effetti contradditori, imprevedibili e forsanche grotteschi. Graham (2002) propende ad esempio per una tesi continuista, secondo

cui la spinta verso l'ubiquità dei sistemi di sorveglianza implica una loro normalizzazione e regolarizzazione come parte integrante dello spazio urbano. In questa interpretazione, la sorveglianza diviene un'infrastruttura invisibile e onnipresente, che "sostiene" (nel senso in cui i pilastri sostengono gli edifici) tutta una serie di ulteriori processi socio-tecnici nello spazio urbano. Lianos (2001) propende al contrario per una tesi radicalmente decentralista: il controllo istituzionale contemporaneo per questo autore è acentrico e acefalo, "periottico" più che panottico. Sorvegliare gli individui, al limite, non serve più: è sufficiente creare delle posizioni individuali differenziali di inclusione/esclusione dal sistema e promuovere la competizione individuale per l'inclusione nel sistema; non c'è bisogno di sorvegliare né gli inclusi né gli esclusi, ma solo di regolare le vie di accesso (Bigo 2006 vi aggiunge un'analisi della violenza di messa al bando degli esclusi).

La tesi di Lianos, che punterebbe verso una irrilevanza della sorveglianza, incontra senza dubbio diverse difficoltà empiriche. Tuttavia essa consente anche di illustrare un aspetto importante della questione: in molti casi, non abbiamo infatti a che fare con una sorveglianza sistematica di lungo corso, come ad esempio sono le attività investigative sotto copertura o la sorveglianza dei nemici politici. Poiché i dati che riguardano una persona sono costantemente registrati in automatico da una serie di organizzazioni con cui quella persona entra in contatto pressoché ogni giorno (transazioni economiche, lettura della email, navigazione in rete e passeggiata per la strada) e sono conservati in archivi pressoché *sine die*, si rende in seguito possibile un atto di sorveglianza puntuale, compiuta solo all'occorrenza secondo procedure tecniche di visibilizzazione specificamente scelte. Se da un lato questo soggetto sorvegliante, post-orwelliano sì, ma purtuttavia in grado di muoversi attraverso archivi disparati (e non necessariamente connessi tra loro, o quantomeno non progettati per esserlo) non è stato ancora sufficientemente studiato (il che non si preannuncia certo come un compito facile!) vale comunque la pena cercare di chiarirsi la modalità specifica con la quale si svolge questo tipo di sorveglianza. Si tratta infatti di una pratica di *tracking*, di tracciamento che assume un ruolo centrale in molte pratiche.

Nel gergo idraulico, un tracciatore è un liquido che viene iniettato lungo tubi o canali al fine al fine di comprenderne le geometrie e le giunture non visibili (un modo delicato di trattare con le scatole nere). Tracciare significa essenzialmente poter seguire, o risalire a ritroso, un percorso che si svolge o si è svolto all'interno di un campo e/o lungo un network predefinito. In grande misura, occorre riconoscere che tanto lo spazio urbano contemporaneo quanto lo spazio informatico sono precisamente configurati come campi e reti di questo tipo, su cui i percorsi individuali risultano tracciabili. Per Picon (2008), ad esempio, lo spazio urbano per intero viene oggi ridotto a serie di occorrenze, eventi e situazioni, modellandosi morfologicamente sullo spazio informatico. In questa versione, la nozione di evento viene privata di ogni imprevedibilità, di qualsiasi fattore di apertura o instabilità (com'era ad esempio l'evento teorizzato da Deleuze, Foucault e Derrida – l'apparizione del padre di Amleto), per denotare un mero accadimento all'interno delle possibilità della matrice, un sintagma ridotto ad epifenomeno del paradigma. In congiunzione con il fatto che tutte le occorrenze possono essere registrate – per

non dire che lo sono già – lo sviluppo delle tecniche di *data mining* e degli *spyware* che operano analisi di tipo reticolare fa intravedere ad alcuni un superamento quantitativo imponente delle limitazioni inerenti a forme precedenti di sorveglianza (Marx 2002). Tra gli *spyware*, hanno goduto di una certa fama applicazioni dai nomi ameni, quali Echelon, Carnivore, Total Information Awareness, nomi che appunto evocano superlative capacità di "macinare dati" al fine di ridurre ogni evento ad un'occorrenza codificata e collocabile.

È certo che gli oggetti abbiano una vita sociale; quelli che contengono dispositivi di sorveglianza ne hanno però probabilmente una più vivace. Gli spazi e gli oggetti della vita quotidiana vengono a tal punto infusi di software e di processi computazionali informatici che qualcuno, in una sorta di implicito requiem per Lefèbvre, ha parlato di una "produzione automatica dello spazio" (Thrift e French 2002). Simili oggetti sempre più *smart* mettono in atto una sollecitazione dei propri utilizzatori, i quali vengono informati, istruiti, consigliati e interpellati da tali artefatti molto più spesso – per non dire ininterrottamente – che dai meno complessi artefatti loro predecessori: un telefono intelligente richiede più, non meno attenzioni di uno stupido. Al contrario di quanto auspicato da Weiser (1991) e da altri tecnoutopisti del Massachusetts Institute of Technology, diventando ubiqua la tecnologia non è diventata più "tranquilla", bensì più vociferante. Non solo gli oggetti vengono infusi di software, ma in un certo senso lo stesso accade anche agli esseri umani. Ognuno di noi dispone di decine di login e profili personali su siti di acquisto online, abbonamenti, riviste, forum di discussione, piattaforme di *social networking*, videogiochi e così via. A molti di questi profili non dedichiamo alcuna attenzione ma ad alcuni teniamo particolarmente (il nostro profilo Facebook, il nostro profilo sul sito dell'organizzazione per cui lavoriamo, il nostro profilo nel forum di appassionati di agricoltura biologica o di pesca sportiva). Sebbene nessuno di questi spazi sia progettato esplicitamente per essere uno spazio di sorveglianza, è il funzionamento stesso di questi dispositivi informatici a svolgersi "già da sempre" in un formato sorvegliante.

La chiave per interpretare questi fenomeni non è forse neppure tanto la computazione – la quale è lungi dall'essere irrilevante, ma è già stata ampiamente esplorata – quanto la *trasversalità*. La trasversalità è una caratteristica di ogni topologia di rete, dato che la robustezza di una rete dipende proprio dalla possibilità di trasversalizzare i percorsi e, *a fortiori*, rende l'attività di tracciamento, come si è detto sopra, centrale. Il funzionamento in rete delle pratiche di sorveglianza sposta pertanto una serie di confini rispetto al ragionamento sui limiti attuali della sorveglianza.

## 6. La frontiera: il sociale

Per qualche perversa ragione nella seconda metà del ventesimo secolo i sociologi si erano specializzati nel dimostrare che qualsiasi loro oggetto di studio era "una costruzione sociale". Con un gioco di parole a proposito di quella *vague* fortunatamente ormai tramontata, si potrebbe dire che non tanto la sorveglianza è un'attività socialmente costruita, quanto la sorveglianza *è la società stessa*.

Se per Foucault il guardiano del *panopticon* non doveva necessariamente avere delle qualifiche particolari ma poteva essere al limite una persona qualunque che venisse a trovarsi nella posizione di osservazione all'interno del dispositivo di sorveglianza, oggi si trova che poliziotti, datori di lavoro, revisori di progetto, gestori di servizi di sicurezza, agenti pubblicitari, truffatori, genitori, amici affezionati e amanti gelosi controllano di routine – certo per motivi e con effetti di volta in volta diversi – informazioni su interessi e attività che sono liberamente inviate a proposito di sé dai membri iscritti a piattaforme online di *social networking*. Molti non sospetteranno mai di non essere stati chiamati a un colloquio di lavoro o invitati a una serata a causa di alcune di quelle informazioni. Si è parlato sopra di "atti di sorveglianza puntuale"; può essere utile rilevare che anche una banale ricerca su Google costituisce uno di tali atti.

Le piattaforme online di *social networking* sono state definite un "*panopticon* partecipativo" (Whitaker 1999), anche se, in base a quanto si è detto nel primo paragrafo, l'espressione è ridondante. Ad ogni modo, secondo Abe (2009), mentre l'immagine tradizionale della sorveglianza era sinistra e repressiva, la sorveglianza decentralizzata in rete appare come simpatica e divertente; questo sarebbe l'unico modo per riuscire a spiegare perché la gente desideri essere presente su queste piattaforme pur essendo perfettamente consapevole degli effetti che ne conseguono. Ciò segnalerebbe il passaggio da una logica di sorveglianza repressiva e persecutoria a una partecipativa e seduttrice. Ad esempio, una ricerca sugli studenti di una università australiana (Dawson 2006) ha mostrato che esiste un notevole grado di consapevolezza tra gli studenti riguardo al livello di sorveglianza online nel campus, ma che, anche se ciò può indurre ad alcune auto-limitazioni, non riduce però nel complesso il livello di partecipazione. Si potrebbe sostenere che le persone non vogliono chiamarsi fuori dal regime di visibilità sorvegliante perché non vogliono rinunciare ai vantaggi che lo stare in quel regime comporta (Lianos 2001). In un certo senso, proprio a causa dei vantaggi che offre, il sistema può quasi contare sul fatto che, posta di fronte all'alternativa secca e irrevocabile tra inclusione o esclusione, la grandissima maggioranza preferirà sempre l'inclusione, anche quando ciò implichi l'acconsentimento a pratiche di sorveglianza e l'effettivo assoggettamento ad esse.

Tuttavia, occorre sottolineare l'importanza del fattore del piacere nella partecipazione a questi dispositivi. Il nesso tra utilità, piacere e desiderabilità del panottico partecipativo deve essere ancora esplorato in modo esauriente. I commentatori ottimisti hanno sostenuto che la sorveglianza partecipativa presenta numerosi aspetti positivi, sia generando un senso di *empowerment* tra gli utenti attraverso la costruzione di soggettività online e la possibilità di adire a nuove forme di socialità (Albrechtslund 2008), sia rendendo possibili attività di *civic watch* e sorveglianza dal basso da esercitare sugli attori politici ed economici più potenti, forme cioè che si contrappongono e controbilanciano quelle tradizionali della sorveglianza dall'alto (Häyhtiö e Rinne 2009). Secondo Humphreys (2010) anche i *mobile social networks* – ovvero le piattaforme di reti sociali applicate a dispositivi mobili come gli smartphones e che includono varie forme di geolocalizzazione – sono in grado di rafforzare i legami sociali. Al contrario, i commentatori più critici, scettici, al-

larmati o moralisti hanno notato come la nostra capacità di venire a sapere così tante cose a proposito degli altri in ogni momento in cui lo desideriamo apra in realtà la via a un "complesso voyeuristico-esibizionista" (Koskela 2004; Andrejevic 2007). Tale circuito di voyeurismo-esibizionismo su vasta scala si tradurrebbe in una ricerca esasperata e ansiogena di *meetingness* inevitabilmente connessa a un controllo sociale capillare.

Laddove un autore come Negri (2000) ha tessuto a più riprese il panegirico della "produzione comune" della moltitudine che avviene attraverso la cooperazione in rete (non solo attraverso le reti informatiche, a cui però Negri più volte si richiama) e il cui plusvalore viene poi espropriato dal capitale parassitario, lo scenario della vacuità, dell'autoreferenzialità, dell'emotivismo e dell'infantilismo di molta di questa produzione comune cooperativa presente online potrebbe indurre a una valutazione maggiormente circospetta. Il paradosso è che persino persone che sono inquietate – se non addirittura rese paranoiche – dall'idea di essere esposte alla sorveglianza mettono contemporaneamente in atto dei comportamenti che sono, da un punto di vista oggettivo, di tipo esibizionistico. Per non parlare del fatto che le pratiche di *sousveillance* possono facilmente tramutarsi in forme di vigilantismo che danno luogo a episodi di giustizia sommaria, se non di vera e propria persecuzione, caccia alle streghe e linciaggio popolare. Nel famoso caso noto come *dog shit girl* avvenuto nel 2005 in Corea del sud, una ragazza che non aveva raccolto gli escrementi del proprio cane fu filmata con un cellulare da un passante; non appena il video fu messo in rete alcuni auto-appuntati vigilantes di internet fecero partire una durissima campagna di identificazione, diffamazione e umiliazione della colpevole al termine della quale la ragazza non solo implorò pietà, ma abbandonò l'università e secondo alcune fonti contemplò il suicidio.

La ricerca della visibilità come riconoscimento da parte degli altri sembra insomma inestricabilmente avvinta all'ottenimento della visibilità come controllo sorvegliante. Alla lista delle caratteristiche dei regimi di visibilità sopra enucleate, vanno aggiunte la dimensione delle affettività di massa, quali il piacere e l'odio, e le modalità di diffusione e contagio di tali affettività.

## 7. Conclusioni

La considerazione basilare da cui queste brevi e incomplete annotazioni hanno preso le mosse è che la sorveglianza si costituisce come un insieme di relazioni socio-tecniche che danno forma a relazioni di visibilità e intervisibilità. In breve, siamo *presi in regimi di visibilità*.

Le tecnologie della sorveglianza non sono però un'invenzione della nostra epoca e, in tal senso, molta letteratura nell'ambito dei *surveillance studies* e dei *new media studies* andrebbe "de-eccezionalizzata". Come ci hanno insegnato i paleoantropologi da Leroi-Gourhan in poi, il processo di ominazione è un processo intrinsecamente tecnologico. Dispositivi di sorveglianza molto antichi sono ad esempio i campanacci attaccati al collo degli animali e gingilli attaccati al polso dei bambini. Forse oggi ci troviamo in un momento storico in cui un insieme di nuovi allinea-

menti tecnologici e di nuove modalità di estroflessione antropologica stanno ridefinendo il soggetto sociale. Certamente, abbiamo un problema con la gestione delle distanze sociali – che, ci ha mostrato Canetti (1960), nascono prima di tutto come distanze fisiche – in un contesto in cui le tecniche di mediazione e i mediatori tra queste distanze sono cambiati rispetto al passato.

Alla luce di quanto si è detto sin qui, ci si potrebbe iniziare a chiedere se l'antica contrapposizione tra, da un lato, gli *arcana imperii* – un dominio che si esercita osservando senza essere osservati – e, dall'altro, lo spettacolo del potere – un dominio che si esercita esibendo senza osservare – regga ancora. Infatti oggi non sono probabilmente più separabili due dispositivi di visibilità intorno a cui si sono a lungo articolate le pratiche di sorveglianza: da un lato il controllo della formazione delle disposizioni individuali, dall'altro la determinazione degli estremi gestibili di situazioni di massa. È dunque necessario iniziare a studiare la sorveglianza nel contesto più ampio della sincronizzazione (come altresì delle dissincronie) delle affettività sociali nel campo della distribuzione delle visibilità e delle intervisibilità.

## Bibliografia


Aid, M.M. (2009) *The Secret Sentry: The Untold History of the National Security Agency*, London, Bloomsbury.

Albrechtslund, A. (2008) "Online Social Networking as Participatory Surveillance", in "First Monday" 13. Online: http://firstmonday.org/article/view/2142/1949.

Aly, G. e Roth, K.H. (2004) *The Nazi Census: Identification and Control in the Third Reich*, Philadelphia, Temple University Press.

Amoore, L. e Hall, A. (2009) *Taking people apart: digitised dissection and the body at the border*, in "Environment and Planning D" 27(3), pp. 444-464.

Andrejevic, M. (2007) *iSpy: Surveillance and power in the interactive era*, Lawrence, University Press of Kansas.

Bennett, C.J. e Lyon, D. (a cura di) (2008) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, New York, Routledge.

Bigo, D. (2006) *Security, Exception, Ban and Surveillance*, in D. Lyon (a cura di) *Theorizing surveillance: the panopticon and beyond*, Cullompton, Willan Publishing.

Bowker, G.C. e Star, S.L. (1999) *Sorting things out. Classification and its consequences*, Cambridge, MIT press.

Brighenti, A.M. (2010) *Visibility in Social Theory and Social Research*, Basingstoke, Palgrave Macmillan.

Canetti, E. (1960) *Masse und Macht*, Hamburg, Claasen; trad it. *Massa e potere*, Milano, Adelphi, 2002.

Dandeker, C. (1990) *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, New York, St. Martin's Press.

Dawson, S. (2006) *The impact of institutional surveillance technologies on student behaviour*, in "Surveillance & Society", 4(1/2), pp 69-84.
Ellul, J. (1965) *The technological Society*, London, Cape.
Foucault, M. (1975) *Surveiller et punir: naissance de la prison*, Paris, Gallimard.
Foucault, M. (2004[1977-1978]) *Sécurité, territoire, population*, Paris, Gallimard - EHESS.
Gilardi, A. (2003) *Wanted! Storia, tecnica ed estetica della fotografia criminale, segnaletica e giudiziaria*, Milano, Bruno Mondadori.
Graham, S. (2002) *CCTV: The Stealthy Emergence of a Fifth Utility?*, in "Planning Theory and Practice", 3(2), pp. 237-241.
Gray, M. (2003) *Urban Surveillance and Panopticism: will we recognize the facial recognition society?*, in "Surveillance & Society", 1(3), pp. 314-330.
Haggerty, K.D. e Ericson, R. (2000) *The surveillant assemblage*, in "British Journal of Sociology", 51(4), pp. 605-622.
Haggerty, K.D. e Samatas N. (a cura di) (2010) *Surveillance and democracy*, New York, Routledge.
Häyhtiö, T. e Rinne J. (2009) *Little Brothers And Sisters are watching. Reflexive civic watch through computer-mediated communication*, in "Information, Communication & Society", pp. 1–20.
Humphreys, L. (2010) *Mobile social networks and urban public space*, in "New Media & Society", 12(5), pp. 763-778.
Jain, A.K., Bolle R. e Pankanti, S. (a cura di) (1999) *Biometrics. Personal identification in networked society*, New York, Springer.
Klauser, F. (2009) *Interacting forms of expertise in security governance: the example of CCTV surveillance at Geneva International Airport*, in "British Journal of Sociology", 60(2), pp. 279-297.
Koskela, H. (2004) *Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism*, in "Surveillance and Society", 2(2), pp. 199-215.
Lianos, M. (2001) *Le nouveau contrôle social*, Paris, L'Harmattan.
Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*, London, Open University Press, trad. it. *La società sorvegliata*, Milano, Feltrinelli, 2002.
Lyon, D. (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London, Routledge; trad. it. *Massima sicurezza: sorveglianza e "guerra al terrorismo"*, Milano, Cortina, 2005.
Lyon, D. (a cura di) (2006) *Theorizing surveillance: the panopticon and beyond*, Cullompton, Willan Publishing.
Lyon, D. (2007) *Surveillance studies: An overview*, Cambridge, Polity Press.
Marx, G.T. (2002) *What's new about the 'new surveillance'? Classifying for change and continuity*, in "Surveillance & Society", 1(1), pp. 9-29.
Marx, G.T. (2005) *Some Conceptual Issues in the Study of Borders and Surveillance*, in E. Zurei, e M.B. Salter (a cura di) *Global Surveillance and Policing: Borders, Security, Identity*, Cullompton, Willan Publishing.
Marx, G.T. (2006) *Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – 'Hey Buddy Can You Spare a DNA?'*, in T.

Monahan (a cura di) *Surveillance and Security: Technological Politics and Power in Everyday Life*, New York, Routledge.
Mathiesen, T. (1997) *The Viewer Society. Michel Foucault's Panopticon Revisited*, in "Theoretical Criminology", 1(2), pp. 215-234.
Monahan, T. (a cura di) (2006) *Surveillance and Security: Technological Politics and Power in Everyday Life*, New York, Routledge.
Negri, A. (2000) *Kairòs, Alma Venus, Multitudo*, Roma, Manifestolibri.
Picon, A. (2008) *Toward a city of events. Digital media and urbanity*, in "New Geographies", 0, pp. 32-43.
Poster, M. (1990) *The Mode of Information: Poststructuralism and Social Contexts*, Chicago, University of Chicago Press.
Scott, J.C. (1998) *Seeing like a state*, Yale, Yale University Press.
Simmel, G. (1908) *Sociologia*, trad. it. Torino, Edizioni di Comunità, 1998.
Tistarelli, M. e Nixon, M.S. (a cura di) (2009) *Advances in Biometrics: Third International Conferences*, ICB 2009, Alghero, Italy, June 2-5, 2009. Berlin, Heidelberg, New York, Springer.
Thrift, N. e French, S. (2002) *The automatic production of space*, in "Transactions of the Institute of British Geographers", 27(3), pp. 309-335.
Weiser, M.D. (1991) *The Computer for the 21st Century*, in "Scientific American", 265(3), pp. 66-75.
Whitaker, R. (1999) *The end of privacy: how total surveillance is becoming a reality*, New York, New Press.
Zurei E. e Salter M.B (a cura di) (2005) *Global Surveillance and Policing: Borders, Security, Identity*, Cullompton, Willan Publishing.

**Technologies of Visibility. Notes on Current Surveillance Practices**

**Abstract.** Surveillance is defined by a set of socio-technical patterns that shape visibility and inter-visibility relations. The text outlines connections deemed to be central to develop a better understanding of the development and implementation of a range of technologies that re-shape visibility relations among social subjects, sites and events. The crucial question focuses on how the individual body and the body of populations come to form two poles or two action fields of control, and how factors such as docility, participation and sociability are mobilized in new surveillance formations.

**Keywords:** surveillance; visibility; anatomopolitics; biopolitics; information management

* * *

**Andrea Mubi Brighenti,** Università di Trento
Dipartimento di Sociologia
Via Verdi, 26 – 38122 Trento
Email: andrea.mubi@gmail.com