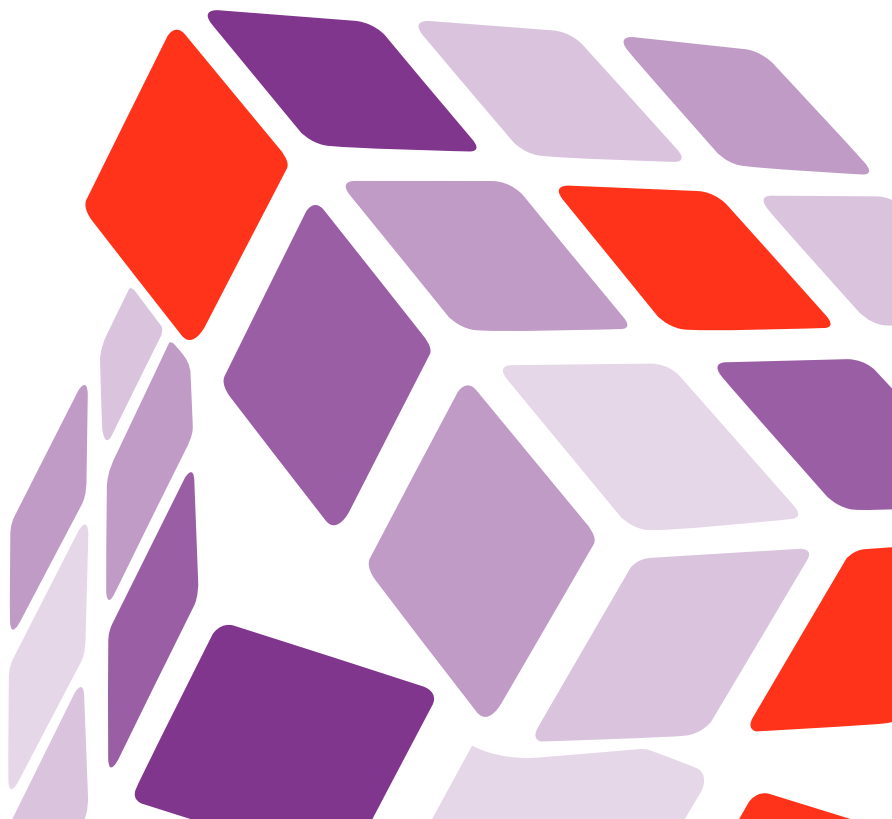


KULTUR UND MEDIEN

SMART CITY

**ÜBERWACHUNG UND KONTROLLE
IN DER «INTELLIGENTEN STADT»**

JATHAN SADOWSKI UND FRANK PASQUALE



INHALT

Einleitung	2
Was ist eine «Smart City»?	4
Die Ideologie der «Smart City»	8
«Smart Citys» in Kontrollgesellschaften	15
Die sanfte Gewalt biometrischer Überwachung	20
Die brutale Gewalt von Polizeitechniken	24
Cyborg-Urbanisierung und verschwommene Grenzen	29
Die Zurückeroberung der Kontrolle	32
Literatur	36

EINLEITUNG

Die Vorstellung von Städten als Orten, in denen wir uns zugleich daheim und fremd fühlen können, hat einen gewissen Reiz. Man kennt die Straßen und Geschäfte, die Alleen und Gassen, kann aber dennoch ganze Tage dort verbringen, ohne erkannt zu werden. Städte werden jedoch zunehmend von den Eliten mit «intelligenten» oder «smarten» Technologien versehen und damit zu Plattformen für das «Internet der Dinge» gemacht: für in physische Objekte eingebettete Sensoren und Rechner, die sich über das Internet miteinander verbinden, kommunizieren und Informationen übertragen. Es gibt kaum mehr Möglichkeiten, sich diesem umfassenden Netz der Überwachung und der damit einhergehenden Machtverhältnisse zu entziehen (vgl. Hollands 2008; Townsend 2014; Neirotti u. a. 2014). In nicht allzu ferner Zukunft werden Geschäfte oder Galerien mehr über ihre KundInnen und BesucherInnen wissen als diese über die Läden, in die sie gehen (Arnsdorf 2010). Software zur Gesichtserkennung und Smartphone-Signale geben Hinweise auf unsere Identität, unsere Konsumgewohnheiten und Reputation: Sind wir Ladendiebe oder sitzt bei uns das Geld eher locker, sind wir «Dauerschuldner» oder «Goldbarone»? Um nur zwei Bezeichnungen zu nennen, die unter MarketingexpertInnen durchaus verbreitet sind (Castle Press 2010).

«Big Data» ist die neue Währung der Handelswelt, doch es verhält sich damit wie mit dem Geld: Manche haben hierzu einen viel besseren Zugang als andere. Wer als Privatperson bei einer Bank einen Kredit beantragt, muss in der Regel umfangreiche persönliche Angaben

machen und entsprechende Unterlagen beibringen, während die Bank dagegen keiner vergleichbaren Pflicht unterliegt. Niemand verlangt von Finanzinstituten, Details ihrer internen Entscheidungsprozesse offenzulegen (Pasquale 2015). Eine ähnliche Dynamik entfaltet sich auch im Internet der Dinge: Mächtige Akteure ziehen zentripetal eine immer größere Menge von Nutzerdaten an sich, verweigern den NutzerInnen sowie den Aufsichtsbehörden aber den Zugang zu diesen Informationen, selbst in höchst problematischen Fällen der Datenverwendung oder des -missbrauchs. Es ist heute nicht mehr sinnvoll, sich «das Internet» als etwas vorzustellen, worauf man über einen Computer zugreift, denn wir befinden uns längst in einer Situation, in der die Stadt selbst als Plattform und Knotenpunkt vernetzter Informations- und Kommunikationstechnologien gedacht und in diese Richtung umgestaltet wird.

In der Zeitschrift *Wired* wurde in einem Leitartikel über das Internet der Dinge folgende Frage gestellt: «Haben Sie jemals in Ihrer Wohnung einen Gegenstand verloren und sich gewünscht, Sie könnten einfach einen Suchbegriff eingeben, um ihn wiederzufinden, wie Sie es auch bei einem auf Ihrer Festplatte verschwundenen Dokument tun würden?» (Wasik 2013) Das ist, so wird uns weisgemacht, bereits möglich, dank einer Startup-Firma namens StickNFind Technologies, die günstige kleine «Sticker-Sensoren» vertreibt. Was, wenn Ihr Kind im Einkaufszentrum verloren geht? Smart-Fashion-RFID-Etiketten sorgen dafür, dass es von einem Netzwerk erfasst ist und seine Spuren jederzeit zu verfolgen sind. Und warum sollte man mit Signaltechnik

ausgestattete Bekleidung nur für Kinder verwenden? Bald werden Ihr Auto, Ihr Haus, Ihre Haushaltsgeräte und jeder andere Teil Ihres Umfelds dauerhaft miteinander vernetzt sein und ständig miteinander kommunizieren. Bezogen auf die Stadt bedeutet dies, dass diese zu einem Kokon der Konnektivität wird, der uns verschlingt, oder zu einem Netz, in dem wir gefangen sind, je mehr «intelligente» Technologien in unseren Alltag integriert werden. Diese Technologien werden uns als Mittel angepriesen, mit denen wir etwas (auf-)finden können oder mit denen wir mobiler werden. Es handelt sich um Suchtechnologien (wenn wir uns ihrer bedienen) und um «Reputationstechnologien» (wenn sie verwendet werden, um uns zu bewerten) (Pasquale 2015). Mit ihnen wird kartografiert, kategorisiert und klassifiziert – und was könnte harmloser daherkommen als reine Informationen? Die Kosten und Nutzen dieser Innovation zu kalkulieren ist überaus mühsam und hat viel mit ideologischen Überzeugungen zu tun. Wir wissen nicht, welche üblen und abstrusen Formen der Anwendung sich noch ergeben werden. Daher könnten Analysen und Projektionen, die sich mit Zukunftsszenarien befassen, eine wertvolle Alternative zu Kosten-Nutzen-Studien sein (Verchick 2010), insofern sie anerkennen, dass es ein Spannungsverhältnis gibt zwischen dem Zuwachs an Möglichkeiten und Annehmlichkeiten, die uns das Internet der Dinge bietet, und dem damit einhergehenden Verlust an Privatsphäre. Unternehmen oder Regierungen tendieren dazu, mögliche negative Auswirkungen des Internets der Dinge herunterzuspielen und Studien dazu als paranoide Projektionen abzutun. Oftmals werden sozialwissenschaftliche oder politische Analy-

sen zur umfassenden Überwachung und Kontrolle städtischer Räume vonseiten der Technokraten in verzerter Form wiedergegeben. Außerdem sind ihre Evaluierungsinstrumente, mit denen sie gern eine «Zustimmung» der BürgerInnen zur Überwachung nachweisen, derart manipulierbar, dass damit selbst die fragwürdigsten Kontrolltechnologien – etwa die drohnengestützte Überwachung von Menschenmengen bei Großdemonstrationen oder beim Autoverleih einsetzbare Technologien, mit denen ein Pkw bei verspäteter Zahlung binnen Minuten stillgelegt werden kann – als Ausdruck des demokratischen Willens und der Rationalität des Marktes befürwortet werden können.

Da es sich die Technokraten in der Regel bequem machen und sich einfach blind stellen gegenüber den besorgniserregendsten Aspekten der «Smart City», bedarf es eines ausgewogeneren theoretischen Ansatzes, um darauf zu reagieren. Dieser sollte unseres Erachtens die Eigenschaften und Folgen der vorherrschenden sozialpolitischen Logik offenlegen, die viele der zahlreichen mit der «Smart City» im Zusammenhang stehenden Praktiken und Ideologien durchzieht und miteinander verbindet. Wir beginnen mit einem Überblick zu den Hintergründen und Protagonisten der «Smart City», der sich auf eine Reihe aktueller analytischer Arbeiten zum Thema stützen kann. Es folgt eine kritische Einführung in die Ideologie der «Smart City», wobei wir uns auf die Erklärungen und Bestrebungen einiger ihrer bedeutendsten wirtschaftlichen, politischen und akademischen BefürworterInnen konzentrieren. Dem stellen wir unsere Deleuze'sche Alternative gegenüber, indem wir eine Gesellschaftstheorie der «Smart City» skizzie-

ren, in der sie als eine Form der Kontrolle (und nicht etwa als Emanzipation) ihrer BewohnerInnen interpretiert wird. Als Beispiele des sich hieraus ergebenden «Spektrums der Kontrolle» gehen wir näher auf die biometrische Überwachung als Form des Monitorings und auf die automatisierte Polizeiarbeit als besonders brutale und zielgenaue Form der Manipulation ein. Im vorletzten Abschnitt werden die Herausforderungen thema-

tisiert, die mit dieser weitreichenden Integration von Mensch, Maschine und Stadt in unserer «postdigitalen Ära» (Jurgenson 2012) einhergehen. Der Aufsatz endet mit normativen Überlegungen, wie mit diesen allgegenwärtigen Überwachungs- und Kontrollmechanismen, die dabei sind, eine entscheidende Infrastruktur für die «Smart City» zu konstituieren, umgegangen werden soll.

WAS IST EINE «SMART CITY»?

Die Bewegung für «Smart Citys» hat in den letzten Jahren weltweit rasant an Bedeutung gewonnen – das gilt für ihren Marktwert, das ihr zur Verfügung stehende Kapital, die technischen Entwicklungen und auch für ihren gesellschaftlichen Einfluss. In einem 2013 vom britischen Ministerium für Wirtschaft, Innovation und Qualifikation veröffentlichten Bericht wird der «weltweite Markt für mit Smart Citys zusammenhängende Problemlösungen und für die zu ihrer Umsetzung erforderlichen zusätzlichen Dienstleistungen für 2020 auf 408 Milliarden US-Dollar» geschätzt. Die exponentielle Ausdehnung des Internets der Dinge hängt mit diesem Wachstum zusammen. Laut häufig zitierten Zahlen von Cisco – einem Riesen in der Telekommunikationsbranche, die für den Bereich des Internets der Dinge und den Ausbau von «Smart Citys» besonders wichtig ist – waren im Jahr 2010 bereits «mehr als 12,5 Milliarden Geräte» miteinander vernetzt, für 2015 wird die Zahl auf 25 Milliarden Geräte geschätzt, 2020 soll sie 50 Milliarden betragen.¹ Weniger konservativen Schätzungen zufolge wird sich der Markt für «Smart Citys» in

den nächsten fünf bis zehn Jahren in einer Größenordnung von mehreren Billionen US-Dollar bewegen, wobei der Markt für das Internet der Dinge noch stärker wachsen soll. Interessant ist in diesem Zusammenhang auch die Ankündigung von IBM, in den nächsten vier Jahren drei Milliarden US-Dollar in den Aufbau einer neuen Abteilung, die ausschließlich für das Internet der Dinge zuständig sein soll, stecken zu wollen (Reuters 2015) – eine Investition, die sicherlich auch eine andere, bereits jetzt lukrative und milliarden-schwere Initiative von IBM, das «Smarter-Planet-Programm», befördern wird. Die auf Stadtplanung und Governance-Aspekte fokussierte Bewegung hat bereits viel unternommen, um die Werbetrommel zu rühren für mehr «Intelligenz» und um die Implementierung entsprechender Maßnahmen voranzutreiben. Das zeigen die Bestrebungen der wichtigsten *corporate players*, «Intelligenz» als Ideal zu verkaufen und kommunale Entscheidungsträger und Investoren für den Smartness-Hype zu begeistern. Die-

¹ Vgl. <http://share.cisco.com/internet-of-things.html>.

se Unternehmen reagieren nicht einfach auf die Nachfrage in einem bereits existierenden Markt, sondern haben viel dafür getan, diesen Markt überhaupt erst zu schaffen und ihn auf bestimmte Weise zu gestalten.

Trotz massiven Wachstums der Bewegung und beeindruckender Investitionssteigerungen bleibt weiterhin völlig unklar, was unter einer «Smart City» eigentlich zu verstehen ist. Es gibt keine allgemein akzeptierte Definition, auf die man zurückgreifen könnte (Hollands 2008). Diese Uneindeutigkeit arbeitet den BefürworterInnen und VerkäuferInnen der Smart-City-Idee in die Hände. Die Bezeichnung wird wie ein flottierender Signifikant gehandhabt, dessen Bezug sich je nach Bedarf ändern lässt. So entsteht eine Dynamik und eine Situation, die für eine Vielzahl von Produkten, Praktiken und Politiken anschlussfähig ist. Die FürsprecherInnen der «Smart City» verfügen so stets über die Möglichkeit, sich herauszureden oder sich zu distanzieren, sollte etwas schiefgehen oder eines ihrer vielen Versprechen gebrochen werden.

Die verschiedenen im Umlauf befindlichen Smart-City-Konzepte haben – zumindest aus Sicht der BefürworterInnen – den Vorteil, dass sie alle die digitalen Informations- und Kommunikationstechnologien mit positiven Veränderungen und Innovationen in Verbindung bringen. Im Wesentlichen zielen sie darauf ab, auf der städtischen Ebene ein Internet der Dinge aufzubauen, und zwar über die Installierung von vernetzten, verschiedenen Zwecken dienenden Gegenständen im gesamten urbanen Raum (und selbst in menschlichen Körpern). Die Beispiele, die typischerweise zur Veranschaulichung einer vom Internet der Dinge geprägten Welt herangezogen

werden, sind Verbraucherprodukte – etwa der allgegenwärtige intelligente Kühlschrank, der dem Geschäft meldet, wann die Milch ausgeht. Bruce Sterling (2014: 68) zufolge handelt es sich dabei jedoch um ein «Märchen»: «Das tatsächliche Internet der Dinge will in den Kühlschrank eindringen, ihn vermessen, instrumentalisieren, jegliche Interaktion mit ihm beobachten; es würde mit Freuden einen Kühlschrank zum Selbstkostenpreis abgeben.» Wenn wir den Blick allein auf Konsumgüter und Haushaltsgeräte richten, dann führt uns das auf eine falsche Fährte. Wir verbleiben an der Oberfläche und fragen nicht, was eigentlich hinter dieser absurden Farce von immer neuen Innovationen und der fast schon hysterischen Technikbegeisterung steckt. «Diese großen weltweiten Zusammenschlüsse [von Unternehmen] gibt es nicht deswegen, um den Menschen einen intelligenten Kühlschrank zu verkaufen. Die meisten von ihnen würden es tatsächlich gern sehen, dass die Menschen in einer «Smart City» leben, deren «Intelligenz» sie selbst und zu ihren Bedingungen liefern. An der Zustimmung der Bewohner in ihrer Rolle als Bürger sind sie kaum interessiert» (ebd.). Die «Smart City» ist nicht einfach eine linear verkleinerte Version eines «intelligenten Hauses», in dem all unsere persönlichen und alle Haushaltsgeräte vernetzt, automatisiert und gute Kommunikatoren sind. Es geht um ganz grundsätzliche Dinge wie infrastrukturelle und gesellschaftliche Anwendungsbereiche – also um all das, was die technopolitische Ordnung einer Gesellschaft ausmacht und bestimmt –, und es geht um die Kontrollmacht und die Daten, die aus diesen Anwendungen hervorgehen. Selbstverständlich werden nicht alle «Smart Citys» auf die gleiche

Weise geschaffen. Es lässt sich grob zwischen drei Typen unterscheiden.

Die erste und größte Gruppe ist die der «real existierenden Smart Citys», die durch technische Umrüstungen und Erneuerungen den Übergang von «dumm» zu «smart» vollziehen sollen. Die Zahl der Groß- und Kleinstädte, die solche «Intelligenz-Initiativen» aufgelegt haben, wird weltweit auf mehrere Zehntausend geschätzt, manche gehen von Hunderttausenden aus. In diesen Fällen erfolgt der Ausbau hin zur «Smart City» eher unkoordiniert «in einzelnen unabgestimmten Schritten, was eine Integration in bestehende Governance-Strukturen und die bauliche Umwelt erschwert» (Shelton u. a. 2015: 16). In der Regel sind die zugrunde liegenden Motive politökonomischer Natur. Man folgt zunehmend dem Konzept der unternehmerischen Stadt, demzufolge es die Aufgabe lokaler Regierungen ist, ihre Stadt zu einem wettbewerbsfähigen (regionalen oder globalen) Zentrum von wirtschaftlichen Aktivitäten und Wachstum zu machen (Harvey 1989). «Intelligent werden» erscheint als ein bequemes Allheilmittel, um Austerität zu überwinden, die Verwaltung des städtischen Systems zu verbessern und um zu einem attraktiven Investitionsstandort zu werden – alles mittels «vernetzter Infrastrukturen, die die wirtschaftliche und politische Effizienz steigern sowie soziale, kulturelle und städtische Entwicklung ermöglichen sollen» (Hollands 2008: 307). «Intelligenz-Initiativen», so das Versprechen, geben den Stadtverwaltungen die Mittel an die Hand, um sich wirtschaftlich behaupten zu können.

Die zweite Gruppe von Städten ist die, bei denen die Methode der «Schocktherapie» oder des «Intelligenz-Schocks» zur

Anwendung kommt. Dabei geht es um die schnelle und großräumige Umsetzung «intelligenter» Ideale, Technologien und Politiken und um ihre möglichst umfassende Integration in die bestehende städtische Landschaft. Bislang ist dieser Ansatz noch in keiner Stadt wirklich in Gänze zur Anwendung gekommen, aber es lassen sich Beispiele nennen, in denen der Übergang zur «Smart City» wesentlich schneller erfolgte und weitreichender war als beim typischen Fall der Nach- oder Umrüstung. Das beste Beispiel ist vielleicht das sogenannte Intelligent Operations Center, das IBM 2010 für Rio de Janeiro eingerichtet hat. Dort laufen «Datenströme aus 30 Behörden, die unter anderem für den Straßenverkehr, den öffentlichen Nahverkehr, kommunale Versorgungsleistungen, Rettungsdienste und die Wettervorhersage zuständig sind, in einem einzigen Analysezentrum zusammen. Hinzu kommen Informationen, die städtische Angestellte und die allgemeine Öffentlichkeit über Telefon, Internet und Radio liefern.» (Kitchin 2014: 6) Mit diesem an die NASA erinnernden Kontrollzentrum ist die Stadt Rio in ein «Optimierungs- und Sicherheitssystem» verwandelt worden. Es ermöglicht eine präzisere Überwachung und Regulierung bestimmter Stadtteile und verstärkt damit bereits gängige Praktiken militaristischer urbaner Kontrolle (Wacquant 2008). IBM und andere Technologiefirmen haben anderswo ähnliche Zentren für einzelne städtische Ämter und Einrichtungen wie Polizeibehörden aufgebaut, aber keines von ihnen hat bislang die Größenordnung des Intelligent Operations Center in Rio erreicht. Vieles spricht jedoch dafür, dass Rio eine Vorreiterfunktion einnimmt und wir auch in anderen Städten mit der Einrichtung und

dem Einsatz von ähnlichen Systemen rechnen können.

Drittens gibt es das «idealistische Modell» der «Smart City». Dabei handelt es sich um Projekte, die von Grund auf neu gebaut werden, an Orten, an denen vorher nichts Städtisches existierte. Ein Paradebeispiel hierfür ist New Songdo in Südkorea, das als globales Testfeld (Halpern u. a. 2013) oder urbanes Laboratorium (Gieryn 2006) gilt, um im großen Maßstab die Umsetzung von «intelligenten Systemen in der Wildnis» zu erproben. Die Kosten dieses Projekts belaufen sich auf etwa 40 Milliarden US-Dollar; seine Unterstützer in Wirtschaft und Regierung hoffen, dass New Songdo als die erste richtige «Smart City» in die Geschichte eingehen wird. Christine Rosen (2012) schreibt dazu: «Songdos Anspruch, besonders intelligent zu sein, hat nichts mit der Intelligenz seiner Einwohner zu tun, sondern basiert auf den Millionen drahtloser Sensoren und Mikrorechner, die überall in der Stadt in Oberflächen und Gegenstände eingebaut sind.» Diese Art der Umsetzung des Smart-City-Konzepts stellt wohl die Zukunft dar, zumindest gibt sie uns einen Eindruck von den Möglichkeiten und den ehrgeizigen Plänen für die Stadtentwicklung der Zukunft. Allerdings verweist dieser Typus der «Smart City» auch auf frappierende Ähnlichkeiten zwischen der Ideologie der «Smart City» und der Ideologie, die der modernistischen Architektur des 20. Jahrhunderts zugrunde lag. Man denke nur an Brasília, die Hauptstadt Brasiliens, Verkörperung und Monument modernistischer Ideale und technokratischer Verwaltung, die in nur 41 Monaten (1956–1960) mitten im Regenwald des Amazonas auf einem zuvor gerodeten Gelände hochgezogen wur-

de (Scott 1998). Nach Adam Greenfield (2013: 1274) «begehen die Konstrukteure von Songdo, Masdar und PlanIT Valley [alles klassische Beispiele für Smart Citys] mehr oder minder die gleichen Fehler wie die Erbauer von Chandigarh und Brasília – überdimensionierte und großspurige Planungen, angeleitet von wissenschaftlichem und autoritärem Denken, was sich unter anderem im Bau von gewaltigen Hauptverkehrsachsen zeigt –, ohne dass man sagen könnte, ob dies aus Ignoranz, Geschichtsvergessenheit, Achlosigkeit oder Selbstüberschätzung geschieht.»

Wir halten es trotz der Vielfältigkeit der Methoden und Motive für möglich und notwendig, die sozialpolitischen Logiken, die unseres Erachtens allen diesen Smart-City-Initiativen zugrunde liegen, herauszuarbeiten und zu benennen. Zurzeit sieht es nicht danach aus, als wäre die Entwicklung hin zu «Smart Citys» noch aufzuhalten. Die auf unterschiedliche Weise umgesetzten Ideale und Praxen der Smart-City-Bewegung dominieren inzwischen die stadtentwicklungspolitischen Auseinandersetzungen und «kolonisieren» das Denken der politisch Verantwortlichen. Angesichts des knappen Raums, der uns hier zur Verfügung steht, können wir zu den ideologischen Aspekten nur einen Überblick geben. Dieser dient zur Erläuterung unserer kritischen Gesellschaftstheorie, die für uns im Zentrum dieses Aufsatzes steht. Eine ausführlichere genealogische Analyse der vorherrschenden Diskurse und Ideologien (vor allem die der wichtigsten Akteure auf Unternehmerseite wie IBM, Cisco und Siemens), die diese sozialtechnischen Systeme und Politiken vorantreiben, finden interessierte LeserInnen in Adam Greenfields gründlich recherchiertem

Buch «Against the Smart City» (2013). Wir möchten an dieser Stelle zudem betonen, dass wir die Bezeichnung «Smart City» im Folgenden auch als Kürzel für alle Technologien und Techniken verwenden, die im Zusammenhang mit den Praktiken und Ideologien des Labels «Smart City» stehen – unabhängig davon, wie und in welchem Umfang diese tatsächlich zum Einsatz kommen. Es geht uns nicht darum, die Unterschiede bei den Bedeutungen, die das Konzept der «Smart City» für verschiedene Städte, politische Entscheidungsträger und Unternehmen einnimmt, einzuebnen oder zu ignorieren.

Wir hoffen vielmehr aufzeigen zu können, dass scheinbar voneinander unabhängige Technologien und Techniken einen gemeinsamen Ursprung in bestimmten gesellschaftspolitischen Logiken haben und dass sie diese Logiken reproduzieren. Um dies deutlich zu machen, werden wir näher auf einige ausgewählte Initiativen eingehen. Der folgende Abschnitt jedoch, der auf Greenfields Studie basiert und deren Ergebnisse in gewisser Weise vertieft und aktualisiert, stellt zunächst einmal die Ideologie vor, die hinter den Smart-City-Initiativen steht und von diesen verbreitet wird.

DIE IDEOLOGIE DER «SMART CITY»

Dort, wo unmittelbar Einfluss auf die Politik genommen wird, dominieren bestimmte liberale und vom Meliorismus² geprägte Vorstellungen vom Fortschritt, der durch die Informations- und Kommunikationstechnologien angeblich ermöglicht wird. So preisen zwei Vorstandsmitglieder von Cisco in einem vielfach zitierten Artikel der Zeitschrift *Foreign Affairs* die Vorteile des «Internets of Everything» an und propagieren seine Anwendung auf nahezu sämtliche Bereiche städtischer Infrastruktur und Governance (Chambers/Elfrink 2014). Ihr Versprechen: eine «intelligente und effiziente Verwaltung der wachsenden Städte», die dabei helfen kann, Probleme wie «verstärktes Verkehrsaufkommen, Parkplatzmangel, Umweltverschmutzung, wachsenden Energieverbrauch und Kriminalität» in den Griff zu bekommen. Wer könnte etwas dagegen haben? Der einzige Preis, so versichern Chambers und Elfrink, bestehe in einer geringfügigen

Neujustierung von Governance-Strategien und Anpassungen bei der Auftragsvergabe im Bereich der Informationstechnologien (IT). Erstens müsse «die Welt neu über IT-Investitionen nachdenken, Abstand nehmen vom Einkauf isolierter Dienstleistungen und sich stattdessen auf End-to-End-Lösungen konzentrieren, um disparate und parzellierte Systeme zusammenzuführen». Zweitens komme es auf «eine besonders intensive Abstimmung und Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor» an, wobei die «Einhaltung von festgelegten Vertragsregeln und -fristen entscheidend» sei. Die beiden Autoren, die «Smart Cities» zur «Norm» machen wollen, fordern in einem ihrer im Aufsatz formulierten Grundsätze «die Welt» dazu auf, «sich Technologien auf neue Weise anzueignen». Dabei müssten

² Eine theoretische Strömung, die davon ausgeht, dass die sozialen Verhältnisse durch fortgesetzte Steuerung besser werden (Anm. d. Ü.).

der «Vertrag mit den Bürgern» sowie die Dienstleistungen, die IT-Unternehmen und Regierungen diesen zur Verfügung stellen, neu überdacht werden (ebd.).

Wenn wir die Absichten, die sich hinter dieser technokratisch daher kommenden Agenda der «Smart Citys» verbergen, begreifen wollen, ist es wichtig, darauf zu achten, wie hier eine subtile Verschiebung im politischen Vokabular stattgefunden hat – an die Stelle eines Gesellschaftsvertrags tritt tendenziell ein neuer Vertrag zwischen Staat und Unternehmen (vgl. Sadowski/Selinger 2014). Das erklärt auch, weshalb sechs der von Chamber und Elfrink formulierten Grundsätze «die politischen Entscheidungsträger in den Kommunen» dazu drängen, den von der IT-Branche neu entwickelten Produkten und Dienstleistungen (noch) mehr Bedeutung beizumessen. Den Autoren, beides gewiefte Geschäftsleute, ist die Asymmetrie in den Public-private-Partnerships im Zeitalter des Neoliberalismus nicht entgangen. Wenn Topmanager ein Vielfaches des Gehalts eines hochrangigen Beamten erhalten, dann darf man sich nicht darüber wundern, wenn Letztere es dem Privatsektor bereitwillig erlauben, den öffentlichen Sektor nach dessen Vorbild umzugestalten. Firmen können sich einen ganzen Stab von Betriebswirten, Entwicklerinnen, Designern, Anwältinnen und PR-Spezialisten leisten, die alle darauf geschult sind, eine bestimmte städtische Entwicklung und Zukunft als technokratische *pensée unique* darzustellen. Was fehlt, sind wirkliche «Alternativentwürfe», die man dem von Großkonzernen vertretenen Smart-City-Modell entgegensetzen könnte, was unter anderem damit zusammenhängt, «dass sich die meisten Städte schon län-

ger einem wirtschaftsfreundlichen und unternehmerischen Konzept städtischer Entwicklung verschrieben haben» (Holands 2015: 70).

Selbstverständlich verfolgt Cisco hier kommerzielle Interessen: Der Entwurf, die Herstellung und Installierung der für die anvisierten Netzwerke erforderlichen Hardware sind das Kerngeschäft von Cisco. Dessen zukünftigen Gewinnmargen dürften nicht zuletzt davon abhängen, inwieweit es dem Unternehmen gelingt, überzeugende Narrative der «Smartness» zu entwickeln. Eine Vielzahl von LokalpolitikerInnen und gemeinnützigen Organisationen ist inzwischen ebenfalls auf den fahrenden Zug aufgesprungen. Auch hier dürften materielle Anreize eine Rolle spielen. Darauf verweisen politökonomische Analysen zu Drehtüreffekten auf dem Arbeitsmarkt, womit gemeint ist, dass es inzwischen eine gewisse Durchlässigkeit zwischen dem privaten, dem öffentlichen und dem sogenannten Dritten Sektor gibt. Wenn Beamte ihr Gehalt jederzeit um ein Vielfaches erhöhen können, indem sie sich gefügig und kooperativ verhalten und bei einem entsprechenden Angebot ihre Anstellung in einer Behörde gegen ein Firmenbüro eintauschen, dann verwundert es nicht, dass nur wenige unangenehme Fragen stellen (Carpenter/Moss 2013). Galt früher eine Beratungstätigkeit für Privatunternehmen unvereinbar mit der Ausübung eines öffentlichen Amtes, so sind auch hier die Barrieren heute viel geringer.

Genauso wichtig wie materielle Anreize und Karriereüberlegungen dürfte jedoch sein, dass mit auf technologische Aspekte fokussierten Smart-City-Erzählungen bestimmte urbane Entwicklungen und Veränderungen gerechtfertigt wer-

den können (Söderström u. a. 2014). Der Geograf Rob Kitchin betrachtet die Forschung zu ›Smart Citys‹ – egal ob sie regierungsnahen Kreisen oder dem Unternehmenslager zuzuordnen ist – deswegen als kritisch, weil «ein Großteil dessen, was über ›Smart Citys‹ geschrieben oder gesagt wird, als unideologisch und pragmatisch daherkommt, als Ausdruck des gesunden Menschenverstands» (Kitchin/Dodge 2011: 131). Es ist aber vielmehr Auswuchs einer neoliberalen technologiebesessenen Ideologie sowie einer allgemeineren politökonomischen Haltung, der es vor allem um Gewinnmaximierung und höhere Steuereinnahmen geht. BefürworterInnen von Smart-City-Konzepten tun so, als wollten sie nur ganz nüchtern Probleme lösen, als seien sie über eine bestimmte Nullsummenpolitik erhaben, die sooft zu einem Reformstau führt. Sie neigen dabei allerdings schnell zu einer Einstellung, die Clifford Geertz (1973: 194) in einem berühmt gewordenen Satz zugespitzt zusammengefasst hat: »Ich vertrete eine Gesellschaftsphilosophie, Sie vertreten politische Ansichten, er vertritt eine Ideologie.« Mit dem «Ich» könnte ein Unternehmer gemeint sein, der mit Smart-City-Technologien sein Geld verdient, mit dem «Sie» eine städtische Entscheidungsträgerin, und das «Er» könnte auf die verschiedenen Interessengruppen bezogen sein, die grundlegende Bedenken gegen die ausufernde Überwachung und Zusammenführung von Daten äußern. Eine Zitat aus einer Rede von Samuel Palmisano (2010), ehemaliger Vorstandsvorsitzender, Präsident und Geschäftsführer von IBM, illustriert diese Haltung: «Der Plan, eine intelligentere Erde zu schaffen, ist deswegen realistisch, weil er so erfrischend unideologisch ist.» Doch der

Vorwurf, etwas sei «ideologisch», gehört zu einem der gängigsten Tricks moderner Rhetorik, mit dem diejenigen, die ihre Gegner der Ideologie bezichtigen, ihre eigenen anfechtbaren Werte und Annahmen dethematisieren wollen. Wenn wir selbst im vorliegenden Aufsatz den Begriff der Ideologie verwenden, dann nicht a priori im Sinne einer Anschuldigung, sondern in seiner beschreibenden Funktion. Manchmal steckt dahinter auch eine ironische Absicht, weil so viele Techniker und Neoliberale derart viel Energie darauf verwenden, ihr Handeln als Ergebnis wertfreier Entscheidungen sowie fortschrittsorientierter und außermenschlicher Überlegungen und Kräfte (etwa der Technik oder des Marktes) zu verkaufen.

Es lohnt sich, an dieser Stelle kurz auf die Überlegungen des Philosophen und Rechtstheoretikers Lawrence Solum einzugehen, der ein Gedankenexperiment zu «Smart Citys» vorgeschlagen hat. Dies hilft uns dabei, besser den politischen Charakter der Smart-City-Rhetorik zu verstehen. Solum schreibt über Singapur: Diese Stadt verfügt über «intelligente Kreuzungen, deren Ampelschaltungen je nach Verkehrslage variieren» (Baum 2001), und es sind noch viel ausgefeiltere Methoden zur Kontrolle des Autoverkehrs denkbar. Solum (2014: 75) erwägt die Entwicklung einer «Artificially Intelligent Traffic Authority», die sich an «Veränderungen des Fahrverhaltens und des Verkehrsflusses anpassen würde». Das System wäre in der Lage, «jederzeit Änderungen vorzunehmen und kontrollierte Experimente durchzuführen, um auszuwerten, wie sich verschiedene Kombinationen auf die Verkehrsentwicklung auswirken» (ebd.) – was an Jim Manzi (2012) Empfehlung an Verwaltung und

Politik erinnert, diese müssten grundsätzlich experimentierfreudiger werden. Das von Solum (2014: 75) vorgestellte System hätte jedoch keine Toleranz gegenüber Experimenten Einzelner, insbesondere dann, wenn diese auf die Übertretung seiner Regeln hinausliefen. Vielmehr würden, so seine Vorstellung, «Verstöße durch ein ausgefeiltes System elektronischer Überwachung ermittelt», die «Zuwiderhandelnden identifiziert und durch an wichtigen Kreuzungen stationierten Kränen augenblicklich aus dem Verkehr gezogen».

Solum bedient sich dieses Beispiels, um die übliche juristische Unterscheidung zwischen menschlicher und künstlicher Intelligenz aufzuheben. Es geht ihm weniger darum, tatsächlich das Verkehrssystem zu verbessern. Sein Szenario eignet sich auch, um auf die rechtlichen und politischen Probleme automatisierter Strafverfolgung aufmerksam zu machen, die selbst in einem scheinbar rein technischen Bereich wie der Verkehrsführung unweigerlich auftreten. Würden die von Solum angedachten Kräne mit der gleichen chirurgischen Genauigkeit auch Demonstranten aus dem öffentlichen Raum entfernen, wenn diese, wie etwa in Ferguson geschehen, Straßen blockieren (Harcourt 2012)? Würden Personen mit abgelaufenem Führerschein oder Autokennzeichen ebenfalls herausgegriffen werden? Dass dieses Szenario schon zur Hälfte Realität ist, zeigen Erfahrungen aus den USA: Dort sorgen auf besonders einkommensschwache Kunden spezialisierte Kreditunternehmen dafür, dass deren Pkw per Fernbedienung lahmgelegt wird, wenn Zahlungen ausbleiben (Sadowski/Pasquale 2014).

Die Herausforderung für die BefürworterInnen von «Smart Citys» besteht dar-

in, mehrere Spannungen oder gar offene Widersprüche, die ihr Idealtypus der unternehmerischen Governance aufweist, aufzulösen oder zumindest abzuschwächen. Wer wird letztlich verantwortlich sein für die geforderten «hyperkollaborativen Partnerschaften zwischen dem öffentlichen und dem Privatsektor»? Mit welchen Sanktionen soll beispielsweise die Nichteinhaltung von festgelegten Fristen bestraft werden? Wer verhängt diese Sanktionen? Und welche Probleme sollen eigentlich mit den sogenannten End-to-End-Lösungen behoben werden, und wie würde die Umsetzung solcher «Lösungen» aussehen?

Sollten etwa, um einige weitere naheliegende Fragen und Beispiele zu nennen, neue Formen der Überwachung vor allem bei der Verfolgung von Drogendelikten Verwendung finden? Oder wollen wir sie nutzen, um Hinweisen auf Wirtschaftsverbrechen nachzugehen oder um illegales Arbeitgeberverhalten zu sanktionieren? Lohndiebstahl etwa ist ein massives Problem, wird aber von den Behörden selten ernst genommen (Bobo 2011). Sollen in Restaurants installierte Kameras und Sensoren vor allem dazu dienen, die Beschäftigten zu kontrollieren und sie davon abzuhalten, Lebensmittel zu entwenden? Oder ist es wichtiger, Lebensmittelvergiftungen zu verhindern oder Verstöße gegen Sicherheitsauflagen zu ahnden? Gehört zu den Zielen der «Verkehrskontrolle» auch, die gesundheitsgefährdende nächtliche Lärmbelästigung durch Motorräder in vielen Stadtvierteln zu reduzieren? Oder betrachtet man dies als Lapalie, für die es keine computerbasierte Überwachung braucht? Jedes Jahr werden Millionen solcher Verkehrsvergehen von der Polizei mit großer Kulanz behan-

delt, während sich in der Öffentlichkeit aufhaltende AfroamerikanerInnen unter dem Vorwand, «Gehwege zu blockieren», regelmäßig von Sicherheitskräften schikaniert werden (Taibbi 2014). Hätte für automatisierte Autoüberwachungssysteme Priorität, den Tod von Fußgängern zu verhindern, oder wäre das Ziel eher die Gewährleistung eines gleichmäßigen Verkehrsflusses in Richtung Stadt und aus der Stadt heraus, um Autofahrern Zeit zu ersparen?

Basierend auf fragwürdigen Kosten-Nutzen-Rechnungen bietet die neoliberale Ideologie viel zu häufig und vorschnell «naheliegende» und kaum hinterfragte Antworten an. Zu den wichtigsten Zielsetzungen des Neoliberalismus zählen die Verbesserung des wirtschaftlichen Umfelds sowie die Übertragung von Marktlogiken auf alle Bereiche des menschlichen Lebens. Doch selbst wenn man diese neoliberalen Vorgaben akzeptiert, sind die Probleme kaum zu übersehen, die sich etwa ergeben, wenn von staatlichen Akteuren erwartet wird, wirtschaftliche Ziele zu verfolgen (und umgekehrt). Der Staat selbst sieht sich gezwungen, die «Emanzipation» seiner Untertanen von seinen Strukturen voranzutreiben und diesen Vorgang zugleich koordinieren zu müssen. Philip Mirowski (2013: 58) beschreibt dies als eine Tendenz des Neoliberalismus, alles auf einmal haben zu wollen: «Es wird lautstark vor den Gefahren einer Ausweitung staatlicher Zuständigkeiten gewarnt, zugleich aber stellt man den starken Staat, der ihnen zusagt, als zahnlos dar.» Solche Spannungen sind ein formales Merkmal ideologischen Denkens: Dabei wird versucht, in Theorie oder Praxis widersprüchliche Verpflichtungen abzuschwächen und anzupassen (vgl. Geertz 1973).

Auch wenn man solche ideologischen Ansichten vor allem mit der Wall Street und Silicon Valley in Verbindung bringt, sind sie selbst in unseren wichtigsten gesetzgebenden Körperschaften präsent. Im Februar 2015 fand im Senat des US-Kongresses eine Anhörung unter dem Titel «Die vernetzte Welt: Untersuchung des Internets der Dinge» statt,³ wo eine Reihe von SenatorInnen und fünf ExpertInnen zu Wort kamen. Fast alle zeigten sich begeistert von dem Versprechen eines «intelligenteren Lebens», das wir angeblich dank des Internets der Dinge demnächst alle führen werden. Zwar wurde gelegentlich auf grundlegende Probleme wie Gefährdungen der Sicherheit und der Privatsphäre verwiesen, doch galten die meisten Sorgen der «Überregulierung». In seiner Erklärung brachte der demokratische Senator Cory Booker aus New Jersey recht anschaulich die politökonomische Ideologie, die in dieser Anhörung allgegenwärtig war, zum Ausdruck. Bookers Position, die er mit besonders viel Enthusiasmus und besonders klaren Worten vorbrachte, ist in gewisser Weise repräsentativ, sodass wir ihn hier ausführlich zitieren:

«Wir haben heute die ungewöhnliche Chance, parteiübergreifend und aus tiefst patriotischen Motiven heraus ein Programm zu entwickeln für etwas, das zu einem explosiven Wachstum unserer Wirtschaft beitragen kann. Es geht um Billionen von Dollar, um die Schaffung zahlloser Arbeitsplätze, um die Verbesserung der Lebensqualität und um die Demokratisierung unserer Gesellschaft. Damit entstehen neue Möglich-

³ Vgl. www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=d3e33bde-30fd-4899-b30d-906b47e117ca&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a.

keiten für marginalisierte, an den Rand gedrängte Menschen und können Rassen- und Klassenschranken eingerissen werden. Auch wenn uns vielleicht die Vorstellungskraft fehlt, um uns diese Zukunft mit all ihren Verheißungen auszumalen, sollten wir diese Zukunft mit offenen Armen begrüßen. [...] Deswegen teile ich das Anliegen, das meine Kollegen von der Republikanischen Partei bereits angesprochen haben. Wir sollten alles tun, um diese Entwicklung zu fördern, und alles unterlassen, was sie einschränken könnte. [...] Alles, was einen solchen Sprung nach vorn für die Menschheit behindern könnte, ist abzulehnen. [...] Und ich meine, dass hier eine Public-private-Partnership angebracht ist. Wir alle haben hier eine Aufgabe zu übernehmen.»

Die Auffassung, die Booker vorgetragen hat, mag radikal klingen, ist sie aber nicht. Er vertritt hier vielmehr Mainstream-Ansichten. Das Mindeste, was man demnach von uns erwarten kann, ist, die Entfaltung der Innovationskräfte nicht zu behindern. Aber eigentlich will man uns dazu verpflichtet, Innovationen wie das Internet der Dinge und diejenigen, die dieses erfunden haben und propagieren, jede erdenkliche rechtliche, materielle und ideologische Unterstützung zukommen zu lassen. Wer kritische Fragen zur Zukunft stellt oder gar die Absicht hat, technische Entwicklungen zu entschleunigen und zu regulieren, blockiert in dieser Sicht nicht nur Chancen enormen wirtschaftlichen Wachstums, sondern auch eine Kraft, die mehr Demokratie und soziale Gerechtigkeit verspricht.

Bookers Sprache erinnert an die Marktschreierei des Finanzkapitals – just an jene Interessengruppe, die er 2012 nach Kräften verteidigte, nachdem Barack Ob-

ama, also sein Parteichef, vorsichtig angedeutet hatte, es sei an der Zeit, über die Schließung von Steuerschlupflöchern für Private-Equity-Fonds nachzudenken. Für die Kapitalmärkte ist die Überbewertung der «Smart City» von entscheidender Bedeutung, da die extrem ungleiche Vermögensverteilung Rentiers erlaubt, von den geringfügigen Zinsen auf nahezu risikofreie Staatsschulden gut zu leben. Nimmt man Expertenwarnungen vor den jetzt bereits im Internet der Dinge grassierenden Sicherheitsproblemen ernst, dann wird das «smarte Kapital» die «Smart City» demnächst wohl noch stärker als eine lukrative spekulative Anlagemöglichkeit betrachten. (Bruce Schneier [2014] hat darauf hingewiesen, dass mit der Einbettung von Rechenleistungen in Hardware, was auf einen Großteil des Internets der Dinge zutrifft, Sensoren und Router «besonders anfällig für Manipulierungen werden, ohne dass es ein gutes Mittel gibt, diese Sicherheitslücken zu schließen».) Je riskanter die Investition, umso spektakulärer muss der potenzielle Gewinn sein: Daher werden Smart-City-Technologien immer häufiger als epochal, bahnbrechend oder weltverändernd beworben.

Die Rhetorik ist natürlich nicht immer so vollmundig. Es gibt auch gegenläufige Tendenzen, bei der Beschreibung von Technologien einen eher nüchternen, analytischen und mechanisch-objektiven Ton anzuschlagen. Nichtssagende Überparteilichkeit ist ein weiteres beliebtes rhetorisches Mittel. Smart-City-Befürworter schreiben Manifeste, Handbücher und Aufrufe und führen hier immer wieder die gleichen offensichtlichen Probleme an, bei denen wir uns alle einig sind, dass sie gelöst werden müssen (Newsom 2013; Townsend 2014). Da-

mit wird unter anderem aber verschleiert, was bei der automatisierten Überwachung und Reglementierung eines jeden Augenblicks und eines jeden Ortes auf dem Spiel steht. So mag uns eine vor Schlaglöchern warnende App zu mehr Informationen über ein für Autos schädliches Übel verhelfen (wenn es auch nicht die Beseitigung dieses Übels garantieren kann). Aber nicht jeder ist mit der Einschätzung einverstanden, wir bräuchten «postprogressive» Stadtverwaltungen, die sich «auf Ergebnisse und *nicht* auf Regeleinhaltung» konzentrieren (Goldsmith/Crawford 2014: 6) – jedenfalls dann nicht, wenn mit den angestrebten «Ergebnissen» weitaus mehr gemeint ist als nur eine zügige Müllentsorgung oder Straßen ohne Schlaglöcher. Tatsächlich ist bereits die Entscheidung, Ressourcen für die Planung von Fahrbahnen einzusetzen (und nicht etwa für die Belüftung von Zügen und Bussen oder für Grünflächen) eine grundsätzlich politische. So feiern Goldsmith und Crawford ein neues «intelligentes» Verfahren zur Erkennung von Fingerabdrücken als hilfreiches Instrument der Verbrechensbekämpfung (ebd.: 112), ohne auch nur zu erwähnen, dass mit solchen Fingerabdruck-Datenbanken neue Unterklassen von Personen produziert werden, die de facto keine Chance mehr auf eine Anstellung haben. Smart-City-BefürworterInnen könnten einwenden, dass in jedem politischen System um die Mittelverteilung gestritten wird und dass man von ihren Sensoren, Apps, offenen Datenbanken und Verlaufsberichten nicht erwarten kann, dass sie solche Konflikte beseitigen. Aber es gibt noch weitere Sachzwänge: So benötigen etwa politische Auseinandersetzungen, Reflexionen und Aktivitäten Zeit. Die Zeit, die etwa damit zugebracht

wird, eine «Plattform» einzurichten, «mittels derer sich Bürger über SMS- und Mailboxnachrichten, soziale Netzwerke und verschiedene Apps mit der Stadtverwaltung sowie miteinander verständigen können» (ebd.: 4), steht nicht für die Aufklärung darüber zur Verfügung, wie die Steuerhinterziehung der Wohlhabenden erst jenen Personalangelmangel herbeigeführt hat, zu dessen Behebung «Smart Citys» durch die «Kräftebündelung» der verbliebenen städtischen Angestellten dann beitragen sollen (Winters 2011; Bady 2013). Die Schulen von Newark in New Jersey bräuchten Mark Zuckerbergs Spende über 100 Millionen US-Dollar nämlich gar nicht, wenn sich nicht so viele andere Milliardäre erfolgreich dafür eingesetzt hätten, die Steuern für Reiche zu senken, und wenn sie sich nicht dafür entschieden hätten, ihr Vermögen im Ausland zu parken und den Regulierungsbehörden die Zähne zu ziehen. Jedes Mal, wenn ein Unternehmer und mehrfacher Milliardär den Einsatz innovativer neuer Methoden vorschlägt, um den «Output» von Regierungsangestellten zu messen und zu maximieren, sollten kritische BürgerInnen aufmerken und fragen: Warum sind wir überhaupt an diesem Punkt angelangt? Woher kommt der Druck, ständig «aus weniger mehr» zu machen? Konzentriert man sich auf die technischen Herausforderungen des «Mehrmachens», dann verhindert man dadurch eine kritische Auseinandersetzung darüber, weshalb es überhaupt «weniger» staatliche Ressourcen und Angestellte gibt.

Die hinter dem Ideal der «Smart City» stehenden Akteure aus Wirtschaft und Politik haben mit zwei Strategien zur einer Verzerrung der Debatte beigetragen: Erstens ist ihr einseitiger Fokus auf

Transparenz- und Effizienzsteigerungen zu nennen, der die revolutionären Veränderungen bei der Strafverfolgung (hinsichtlich Intensität und Reichweite) und die negativen Auswirkungen außer Acht lässt, die mit dem Ausbau von umfassenden Überwachungssystemen verbunden sind, auch deswegen weil man sie so leicht in ein Regime räumlichen Rechts einbetten kann. Zweitens reduzieren sie die vielen politischen und ethischen Fragen, die die über das Internet der Dinge vorangetriebene Digitalisierung des Raums aufwirft. Für sie sind, wenn überhaupt, nur nachträgliche Korrekturen und Beschränkungen technischer Systeme denkbar, und auch dann nur, um die «Privatsphäre» in einem individualistischen Sinne zu schützen, nämlich als Recht auf eine Kontrolle über die Sammlung von Informationen über sich selbst. Denkt man in Kategorien einer Hermeneutik des Verdachts, dann ergibt sich eine umfassendere – und äußerst be-

unruhigende – Perspektive auf «Smart Citys». Selbst an dem Ende des vom Internet der Dinge geschaffenen «Spektrums der Kontrolle», an dem die Eingriffe am geringfügigsten sind, steht weitaus mehr auf dem Spiel, als dass dies einige nebulöse Bedenken in Bezug auf die Wahrnehmung und Reputation von Menschen, die üblicherweise unter dem Begriff der «Privatheit» zusammengefasst werden, vermuten lassen. Und am anderen Ende des Spektrums geht es um wirklich viel. Das Internet der Dinge ist nicht einfach eine Möglichkeit, Menschen zu beobachten und zu überwachen, sondern mit ihm können auch bestimmte Interaktionsmuster erzeugt und reproduziert werden (Bogard 1996). Sobald genügend Daten über die Menschen gesammelt und diese dann in einer Maschine, die ihr Verhalten simulieren kann, gespeichert worden sind, wird es irgendwann möglich sein, Menschen durch Roboter zu ersetzen.

«SMART CITYS» IN KONTROLLGESELLSCHAFTEN

Was erfordert eine Gesellschaftstheorie der «Smart City»? Anders als die Ideologie ihrer BefürworterInnen ist eine Gesellschaftstheorie eine «systematische, von historischen Kenntnissen unterfütterte und empirisch ausgerichtete Theorie, die das Wesen des «Sozialen» zu erklären versucht», wobei das Soziale «zu verstehen ist als das ganze Spektrum wiederkehrender Formen, Muster und Merkmale von zwischenmenschlichen Interaktionen und Beziehungen» (Cotterell 2006: 15). Im städtischen Raum und Umfeld sind die Interaktionen idealtypisch geprägt von den Spannungs-

verhältnissen Umverteilung/Extraktion, Unterdrückung/Emanzipation sowie Anerkennung/Missachtung (Fraser 1995). Eine genauere Untersuchung dessen, was es bedeutet, ein überwachtes Subjekt oder ein Datensubjekt zu sein, würde zeigen, wie schutzlos jede und jeder in der «Smart City» Extraktion, Unterdrückung und Missachtung ausgesetzt ist. Foucaults Begriff der Biomacht ist gut geeignet, um hier einige Aspekte zu klären. Eine Form der Biomacht ist, wie Foucault (1986: 134 f.) schreibt, «um den Körper als Maschine zentriert [...]. Seine Dressur, die Steigerung seiner Fähigkei-

ten, die Ausnutzung seiner Kräfte, das parallele Anwachsen seiner Nützlichkeit und seiner Gelehrigkeit, seine Integration in wirksame und ökonomische Kontrollsysteme – geleistet haben all das die Machtprozeduren der Disziplinen: politische Anatomie des menschlichen Körpers.» Im Gegensatz zu den Wirkungsweisen der souveränen Macht, die das Recht ausübte, «sterben zu machen oder leben zu lassen» (ebd.: 134), ist die disziplinierende Biomacht darauf aus, Körper und Bevölkerungen zu verwalten und zu steuern. In der «Smart City» wird mit Menschen genau auf diese Weise umgegangen – wenn BürgerInnen etwa als analoge und digitale Informationsschnittstellen oder gar als «Bürger-Sensoren» betrachtet werden (Gabrys 2014: 32). Darüber hinaus wird die Stadt als solche aber auch neu erfunden und rekonstruiert, nämlich als Maschine, die verwaltet und gemanagt werden kann und muss. Ein von Foucaults Begriff der Gouvernementalität inspirierter Theoretiker hat diese Art von Disziplinierung als *smartmentality* bezeichnet (Vanolo 2014). Der Begriff Biomacht ist zweifellos hilfreich, erhellt aber nur einen Ausschnitt des Gesamtgeschehens. Wir stützen uns bei unserem Versuch, die «Smart City» zu ergründen, daher auf einen weiteren theoretischen Ansatz, der explizit den Anspruch formuliert hat, über die Foucault'sche Disziplinargesellschaft hinauszugehen, so wie Foucaults Modell bereits das Konzept der «Gesellschaften der Souveränität» hinter sich gelassen hatte. Die Rede ist von Gilles Deleuzes' (1993) Theorie der «Kontrollgesellschaft». War das Symbol der souveränen Macht Foucault zufolge das Schwert und das der Disziplinarmacht die Fabrik, dann spielen in der Kontrollgesellschaft

Computernetzwerke eine entscheidende Rolle (Deleuze 1993). Nun verschwinden durch die Herausbildung einer neuen Art der Machtausübung die anderen nicht einfach aus der Welt. Die Frage ist daher, welche davon heute die dominante Funktionslogik ist. Bezogen auf Informations- und Kommunikationstechnologien und insbesondere auf die vernetzten Technologien der «Smart Citys» verdeutlicht der von Deleuze vorgeschlagene Deutungsrahmen die Logiken, die all diesen Praktiken und Ideologien zugrunde liegen. Im Folgenden wollen wir skizzieren, was diese Gesellschaftstheorie mit Blick auf die «Smart City» leisten kann.

Die Deleuze'sche «Kontrollgesellschaft» hat mindestens drei zentrale Komponenten – Dividuen, Rhizome und Passwörter – die zusammen genommen eine anhaltend wirkmächtige Logik hervorbringen. Wenn eine Person eine andere Person beobachtet, dann liefert deren elementarer Wahrnehmungsapparat (Augen und Sehvermögen) zumindest eine oberflächliche ganzheitliche Bewertung dieser Person. Es ist beispielsweise schwer vorstellbar, dass man bei der Betrachtung der Kleidung nicht auch zugleich das Geschlecht wahrnimmt oder den Umstand, dass jemand hinkt, schnell geht, groß oder klein ist. Hinzu kommen noch Hunderte anderer impliziter Informationen, die das Auftreten einer Person vermitteln kann. Werden Menschen dagegen von Sensoren überwacht, dann werden aus Individuen «Dividuen»: Entitäten, die jederzeit in eine beliebige Anzahl von Teilaspekten aufgespalten werden können, wobei einzelne gesondert untersucht und überwacht werden. Was eine Person tut, wird weniger wichtig als das, was eventuell nach der Auswertung der von ihr ausgesandten Datenströme

passiert. So können die Metadaten eines Telefonanrufs viel weitreichendere Folgen haben als das eigentliche Gespräch, obwohl dies doch gewöhnlich als Sinn und Zweck eines Telefonanrufs erachtet wird.

Durch digitale Technologien wird das Individuum atomisiert und in Datenströme aufgelöst, die dann in Prozessoren eingespeist werden. Je mehr die direkte Steuerung von materiellen Gegenständen wie Türen, Zäunen und Autos um sich greift, desto mehr verliert der kommunikative Dialog, das Kennzeichen menschlicher Interaktion, an Bedeutung. Diese Beziehungen sind im Kern nicht mehr kommunikativ, sondern strategisch, um eine von Habermas (1987) eingeführte Unterscheidung aufzugreifen. Es ist nicht länger der «zwanglose Zwang des besseren Arguments», der Wirkung entfaltet, auch nicht gutes Zureden oder andere Überzeugungsmittel, sondern es ist allein die Macht der Programme, die Manager und Software-Entwickler meist zeitlich und räumlich fernab der konkreten Umsetzung einzelner Programmregeln entworfen haben (Habermas 2014: 316).

Weitere Beispiele: Software zur Gesichtserkennung erfasst neben dem Gesicht implizit die ganze Person, die damit verbunden ist, und speist die diesbezüglichen Informationen in ein Netzwerk ein, unabhängig davon, ob dies von der Person gewollt ist oder nicht. Es gibt HackerInnen, die behaupten, sie könnten mittlerweile anhand von Fotos Fingerabdrücke identifizieren (Santus 2014), was für die Strafverfolgung ein gewaltiger Fortschritt wäre. Über den Einsatz von Gesundheitsarmbändern und die Sammlung und Auswertung körperspezifischer Daten entstehen ganz neue Bilder des Selbst. Ortungsgeräte ermitteln

georäumliche Koordinaten. Das Cell-All-Programm des US-amerikanischen Ministeriums für Innere Sicherheit ist in der Lage, «tödliche» Chemikalien zu identifizieren. Ein RFID-Lesegerät wiederum interessiert sich nur für den Chip in meiner Geldbörse. Für die biometrische Türverriegelung zählen nur meine Fingerabdrücke oder meine Iris. Die Liste der Instrumente und Programme, mit denen Menschen individualisiert werden, ist inzwischen recht lang. Es handelt sich hierbei um «synekdochische» Identitäten: Ein bestimmter Faktor (welcher, das hängt vom System ab) steht stellvertretend für das Ganze und wird zum Einzigem, was von Bedeutung ist.⁴

Die vielen technischen Systeme, die diesen Prozessen zugrunde liegen und häufig unserem Blick entzogen sind, lassen sich nach Deleuze als «Rhizom» bezeichnen: Wie die Wurzeln und Triebe von sich schnell ausbreitenden und äußerst robusten Pflanzen scheinen sie überall präsent zu sein. Rhizome sind Assemblages von Begriffen, Beziehungen, Materialien und Handlungen. Sie haben keine klaren Grenzen, sie sind fließend, immer aktiv, eine pulsierende Kraft, die mit unterschiedlicher Intensität von verschiedenen Richtungen aus wirksam ist. Der vernetzte, «intelligente» technologische Apparat der Stadt kann gleichzeitig Chemikalien in der Atmosphäre registrieren, sich im Raum bewegende Körper verfolgen, Gesichter von Menschen auf der Straße erkennen und diese überwachen, Polizeikräfte entsenden, um unerwünschte Personen zu entfernen, den Straßenverkehr steuern und vieles mehr. Selbst wenn man diesen sich heraus-

⁴ Synekdochisch bezieht sich auf eine rhetorische Figur, wobei ein Wort durch einen Begriff weiterer oder engerer Bedeutung ersetzt wird (Anm. d. U.).

bildenden rhizomatischen Überwachungs- und Kontrollapparat nur als einen Schwarm unverbundener «dummer» Maschinen sieht, ist diese Vorstellung beängstigend. Niemand will wohl zum Opfer von dessen Algorithmen werden. Je mehr sich technische Netzwerke ausweiten und je mehr miteinander verknüpft wird, desto selbstverständlicher werden sekundäre Formen der Datennutzungen, die vor einigen Jahren, als die «Nutzer» damit begannen, sich in das Internet der Dinge einzubringen, noch unvorstellbar waren (Hoofnagle 2003). Die verschiedenen Sammler und Händler von Daten – seien es Privatfirmen oder staatliche Stellen – werden für die Massen von Informationen immer neue Verwendungen finden. Biometrische Schließsysteme sind nur ein Beispiel. Neben der Protokollierung und Auswertung von Informationen zur Identität der eingelassenen Personen oder zum Zeitpunkt und Ort des Einloggens dürfte für die Behörden noch von größerem Interesse sein, zu erfahren, wem der Zutritt verweigert wurde.

Menschen als Dividuen sind nur frei, solange all ihre «Passwörter» funktionieren: jene Produkte der Dividualisierung, die über Zugang und Ausschluss entscheiden und die es einem erlauben, sich frei durch das rhizomatische System zu bewegen, oder einen davon abhalten. (Du willst durch eine elektronisch verriegelte Tür? Dein PIN ist das Passwort. Du willst etwas kaufen? Deine Kreditkarte ist das Passwort.) Das Leben ist voll von diesen Passwörtern. Aber jederzeit kann eines dieser Passwörter abgelehnt oder für ungültig erklärt werden – zu Recht oder zu Unrecht, mit deinem oder ohne dein Wissen. Und in dem Moment, in dem dies passiert, wird das Ausmaß der Kontrolle,

die diesem Netzwerk zugrunde liegenden Mechanismen über dich ausüben, unübersehbar. Deleuze (1993: 261) entwirft das Bild von einer Stadt, «in der jeder seine Wohnung, seine Straße, sein Viertel nur dank einer elektronischen (dividuellen) Karte verlassen kann, mit der sich bestimmte Schranken öffnen lassen. Genauso denkbar ist es, dass diese Karte nur zu festgelegten Tagen oder Stunden nutzbar ist». Der zunehmende Verfall städtischer Infrastruktur an vielen Orten, zusammen mit der weiteren Ausbreitung der Kletterranken dieses Rhizoms, lässt für immer mehr BewohnerInnen der Stadt ein bedrückendes Szenario mit kafkaesken Zügen entstehen.

Viele technologiekritische Menschen betrachten diese erschreckenden Entwicklungen bei den Kontrollmöglichkeiten als eine Art Frankenstein-Monster oder als Zauberlehrlingsphänomen: Wir haben durch die gedankenlose Einführung bestimmter Technologien etwas entfesselt, was wir nun nicht länger im Griff haben.⁵ Aufgabe von Gesellschaftstheorie sollte es jedoch sein, nach den Ursachen und den verantwortlichen Akteuren zu fragen sowie diejenigen gesellschaftlichen Kräfte zu identifizieren, die Dividualisierungsprozesse vorantreiben und an diesem Kontrollnetz aktiv weben, das die zeitlichen und räumlichen Optionen der städtischen Bevölkerung beschneidet (Krieger 1994). Es mag sein, dass die Mehrheit der Bevölkerung ihrer Dividualisierung zustimmen würde, aber die wenigsten sind dazu in der Lage, die Rahmenbedingungen dafür festzulegen und diese auch durchzusetzen (Rothkopf 2009).

Eine ausführliche Studie zu den Ursachen und zum Kontext der letzten Fi-

⁵ Langdon Winner führt im ersten Kapitel seines Buches «Autonomous Technology» (1977) mehrere Beispiele hierfür an.

nanzkrise (Mirowski 2013) bietet uns einige Anhaltspunkte, wie sich die beschriebenen «Intelligenz-Initiativen» in den Kontext neoliberaler Ideologien und Strategien einordnen lassen: «Den technokratischen Eliten ist es gelungen, die Fiktion aufrechtzuerhalten, «die Menschen» könnten mitentscheiden, während sie längst damit beschäftigt waren, das politische System im neoliberalen Sinn umzubauen. Statt darauf zu warten, dass sich die eher wankelmütige Öffentlichkeit ihren Ansichten anschließt, wurden ziemlich schnell folgenreiche Fakten geschaffen» (ebd.: 77). Bei mehreren Smart-City-Initiativen der jüngeren Vergangenheit spielte die Unterscheidung zwischen Kontrolle und Zustimmung/ Einverständnis eine nicht unwichtige Rolle. Die um sich greifende Vernetzung von Überwachungssensoren und die rechnerische Verarbeitung von Sensordaten, der Aufbau von virtuellen Datenbanken und deren Verknüpfung mit den physikalischen städtischen Strukturen, all das ist viel leichter zu legitimieren, wenn man behaupten kann, die Bevölkerung habe hierzu politisch und individuell ihr «Einverständnis» erklärt. Es gilt jedoch Zweifel an der Gültigkeit und Reichweite dieser Zustimmung anzumelden, wenn diese nur vage oder vermittelt erteilt wurde. So ist bekanntlich die Anerkennung von Nutzungsbedingungen im Internet meist nicht mehr als ein rein formaler und ausgehöhlter Akt der «Zustimmung», der mehr an eine Geste der Unterwerfung und Ergebnislosigkeit erinnert. Wenn man genauer hinschaut, ergibt sich aus den grundlegenden Beziehungsmustern in der «Smart City» ein lückenloses «Spektrum der Kontrolle», bei dem eine Reihe verschiedener Tech-

nologien zum Teil überlappend zum Einsatz kommt, von denen einige ihre Verdienste haben mögen, andere jedoch eher unheimlich und zutiefst beunruhigend sind.

Der Begriff «Spektrum der Kontrolle» ist hier mehr als nur ein rhetorischer Kniff.⁶ Er dient zur symbolischen Visualisierung einer Textinterpretation – der Text ist in diesem Fall die Stadt, verstanden als eine Art ästhetisches Objekt und als Software-Programm. Nach Charles Taylor (1971: 3) stellen Interpretationen, sozialwissenschaftlich betrachtet, den «Versuch» dar, «einen in gewisser Hinsicht verwirrenden, undurchsichtigen, unverständlichen oder scheinbar widersprüchlichen Forschungsgegenstand zu erhehlen und seine Bedeutung zu begreifen». Genauso wie bei Experten für Literatur, Recht und Kunstgeschichte, die mit geschultem Blick Bücher, Gesetze oder Bilder analysieren und deuten, geht es darum, die zunehmend hoch technisierten Governance- und Steuerungssysteme der Stadt als expressive Texte zu betrachten, die einer Interpretation bedürfen.

Sowohl die Rhetorik der «Smart City» als auch die Stadt selbst begreifen wir als Texte oder Textentsprechungen. Angesichts der vielfältigen theoretischen und rhetorischen Anstrengungen, die Spreu vom Weizen zu trennen, den «Zwangsanteil» zu senken und mehr auf «Einverständnis» zu setzen, sind diese Texte inzwischen unklar und verworren. Hinter diesen Bemühungen mögen gute Absichten stecken. Letztlich kann diese normative Agenda jedoch nichts zur Auflösung der Verwirrung und der Widersprüchlichkeit beitragen, weil nämlich mit dem Internet der Dinge und der

⁶ Der Begriff fungiert als das, was Robert Merton (1968: 39) als eine «Theorie mittlerer Reichweite» bezeichnet hat.

allumfassenden Überwachung nicht so sehr eine «smarte» als vielmehr eine «Cyborg-Stadt» entsteht (Gandy 2005). Damit sind urbane Orte gemeint, wo der Zugang zu bestimmten prothetischen Erweiterungen des Selbst immer umkämpfter wird. In solchen «Cyborg-Städten» sind Zustimmung und Zwang, Kontrolle und Autonomie keine Gegensätze – sie sind vielmehr Teil eines Kontinuums. Man wird den Alltagserfahrungen der BewohnerInnen von «Smart Citys» nicht gerecht, wenn man versucht, sie mit solchen binären Kategorien zu erfassen. Denn nur ganz wenige können es sich leisten, auszuscheren und die wirtschaftlichen Zwänge zu ignorieren, die mit dieser «Zukunft, in der alles offengelegt ist» (Peppet 2011: 1 u. 153), einhergehen (vgl. Angwin 2014).

Unser theoretisches Konzept «Spektrum der Kontrolle» ermöglicht es, Zusammenhänge zwischen Technologien zu erkennen, die zuvor als weitgehend voneinander getrennt und unabhängig galten.

Zunehmend kommen harmlose zusammen mit überaus bedenklichen Instrumenten zum Einsatz oder werden miteinander verknüpft. Jede für die «Smart City» zentrale Technologie kann zu einem späteren Zeitpunkt für ganz andere Zwecke, als ursprünglich vorgesehen, umfunktioniert werden. Claude Lévi-Strauss (2010) hat Prozesse des Denkens und der Reflexion mit der Arbeit des Bastlers oder *bricoleurs* verglichen, der versucht, Probleme mit dem ihm zur Verfügung stehenden Werkzeugen oder Materialien möglichst gut zu lösen. Es lässt sich beim Umgang mit Technologien zum Ausbau der «Smart City» ein ähnlicher Prozess der *bricolage* beobachten, wobei diese Technologien zur Lösung ganz verschiedener kleiner und großer Probleme herangezogen werden – und damit auch Einfluss auf den Prozess der Meinungsbildung nehmen, nämlich darauf, was in einem politischen Gemeinwesen überhaupt als kollektiv zu adressierendes Problem definiert wird.

DIE SANFTE GEWALT BIOMETRISCHER ÜBERWACHUNG

An dem einen Ende des Spektrums der Kontrolle finden wir jene zunehmend überall präsenten Technologien, die ihre Macht eher subtil ausüben. Sie sind inzwischen selbstverständlicher Teil des Alltagslebens geworden und werden kaum hinterfragt. Zum einen sind sich viele Menschen gar nicht mehr darüber bewusst, dass sie tagtäglich mit diesen Technologien zu tun haben und mit ihnen interagieren, zum anderen werden sie gezielt verborgen gehalten und unsichtbar gemacht (vgl. Star 1999).

Der politische Philosoph Giorgio Agamben (2010: 77) hat dies als eine besondere Form der Machtausübung beschrieben, bei der es nicht länger darum geht, «direkt zu beeinflussen, was Menschen tun können». Es geht weniger um «ihr Potenzial» als um das, was ihnen nicht zur Verfügung steht, was sie nicht tun können. Das heißt, wir haben es hier nicht mit den üblichen Zwängen zu tun, die mich davon abhalten, mich auf eine bestimmte Art zu verhalten. Das Problem besteht vielmehr darin, dass ich

nicht länger die Möglichkeit habe, bestimmte Dinge *nicht* zu tun. Nehmen wir das Beispiel des Mobiltelefons. Vor etlichen Jahren, als nur wenige Menschen ein Mobiltelefon besaßen, war es noch unproblematisch, selbst keins zu besitzen oder zu nutzen. Heute jedoch, da fast alle Menschen über ein Handy verfügen und das Prinzip der ständigen Kommunikations- und Betriebsbereitschaft einen Großteil unseres Lebens bestimmt, ist es nahezu unmöglich geworden, ohne ein Mobil- oder Smartphone auszukommen (Peppet 2011; Morozov 2014). Ähnliches gilt für die Autonutzung. Niemand wird gezwungen, sich einen Pkw anzuschaffen. Wenn die Verkehrsinfrastruktur einer Gesellschaft aber darauf aufgebaut ist, dass Menschen individuell Fahrzeuge zur Verfügung stehen, und wenn es kaum Alternativen zur privaten Pkw-Nutzung gibt, dann wird es eher schwierig, sich gegen den Kauf eines Autos zu entscheiden.

Die meisten in der Stadt verwendeten Überwachungstechnologien – insbesondere dann, wenn sie als Teil umfassend vernetzter Systeme eingesetzt werden – sind eher am «subtilen Ende» des Spektrums der Kontrolle angesiedelt. Ein Beispiel hierfür sind Überwachungskameras, die inzwischen in fast allen Großstädten der Welt die Straßen säumen und massenhaft in öffentlichen und privaten Gebäuden installiert worden sind. Videoüberwachung hat sich in den meisten Städten mittlerweile zu einer Art «fünfter kommunaler Versorgungsleistung» (neben Gas, Strom, Wasser und Telekommunikation) entwickelt. «Einmal installiert, neigen Videoüberwachungssysteme dazu, sich auszuweiten. Hier spielen Skaleneffekte eine Rolle. Wenn ein Überwachungssystem einmal ein-

gerichtet und dafür Personal eingestellt worden ist, dann ist es allein aus ökonomischen Gründen sinnvoll, das System auf immer größere Gebiete auszudehnen.» (Graham 2002: 238) In der «Smart City» sind solche Überwachungssysteme inzwischen Alltag: Sie sind allgegenwärtig und ständig im Einsatz, werden von den meisten Menschen aber kaum mehr bewusst wahrgenommen.

Bei der Videoüberwachung handelt es sich um eine flexibel einsetzbare Technologie mit dem Potenzial, mehrere Ebenen komplexer Software hinzuzufügen und in die Hardware zu integrieren. Ein Beispiel hierfür sind biometrische Verfahren, die an umfassende, meist von Datenhändlern verwaltete persönliche Informationen gekoppelt sind. Die Ausbreitung von Überwachungssystemen im Zuge von sogenannten Intelligenz-Initiativen, die dann in der Regel durch noch ausgeklügeltere Auswertungstechnologien ergänzt werden, verändert die polit-ökonomischen Rahmenbedingungen dessen, was es bedeutet, in der Stadt zu wohnen.

Schauen wir uns die biometrischen Verfahren einmal genauer an, mit denen ein biologisches Merkmal oder Gruppen solcher Merkmale identifiziert, gemessen und gespeichert werden können. Es gibt derzeit viele verschiedene solcher Verfahren, und ständig kommen neue hinzu. Die gängigsten konzentrieren sich auf Körpereigenschaften, auf Gesichter, Fingerabdrücke, auf die Iris und Netzhaut sowie auf die DNA von Menschen, andere auf Verhaltensmerkmale wie die Stimme, die Unterschrift, den Gang von Menschen oder darauf, wie sie tippen (es wird zum Beispiel der zeitliche Anstand zwischen Tastenanschlägen gemessen). In der Praxis kommt bei biometrischen

Technologien ein standardisierter Prüfprozess zur Anwendung. Mithilfe entsprechender Sensoren werden bestimmte biologische Merkmale und Muster ermittelt, bei Gesichtern mithilfe von Kameras, bei Stimmen mithilfe von Telefonaufzeichnungen. Diese biometrischen Merkmale werden dann unter Anwendung eines Algorithmus in eine digitale Repräsentation übersetzt, die als *template* (Vorlage) bezeichnet wird und in einer Datenbank gespeichert werden kann. Je größer die Datenbank, umso mehr *templates* stehen zur Verfügung, um Personen zu überprüfen oder zu identifizieren. Maßgeblich ist jedoch der Algorithmus, der benutzt wird, um die *templates* zu erstellen. Dieser entscheidet über die Qualität biometrischer Erkennungssysteme. Wichtig dabei sind folgende Kriterien: Wie schnell kann der Algorithmus biometrische Informationen ermitteln? Wie stark ist er dabei von Umweltbedingungen abhängig? Und wie akkurat sind die von ihm gelieferten Vorlagen?

Die Bedeutung, die die Biometrik für die Informationsökonomie hat, ist gewaltig – das gilt insbesondere für den riesigen Wirtschaftszweig des Datenhandels. In einer Senatsanhörung im Jahr 2013 erklärte John D. Rockefeller IV., damals Vorsitzender des Komitees für Handel, Wissenschaft und Transportwesen: «Im Jahr 2012 erzielten die Unternehmen, die mit Daten handeln, einen Umsatz von 156 Milliarden US-Dollar. Das ist mehr als das Doppelte dessen, was den Nachrichtendiensten in den USA an Mitteln zur Verfügung steht. Diese enormen Umsatzsteigerungen resultieren aus den vielfältigen Bemühungen, immer mehr Einzelheiten unseres Privatlebens in Erfahrung zu bringen und dieses Wissen zu verkaufen.»⁷ Die Bio-

metrik bietet neue Möglichkeiten, aus Daten Profit zu schlagen. Man kann sich das wie eine Art Tagebau vorstellen: Aus Menschen, ihren Körpern (und ihrem Verhalten) werden immer mehr Informationen herausgeholt. Mit diesem Vergleich soll hervorgehoben werden, wie welcher Aggressivität und Hartnäckigkeit biometrische Verfahren vorgehen, wenn sie sich auf bestimmte biologische Eigenschaften konzentrieren und versuchen, Informationen hierzu aus dem Gesamtbild, das der Rest des Körpers, der Mensch und sein Umfeld bilden, herauszulösen.

Die mit biometrischen Methoden gewonnenen detaillierten Personendaten sind Gold wert, weil sie es zum einen Unternehmen ermöglichen, ihre Kundenansprache erheblich zu verbessern, und zum anderen staatlichen Behörden die Kontrolle und Steuerung bestimmter Bevölkerungsgruppen erleichtern können. «Trotz der eindeutigen Verbindungen zwischen Maklerunternehmen, die mit Daten handeln, und Kredit-Rating-Agenturen, trotz Umsätzen in Milliardenhöhe, der Aussetzung von staatlichen Vorschriften, um Konsumenten vor Identitätsdiebstahl zu schützen, und trotz zahlreicher nachweisbarer datenrechtlicher Verstöße hat die Durchschnittsbürgerin von diesen mächtigen Konzernen wahrscheinlich noch niemals etwas gehört.» (Roderick 2014: 740) Da die Maklerfirmen mit allen erdenklichen Mitteln Informationen sammeln und Profile er-

⁷ Vgl. zum Protokoll dieser Anhörung (unter der Überschrift «What information do data brokers have on consumers, and how do they use it?») www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=a47c081a-d653-4272-8d12-d6edc1e04dc6&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=12&YearDisplay=2013.

stellen, würden diese (und vor allem ihre Auftraggeber) – wenn sie auch noch auf von biometrischen Algorithmen erzeugte Datenbanken zugreifen könnten – solche Mengen von Daten anhäufen, dass sie über eine Person (deren Einkommen, Schulden, Krankheiten, Vorstrafenregister, Drogenkonsum etc.) bald mehr wüssten als deren engste Angehörigen. Einige Luxusgeschäfte verwenden bereits Softwareprogramme zur Gesichtserkennung, um damit VIPs und Prominente unter den Geschäftskunden auszumachen (vgl. Salinas 2013). Was sollte sie davon abhalten – wenn die Datenbanken erst einmal umfangreich genug sind –, auch alle anderen Kunden zu identifizieren, die zur Tür hereinkommen? Die Ausweitung von Profiling und Programmen zur Personenfeststellung geht auf den Bedeutungszuwachs von auf «Big Data» setzenden Geschäftsstrategien zurück. Führende Unternehmen im Bereich «Big Data» behaupten, ihre Datensammlungen würden das allgemeine ökonomische Gesetz des abnehmenden Ertrags umkehren: Auf je mehr Daten ein Unternehmen zugreifen kann, umso wertvoller ist sein Bestand, erweitert doch die Kontextualisierung von Profilen die bereits bestehenden Möglichkeiten, Menschen zu sortieren und zu klassifizieren, zu kontrollieren und zu diskriminieren (indem etwa unterschiedliche Preise verlangt werden) oder sogar zu bestechen.

Dies hat unter anderem mit der Art und Weise zu tun, wie die Biometrie die Kommodifizierung des Körpers vorantreibt. «Biometrische Methoden zerlegen Körper in ihre Einzelbestandteile und sorgen dafür, dass man diese transnational vermarkten kann. [...] Aus dem verletzbaren Körper wird robustes Körpermaterial, da

mithilfe von biometrischen Technologien der Körper reproduzierbar, übertragbar und teilbar wird.» (Magnet 2011: 12) Von der Datenökonomie war bereits die Rede, aber was ist mit der Gesichts-, der Iris- oder Gangökonomie? Schon jetzt sitzen ganze Unternehmensabteilungen in den Startlöchern und warten darauf, entsprechende Daten abzuschöpfen und auf vielerlei Weise einzusetzen. Datenmaklerfirmen erstellen inzwischen weitreichende Konsumentenprofile anhand biometrischer Vorlagen; Datenverkäufer und Sicherheitsfirmen verwenden biometrisch erzeugte Daten, um die Reputationen von Personen zu rekonstruieren. Mittlerweile ist die Identität eines Menschen auch daran festzumachen, wie er sich durch die Straßen bewegt, an welchen öffentlichen Plätzen er sich aufhält und in welche Geschäfte er geht. Versicherungsfirmen gieren nach körperbezogenen Daten, die zum Gesundheits- und Fitness-Monitoring eingesetzte Geräte liefern (Sadowski 2014a). Der Fantasie, was mit solchem Wissen und der damit einhergehenden Macht noch alles ange stellt werden kann, sind kaum Grenzen gesetzt.

Biometrische Verfahren sind nicht nur ein neues Mittel, um Menschen in kleinste Teile zu zerlegen und damit noch weiter zu individualisieren. Mit ihnen kann darüber hinaus die Kommodifizierung und Kontrolle von Menschen noch weiter intensiviert werden (durch die Auswertung der neu zur Verfügung stehenden Datenquellen beziehungsweise durch ihre verstärkte biopolitische Steuerung). Derzeit werden in den «Smart Citys» eine hierfür geeignete Plattformen aufgebaut.

Die technologischen Systeme, die in den Städten installiert werden, um diese vernetzt, effizienter, sicherer und «in-

telligenter» zu machen, existieren nicht im luftleeren Raum. Sie «repräsentieren und reproduzieren die vorherrschenden kulturellen Werte und die zurzeit dominante politische Ökonomie» (Monahan 2010: 99 f.). Die am «subtilen Ende» des Spektrums der Kontrolle wirkenden Systeme und Technologien bleiben sowohl in funktionaler als auch materieller Hinsicht eher verborgen im Hintergrund. Nur wenige von uns sind sich der aggressiven Überwachungsmethoden bewusst oder wissen überhaupt von der Existenz all dieser Unternehmen, die mit unseren Daten Geld verdienen, und

deren Methoden, mit denen wir Teil der Datenströme des Kapitals werden. Und selbst wenn uns dieses alles bekannt wäre: Die meisten würden sich wahrscheinlich trotzdem damit «einverstanden» erklären, weil die Option, bestimmte Dinge zu unterlassen, damit wir nicht in die Logik dieser Systeme hineingezogen werden – also etwa nicht länger digitale Plattformen oder Smartphones nutzen, nicht unvermummt auf die Straße oder in ein Geschäft gehen, nicht in einem dicht bevölkerten Stadtteil leben – für die überwiegende Mehrheit der BürgerInnen keine realistische ist.

DIE BRUTALE GEWALT VON POLIZEITECHNIKEN

Am anderen Ende des Spektrums gibt es Kontrolltechnologien, mit denen Macht aggressiv und gewalttätig ausgeübt wird. Zurzeit findet, ausgelöst durch technologische Neuerungen und taktisch motivierte Umstrukturierungen, in vielen Städten eine beunruhigende Machtkonzentration bei den Sicherheits- und Strafverfolgungsbehörden statt. Ein Nebeneffekt, der mit der wachsenden Zahl von öffentlichkeitswirksamen sozialen Bewegungen auf der ganzen Welt in den letzten Jahren verbunden war, besteht darin, uns die Spannweite (und Ausweitung) von repressiven Maßnahmen staatlicher Sicherheitskräfte vor Augen geführt zu haben, die sie einsetzen, um Massenproteste auf den Straßen und Plätzen niederzuschlagen. Die Polizei reagiert auf politische Proteste – unabhängig von ihrer Größe oder davon, ob sie friedlich oder gewalttätig sind – immer wieder mit äußerster Härte und in einer zunehmend militarisierten Art und Weise (Balko 2013).

Ein Beispiel: In den USA sind Zusammenstöße zwischen Protestierenden und der Polizei (im Zuge der Occupy-Bewegung, die sich 2011 an Hunderten von Orten formierte, oder im Zusammenhang mit den Mobilisierungen der Black-Lives-Matter-Bewegung nach den umstrittenen Gerichtsurteilen in den Fällen Darren Wilson und Daniel Pantaleo) manchmal innerhalb von Minuten derart eskaliert, dass von herkömmlicher polizeilicher Schutz- und Ordnungsarbeit kaum mehr die Rede sein konnte. Wer die entsprechenden Bilder gesehen hat, denkt eher an den Aufmarsch von (para-)militärischen Truppen, die auf dem urbanen Schlachtfeld gegen Aufständische in den Krieg ziehen (vgl. Graham 2009; Virilio 1989). Normalerweise gelingt es mit wissenschaftlich erprobten Mitteln des Protestmanagements – das auf «nicht-tödliche Waffen» wie Ohrenscherzen verursachende Schallkanonen (LRAD) oder nervenschädigende Kunststoff-

handschellen zurückgreifen kann –, Menschenmengen in kürzester Zeit aufzulösen. Sehr verbreitet sind inzwischen auch sexuelle Belästigungen und Übergriffe. Fühlen sich staatliche Ordnungskräfte beleidigt oder verbal angegriffen, dann nehmen sie dies häufig zum Anlass, um zuzuschlagen und körperliche Gewalt zu rechtfertigen. In der Polizeiarbeit gehören militärisch anmutende Kampfausrüstungen, das Mitführen von Gewehren, Elektroschockern, Reizgas und Hunden, der Einsatz von Wasserwerfern, Tränengas und allen möglichen Überwachungsmethoden sowie Massenverhaftungen vielerorts inzwischen zum Alltagsgeschäft.

Mit Smart-City-Technologien wäre es möglich, das Ausmaß körperlicher Gewalt im Umgang mit Protesten zu reduzieren. Zugleich eignen sich diese aber auch dazu, die Zielgenauigkeit und Wirksamkeit dieser Gewaltmittel zu erhöhen und sie als Abschreckungsmittel zu nutzen, mit dem kollektive Formen der Organisierung und des Handelns nachhaltig geschwächt und bekämpft werden können. Im Januar 2014 hatten DemonstrantInnen in Kiew eine ominöse Nachricht auf ihren Mobiltelefonen: «Sehr geehrter Leser, Sie sind als Teilnehmer eines Massenaufstands registriert.» Eine derartige Beschuldigung kann einen in der Ukraine aufgrund der jüngsten Verschärfung des Versammlungsrechts schnell einmal für 15 Jahre ins Gefängnis bringen (Walker/Grytsenko 2014). Solche Taktiken sind Teil einer polizeilichen und sicherheitspolitischen Entwicklung, bei der versucht wird, Massenproteste und Demonstrationen mithilfe allein von technischen Mitteln aufzulösen oder am besten erst gar nicht stattfinden zu lassen. Die psychologischen Auswirkungen solcher Maß-

nahmen sind nicht zu unterschätzen, sie reichen weit über den unmittelbaren Anlass hinaus. Allein das Wissen, dass man auch noch Tage und Wochen nach der Beteiligung an einer Protestaktion dank Fernregistrierung durch Polizei oder des Ministeriums für Heimatschutz verhaftet werden kann – ob nun daheim oder auf der Arbeit –, genügt, um Menschen einzuschüchtern und die Reihen der AktivistInnen zu lichten. Dieses Gefühl des völligen Ausgeliefertseins kann auch (wie in der Ukraine geschehen) dazu führen, dass die Menschen tatsächlich revoltieren und die Systemfrage stellen, was für den Fall, dass das alte Regime an der Macht bleibt, schlimmste Kollektivbestrafungen nach sich ziehen kann. So oder so: Der Einsatz wird für alle Beteiligten immer höher.

Paul Virilio hat in seinen Ausführungen zum Ausnahmezustand davor gewarnt, dass die schnelle Befriedung von Konflikten zu einer Art Wettrüsten führen kann, bei dem das Ausmaß der Bedrohungen kontinuierlich gesteigert wird. Die «Verkürzung der Vorwarnzeit, die sich aus der Überschallgeschwindigkeit des Angriffs ergibt», würde «so wenig Zeit für Aufklärungs- und Identifizierungsmaßnahmen und wohlüberlegte Reaktion lassen, dass bei einem Überraschungsangriff der Oberbefehlshaber seine Entscheidungshoheit an die unteren Ränge des Verteidigungssystems abgeben und diese dazu autorisieren müsste, sofort Anti-Raketen-Systeme in Gang zu setzen» (Virilio 2009: 204). Ähnliches kann man sich auch für Konfliktsituationen in «Smart Cities» vorstellen, wenn gängige Maßnahmen zur Auflösung von Menschenmengen in der Öffentlichkeit nicht mehr greifen, weil sich DemonstrantInnen zum Beispiel wirksam darauf vorbereitet haben. Was

läge näher aus Sicht der Machthabenden, für solche Fälle algorithmische Abschreckungsmethoden in Verkehrs- und Polizeisysteme zu integrieren? Das könnte unter unzufriedenen BürgerInnen eine gefährliche Dynamik erzeugen: Einige würden vielleicht dazu gebracht, einfach aufzugeben. Anderen könnten aber (wie die Erfahrungen aus der Ukraine zeigen) zu dem Entschluss gelangen, dass man den König nur mit einem tödlichen Schlag loswerden kann. Wenn politische Systeme selbst mit friedfertigen Dissidenten derart bösartig umspringen, dann erscheinen Umsturzgedanken nicht mehr abwegig. Der politische Raum für demokratische Aushandlungsprozesse und kollektives Handeln würde zwischen den Polen Unterwerfung und Revolution Schritt für Schritt zerstört werden.

Gegenwärtig ist es so, dass Technologien «intelligenter» Massenkontrolle eher auf gesellschaftliche Zustimmung stoßen. So bietet das Unternehmen Persistent Surveillance Systems der Polizei in den USA schon seit Längerem seine Dienste an. Zurzeit wird ein Verfahren getestet, bei dem die Sicherheitsbehörden mithilfe eines Zivilflugzeugs ein umfassendes Überwachungsnetz über die Stadt legen können (Friedersdorf 2014). Die Firmenleitung vergleicht dieses Verfahren mit einer «Live-Version von Google Earth, allerdings mit TiVo-Qualitäten» (Campbell-Dollaghan 2014).⁸ Die Technologie erlaubt es der Polizei, Luftaufnahmen der Stadt anzufertigen, diese zu vergrößern und miteinander zu verbinden, womit Bewegungen bestimmter Fahrzeuge und Personen innerhalb der Stadt sehr präzise verfolgt werden können. Für alles, was mit *crowd control* zu tun hat, wäre dieses in Echtzeit arbeitende «Himmelsauge» ein gewaltiger Zugewinn. Dass Überwa-

chungs- und Strafverfolgungsmethoden immer ausgefeilter und expansiver werden, ist weder überraschend noch neu. Sie ergänzen und perfektionieren nur die bereits im Einsatz befindlichen Programme und Technologien.

Großflächig vernetzte Überwachungssysteme sind eine solide Grundlage, um die nächsten Schritte in Richtung einer weiteren Automatisierung der Polizeiarbeit zu planen. Eine Gruppe von Wissenschaftlern – von denen viele an der US-Militärakademie in West Point beschäftigt sind – warnte vor Kurzem in einem Beitrag vor dem technologischen Wandel, den klassische Polizeimethoden, die üblicherweise auf dem Einsatz einer großen Zahl von Beamten beruhen, zurzeit durchlaufen würden (Shay u. a. i.E.). Mit der zunehmenden Delegation polizeilicher Aufgaben an technische Systeme – Algorithmenanalysen, Robotik, Breitbandsensoren etc. – würden demokratische Grundrechte, wie Dissens und Protest zu äußern, beschnitten. Die Möglichkeiten und Spielräume oppositioneller Aktivitäten würden weiter eingeschränkt. Diese «automatisierten Systeme sind in dieser Hinsicht sehr effektiv, erleichtern eine minutiöse und unermüdliche Strafverfolgung und überzeugen auch noch mit finanziellen Vorteilen» (ebd.: 4; McCoy 2009).

Ein weiteres Beispiel für automatisierte Polizeiarbeit ist der Einsatz von Drohnen und Robotern zur Kontrolle von größeren Menschenmengen und Protesten, der nicht mehr lange auf sich warten lassen dürfte. Die südafrikanische Firma Desert

⁸ TiVO ist die Abkürzung für Television Input / Video Output. In den USA ist es mittlerweile zum Synonym für digitale Videorecorder geworden. Der Marktführer geht dort jetzt noch einen Schritt weiter und kombiniert den Festplatten-Recorder mit Podcasts, Videoblogs und anderen Internet-Angeboten (Anm. d. Ü.).

Wolf hat beispielsweise eine Aufstands-bekämpfungsdrohne entwickelt, die sie *skunk* (Stinktief) getauft hat und die mit einem ganzen Arsenal an «nicht tödlichen» Waffen ausgestattet ist. Neben Stroboskoplichtern, Kameras und Lautsprechern verfügt das «Stinktief» auch noch über vier Paintballgewehre, die sich mit «Farb-, Reizgas- oder Hartplastikgeschossen» laden lassen, um «Menschenmengen aufzulösen oder Einzelne in der Menge zu markieren» (Doctorow 2014). Der erste Abnehmer des «Stinktiefs» wird wohl die Bergbauindustrie sein, um damit gegen Streikende vorzugehen, es bietet sich jedoch an, solche Drohnen auch bei städtischen Protesten einzusetzen. Die Logik ist schließlich in beiden Fällen dieselbe: Es geht darum, all diejenigen zu bändigen und einzuschüchtern, die die herrschenden Macht- und Kapitalverhältnisse stören und verändern wollen. Schließlich erlauben Mittel wie das «Stinktief» der Polizei, noch wirksamer, flexibler und ohne direkten menschlichen Kontakt (was für sie weniger anstrengend und sicherer ist) mit der Artikulation von Dissens umzugehen. Der gezielte Einsatz von Robotern und Drohnen könnte daher bald zu einem festen Bestandteil des Lebens in «Smart Citys» werden. Die Ideologie, die dahinter steckt, ist: Alle Störungen des städtischen Systems sind mit technologischen Lösungen und Instrumenten zu beheben – wobei es eher unerheblich ist, ob sie sich nun gegen Protestierende oder gegen Drogenhändler richten. Und die Reichweite «gewaltloser» Polizeitaktiken wird immer größer. Bald könnte mit technologischen Mitteln die Bildung von größeren Menschenansammlungen von vornherein verhindert werden. Es findet also ein Übergang statt

weg von reaktiven hin zu präventiven Polizeimethoden. In San Francisco hat man vonseiten der Sicherheitskräfte sowohl Zugfahrpläne manipuliert als auch den Zugang zum Internet eingeschränkt, um Menschen davon abzuhalten, an Demonstrationen teilzunehmen. In New York war es ähnlich: Dort hat die für den U-Bahn-Verkehr in New York zuständige Metropolitan Transportation Authority dafür gesorgt, dass Züge nicht an Stationen, in deren Nähe Protestaktionen stattfanden, hielten. Auf diese Weise wurden die Menschen an ihrem Versammlungs- und Demonstrationsrecht gehindert. Die Fähigkeit der Polizei, große Gebiete zu überwachen, aus der Distanz heraus Abschreckungstaktiken anzuwenden, die Strafverfolgung über Automatisierungen zu verschärfen, sowie die Einführung von sogenannten prädiktiven Praxen sollen die Gesellschaft sicherer und geordneter machen.⁹ In dem Maße, wie solche Maßnahmen jedoch dazu genutzt werden, um legitimen Protest und Dissens zu unterbinden, desto mehr verändern sich unsere Gesellschaften hin zu immer mechanisierteren, unorganischen Entitäten, in denen Überwachung hauptsächlich dazu dient, bestimmte Machtverhältnisse zu stützen und auf Dauer zu stellen. Das Staatswesen durchläuft eine grundlegende Transformation und entpuppt sich als eine vollkommen andere Form der gesellschaftlichen Organisation: Es wird zu einer Leviathan-Maschine. Eine Folge sind Gefühle der Entfremdung und des Ausgeliefertseins, die sich gegenseitig verstärken. Es entsteht mate-

⁹ In einem Beitrag in der Zeitschrift *The Police Chief* (Beck/McCue 2009), mitverfasst vom obersten Kriminalbeamten des Los Angeles Police Department, der zugleich Vorstandsvorsitzender einer Beratungsfirma für Sicherheitsfragen ist, wird folgende Frage gestellt: «Was können wir von Wal-Mart und Amazon für die Verbrechensbekämpfung während einer Rezession lernen?» Offenbar ziemlich viel.

riell und politisch eine neue Unterklasse. Die BewohnerInnen der «Smart City» werden tendenziell zu Untertanen, die man dazu antreibt, möglichst produktiv tätig zu sein (mal mehr, mal weniger direkt und repressiv), und denen man kaum mehr die Zeit dazu lässt, ihre eigenen Möglichkeiten oder Wünsche zu überdenken und zu hinterfragen. Immer dann, wenn Big Data als Mittel zum besseren Verständnis und zur besseren Kontrolle der Gesellschaft angepriesen wird, ohne dabei ausreichend auf die Umstände (oder die Denkweisen), die diese Daten hervorgebracht haben, einzugehen, dann ist Vorsicht geboten. Nicht selten werden diese Daten nämlich missbraucht, um ungerechte Entscheidungen oder Maßnahmen zur Disziplinierung und Ausbeutung von Menschen zu rechtfertigen. Beispielsweise kann ein Kreditinstitut einfach hingehen und beschließen: «Wir verlangen 15 Prozent Zinsen von jemandem, der in der Vergangenheit einer Zahlungsverpflichtung nicht nachgekommen ist, und zwar deswegen, weil ein Ergebnis von Datenauswertungen ist, dass es bei solchen Kreditnehmern auch in Zukunft höchstwahrscheinlich wieder zu Zahlungsrückständen kommen wird.» Dabei zeigt sich die Bank völlig gleichgültig gegenüber den konkreten Gründen für die Zahlungsprobleme. Ähnlich könnte die Polizei sagen: «Wir erhöhen in einem bestimmten Stadtteil die Polizeipräsenz, weil hier die Kriminalitätsrate schon länger 10 Prozent über der in anderen Vierteln liegt.» Was ist jedoch, wenn die Zahlungsausfälle eines Kreditnehmers mit persönlichen Schicksalsschlägen oder gar mit übermäßigen Zinsforderungen zusammenhängen, die wiederum Ergebnis diskriminierender Kreditvergabepraktiken waren? Und was ist, wenn die über-

durchschnittlich hohe Kriminalitätsrate in einem Stadtteil Resultat besonderer polizeilicher Aufmerksamkeit und diese wiederum Ausdruck polizeilichen Rassismus ist? Was ist, wenn mit jeder dieser Entscheidungen in Zukunft Zahlungsausfälle oder Straftaten nicht verhindert, sondern eher befördert werden? Dann verwandelt sich die von Big Data versprochene «Wissenschaft zur Regulierung der Gesellschaft» in ein System der Unterdrückung bestimmter sozialer Gruppen. Die solchen Entscheidungen zugrunde liegenden Algorithmen sind dann weit davon entfernt, «objektive Schiedsrichter» zu sein, die sachlich angemessen über Vorteile und Strafen entscheiden. Vielmehr werden sie als Mittel genutzt, subjektive und voreingenommene Entscheidungen und Bewertungen als objektiv und fair darzustellen. Die Betroffenen verlieren zudem das Recht darauf, dass ihr Fall individuell geprüft wird, denn technische Systeme behandeln Menschen nicht als Individuen und Rechtsträger, sondern lediglich als Sammlungen von Datenpunkten.

Stephen Graham (2011) hat in einem Interview in der Radiosendung «Democracy now!» die These vertreten, Städte seien der «räumliche Unterbau der Demokratie». Sie seien die Bühne für öffentliche Auseinandersetzungen und Proteste, die grundlegende gesellschaftliche Konflikte und Herausforderungen thematisieren. Mit der Umwandlung des städtischen Raums in hoch technologisierte Sicherheitszonen werde die Ansicht gestärkt, alles, was nicht den gesellschaftlichen Status quo akzeptiert, habe dort nichts zu suchen und müsse daher eingedämmt oder aufgehalten werden. In seinem Buch «Cities Under Siege» warnt Graham (2011: 121) vor zunehmenden Angriffen auf demokratische Rechte. Er

schreibt: «Immer häufiger werden auf der Straße Protestierende von Kordons militärisch auftretender Polizeikräfte gewaltsam vom Demonstrieren abgehalten oder an Orte abgedrängt, wo ihre politischen Botschaften und Forderungen kein Gehör finden, weil sie dort kaum Zugang zur Öffentlichkeit und zu den Medien haben. Dabei greifen die Sicherheitsbehörden besonders gern auf Methoden wie präventive Festnahmen und die Einrichtung von Sperrzonen zurück.» Mit anderen Worten: Protestierende, Whistleblower, politische AktivistInnen und Fürsprecher der Armen und Benachteiligten werden nicht als integrale Bestandteile einer gut funktionierenden Gesellschaft geschätzt. Diese Haltung ist auch deswegen so problematisch, weil man damit nicht zur Kenntnis nimmt, warum diese eigentlich auf die Straße gehen, und auch nicht darüber nachdenkt, wie die Missstände, die Protestierende in der Regel zu Recht anklagen, behoben werden könnten. Es gibt keinen direkten kausalen Zusammenhang zwischen den beschriebenen Trends bei den Polizeimethoden und

-technologien und der «Smart City». Sie kommen nämlich auch an solchen Orten zum Einsatz, die von «Intelligenz-Initiativen» bisher verschont geblieben sind. Vielmehr dient das Smart-City-Konzept als eine Art Türöffner, das genutzt werden kann, um solche Strategien schneller auszubauen und dauerhaft zu etablieren. Wenn städtische Infrastrukturen mit Überwachungsnetzwerken, Sensoren und Algorithmen ausgestattet werden, erweitert das die Fähigkeit der Polizei, städtische Räume zu überwachen und aktiv einzuschreiten. Diese Formen der sekundären Datennutzung gehen weit über das hinaus, wozu die BürgerInnen vielleicht einmal ihre «Zustimmung» gegeben haben mögen. Und was noch wichtiger ist: Sie drohen eine Entwicklung zu beschleunigen, bei der immer mehr Phänomene als Störungen der öffentlichen Ordnung wahrgenommen werden. Einsprüche gegen diesen fortschreitenden Ausgrenzungsprozess und eine weitere Militarisierung der Polizeiarbeit werden es in Zukunft noch schwerer haben, gehört zu werden.

CYBORG-URBANISIERUNG UND VERSCHWOMMENE GRENZEN

Die Wirksamkeit dieser auf beiden Seiten des Spektrums der Kontrolle angesiedelten Technologien wird noch dadurch gesteigert, dass heute stärker als wohl jemals zuvor die Grenzen zwischen Körper, Stadt und Technologie tendenziell verschwimmen. Personen, Gebäude und Geräte sind nicht mehr immer klar voneinander zu unterscheidende eigenständige Entitäten, sondern Assemblages, bestehend aus Fleisch, Beton und Infor-

mationen. Diese Verbindungen spielen den Mächtigen in die Hände, da sie die rhizomatischen Verflechtungen nutzen können, um ihre Kontrollapparate zu modernisieren und besser zu steuern. Die moderne Stadt lässt sich daher am sinnvollsten mit dem Begriff der «Cyborg-Urbanisierung» erfassen. Die BewohnerInnen sind am besten als urbane Cyborgs zu denken, die nicht in der Stadt leben, sondern *als Teil davon*. Der Geograf

Matthew Gandy (2005: 28) formulierte es folgendermaßen:

«Der Verweis des Cyborgs auf die materielle Schnittstelle zwischen dem Körper und der Stadt wird vielleicht in der materiellen Infrastruktur am deutlichsten, die den menschlichen Körper mit riesigen technologischen Netzwerken verbindet. Wenn wir den Cyborg als kybernetische Schöpfung begreifen, als hybride Kombination von Maschine und Organismus, dann erscheinen städtische Infrastrukturen als eine Reihe wechselseitig verbundener Systeme zur Lebenserhaltung.»¹⁰

Mit städtischer Infrastruktur werden menschliche Bedürfnisse befriedigt: nach fließend Wasser, klimatisch angenehmer Umgebung, Lebensmittelversorgung, Mobilität und Transportmöglichkeiten, Orten des geselligen Beisammenseins. Störungen infolge von Naturkatastrophen wie etwa Hurrikan Sandy erinnern uns daran, wie fragil diese Infrastruktursysteme sein können und wie sehr wir auf sie angewiesen sind. Wir sollten daher nicht nur darüber nachdenken, welche Rolle die bauliche Architektur in Städten einnimmt, wie sie den BewohnerInnen Orientierung oder Schutz bieten kann, sondern auch darüber, welche Rolle bestimmte Software-Architekturen haben sowohl für die Regierung von urbanen Räumen als auch für das Zusammenleben der Menschen, die dort wohnen.

Je mehr Menschen zu urbanen Cyborgs werden, zu Körpern, die mit den Städten verschmelzen, desto komplizierter werden unsere Schnittstellen mit dem System. In libertären Cyborg-Visionen ist der Mensch eine Art Insel: Dem Über-Roboter, der mit einem Außenskelett gepanzert ist und dessen Körpertemperatur und Blutzucker automatisch re-

guliert werden, fehlt es an nichts, und er fürchtet auch nichts. Die individuelle Gesundheit ist jedoch abhängig von der Gesundheit des soziotechnischen Kollektivs. Und der Übergang von analogen zu digitalen Infrastrukturen hat diesen Zusammenhang nur noch weiter vertieft. Derartige Technologien existieren überall und sind nicht mehr zurückzudrängen. Der Schlüsselbegriff ist der der «natürlichen Nutzerschnittstelle», die auf eine reibungslose Interaktion abzielt. Sie heißt eine kybernetische Existenz ohne kinetische Störungen. Das Leben des urbanen Cyborgs wird von diesen Technologien auf verschiedene Weisen – manche davon offensichtlich, andere eher im Hintergrund wirkend – vermittelt und strukturiert.

In ihrem «Cyborg-Manifest» hat Donna Haraway (1991: 163) darauf hingewiesen: «Kein Gegenstand, Raum oder Körper ist an und für sich heilig. Jede Komponente kann mit jeder anderen verbunden werden, wenn sich das richtige Protokoll, der richtige Code konstruieren lässt, der Signale in einer gemeinsamen Sprache verarbeitet.» Haraway ging es hier unter anderem darum, die entscheidenden «Übergänge weg von den bequemen alten hierarchischen Herrschaftsformen hin zu den neuen unheimlichen Netzwerken» zu kartografieren, was sie als «Informatik der Herrschaft» bezeichnet hat. Ähnlich hat es Deleuze (1993: 250 f.) formuliert: «Wir treten ein in Kontrollgesellschaften, die nicht mehr durch Internierung funktionieren, sondern durch unablässige Kontrolle und unmittelbare Kommunikation.» Für ihn hatte dieser Übergang seine Entsprechung in der «Kybernetik und in Computern», wir müssten, so Deleuze, jedoch auch erkennen, dass «die Maschinen [nichts] er-

klären [...] Man muss die kollektiven Arrangements analysieren, von denen die Maschinen nur ein Teil sind.» Deleuzes und Haraways Thesen verweisen auf eine bestimmte technopolitische Logik von Cyborg-Städten, die bedrohlicher – potenziell aber auch emanzipatorischer – ist als der nichtssagende und technokratische melioristische Ansatz, der hinter der Smart-City-Idee steckt. Der Gehalt der Cyborg-Metapher verändert sich, sobald es uns gelingt, uns als Teil einer Cyborg-Stadt zu begreifen, zugleich als Gesamtheit und Teil eines Ganzen – nicht nur als Wesen, die mit rhizomatischen urbanen Assemblages interagieren, sondern als Wesen, die Teil von diesen sind. Der «politische Körper» erhält dadurch eine ganz neue Bedeutung.

Die «Cyborgifizierung» städtischen Lebens wirft kritische Fragen auf und berührt mehrere miteinander verknüpfte existenzielle und soziale Probleme. Das computergestützte System des Belohnens und Strafens, das System sozialer Wohlfahrt und Polizeiarbeit, basiert auf einer Reihe von Beschlüssen: Soll ein bestimmtes (In-)Dividuum überwacht werden, oder soll ihm geholfen werden, indem Angebote unterbreitet werden? Soll etwas in das (In-)Dividuum investiert werden, oder wird es als Objekt betrachtet, das ausgebeutet und ausgepresst werden kann? Für die BewohnerInnen der Städte wird es nun existenziell, zu entscheiden, ob sie um Investitionen konkurrieren oder ob sie bestehende Machtstrukturen hinterfragen wollen, oder ob sie sich einfach treiben lassen wollen, ausgeliefert den Beschlüssen derjenigen, die die Verhältnisse schaffen, die andere zu ertragen haben.

Je mehr sich unser Leben in «codierten Räumen» abspielt, in Räumen, die um di-

gital eingeschriebene Informationen erweitert sind, aber auch in Räumen, die so stark von Informationen geprägt sind, dass diese zu einer notwendigen Komponente ihres Funktionierens werden, desto allgegenwärtiger und unausweichlicher wird die Macht computergestützter Prozesse (Kitchin/Dodge 2011). Der Begriff «Code» kann sich im Englischen auf einen Gesetzestext (wie im Fall der US-Abgabenordnung, dem Internal Revenue Code) oder auf eine Software beziehen (bei der eine «Codierung» von Anweisungen in einem maschinenlesbaren Format stattfindet) (Lessig 1999), er weist aber auch auf ein vorsätzliches Verbergen der Bedeutung hin. Jemand sendet deswegen eine «codierte» Nachricht, weil er oder sie nicht erkannt werden will oder weil Dritte nicht verstehen sollen, was sich gerade abspielt. Im algorithmischen Entscheidungsprozess dominiert häufig dieser dritte mysteriöse Aspekt der Codierung. Bei der Kreditvergabe etwa spielen sehr viele vage oder sogar widersprüchliche Codes eine Rolle, mit denen sich im Prinzip jede Bewertung der Kreditwürdigkeit rechtfertigen lässt. Vielleicht wird Ihnen zum Verhängnis, dass Sie zu viele Konten haben, vielleicht aber auch, dass Sie zu wenige haben. Beides kann jederzeit dazu führen, dass Ihre Kreditwürdigkeit herabgestuft oder der von Ihnen beantragte Kredit abgelehnt wird. Es bleibt im Dunkeln, wer die Entscheidungen über den Zugang zu Krediten und andere Ressourcen trifft, über das Recht, sich frei bewegen zu können, und über viele andere Dinge – und wahrscheinlich müsste man besser fragen, nicht *wer* diese Entscheidungen trifft, sondern *was* diesen zugrunde liegt.

Angesichts der vielen Versprechen und hoffnungsvollen Visionen, die mit «Smart

Citys» verknüpft sind, verwundert es nicht, dass dabei die politischen Inhalte und Vorgaben häufig aus den Augen verloren werden, die in die miteinander verbundenen Technologien und Initiativen wie ein Code eingeschrieben sind. Wenn wir die zu beobachtenden urbanen Transformationen lediglich als neutrale Verbesserungen auffassen, die mehr Effizienz und Sicherheit bringen,

dann übersehen wir dabei die sozialpolitischen und sogar ontologischen Aspekte dessen, was es bedeutet, in diese rhizomatischen Mechanismen eingewoben zu sein, was es bedeutet, ein assimilierter Teil der Cyborg-Stadt und ihrer Funktionsweise zu sein und immer mehr von algorithmischen Entscheidungen sowie einer technologisch erweiterten Gewalt kontrolliert zu werden.

DIE ZURÜCKEROBERUNG DER KONTROLLE

Der hier vorlegte politische Analyse der «Smart City» und unsere Neuinterpretation ihrer sozialtechnischen Assemblages als Cyborg-Stadt haben für uns auch einen normativen Gehalt. Unser Konzept des «Spektrums der Kontrolle» bringt uns dazu, das Prinzip des «Rechts auf Stadt» zu propagieren und zu unterstützen. Dieses Recht wurde zuerst von Henri Lefebvre formuliert, als ein Mittel, mit dem sich die Menschen den städtischen Raum zurückerobern sollten, indem sie die vom Kapital zu verantwortenden Missstände hinterfragen genauso wie die Pflichten und Rechte, die mit dem Status des Staatsbürgers einhergehen (vgl. Purcell 2002). Im Kontext der globalen Ausbreitung neoliberaler und technokratischer Ideologien kommt einem solchen Recht eine wichtige neue Bedeutung zu: Es dient als machtvolle Parole, mit der wir uns gegen die sich ständig weiter ausbreitenden und uns in Beschlag nehmenden Kontrolltechnologien zur Wehr setzen können. David Harvey (2008: 23) erklärt in seinem einschlägigen Essay zum «Recht auf Stadt», worum es bei diesem Recht geht:

«Die Frage danach, welche Art von Stadt wir wünschen, ist nicht zu trennen von der, welche sozialen Beziehungen, welches Verhältnis zur Natur, welche Lebensstile, Technologien und ästhetischen Werte wir wünschen. Das Recht auf Stadt ist weitaus mehr als die individuelle Freiheit, Zugang zu städtischen Ressourcen zu haben: Es ist das Recht, uns selbst zu verändern, indem wir die Stadt verändern. Es handelt sich darüber hinaus um ein gemeinsames, und nicht etwa um ein individuelles Recht, da der Wandel unweigerlich von der Ausübung eines kollektiven Vermögens zur Umgestaltung der Urbanisierungsprozesse abhängt. Die Freiheit, unsere Städte und uns selbst zu schaffen und neu zu schaffen ist [...] eines unserer kostbarsten und zugleich auch eines unserer am meisten vernachlässigten Menschenrechte.»

Selbst wenn dies wichtige Schritte in die richtige Richtung wären, ist mit dem «Recht auf Stadt» nicht einfach nur die Einführung eines *living wage* oder eines Grundeinkommens für alle EinwohnerInnen der «Smart City» gemeint. In einem Umfeld, in dem die wirtschaftlichen und

politischen Eliten immer neue und immer raffiniertere Beobachtungs-, Kontroll- und Manipulationsinstrumente entwickeln (Unger 2004), muss der Kampf um das «Recht auf Stadt» auch ein Kampf um die Verteidigung von Freiheitsrechten sein, wenn diese weiterhin eine Bedeutung haben sollen.

Julie Cohen (2012) hat in ihrem Buch dargestellt, wie wir auf die Ausbreitung «intelligenter» Technologien und Netzwerke reagieren sollten. Sie lehnt explizit die Logik von Big Data ab, nach der ein Mehr an Daten immer von Vorteil ist. Stattdessen setzt sie auf eine «semantische Diskontinuität» zwischen verschiedenen Systemen zur Erfassung und Kategorisierung von Wissen und fordert, Bestrebungen nach vollständiger Interfunktionsfähigkeit und Lesbarkeit sowie nach dem unbeschränkten Zugriff auf verschiedene Datensysteme infrage zu stellen und notfalls auch zu durchkreuzen.

Bereits heute sind wir mit den negativen Folgen einer ungebremsen Datenvernetzung konfrontiert. So hat in den USA die vertikale Integration der Daten von kommunalen, einzel- und nationalstaatlichen Strafverfolgungsbehörden in Verbindung mit der horizontalen Verknüpfung von nachrichtendienstlichen Systemen und Ermittlungseinheiten des Militärs und der Polizei bereits zu einer Reihe von Pannen und Bürgerrechtsverletzungen geführt, ohne dass sich im Gegenzug die öffentliche Sicherheitslage für die meisten Menschen erkennbar verbessert hätte (Citron/Pasquale 2011). In Großbritannien sind Versuche, Gesundheitsdaten zusammenzuführen, aus dem Ruder gelaufen und haben zu erheblicher Aufregung geführt, als herauskam, dass die Gesundheitsämter planten, diese Daten an Versicherungsfirmen zu verkaufen. Es gibt noch

viele weitere abschreckende Beispiele, die die BefürworterInnen von Smart-City-Konzepten nachdenklich stimmen sollten. Ohne eine stetige Konsultation und Abstimmung mit den Bevölkerung und ohne die Androhung schwerer Strafen für das Vergehen des Datenmissbrauchs könnte der anvisierte omnipräsente Überwachungsapparat am Ende mehr schaden als nützen.

Die Legitimität der «Smart City» hängt aber auch von deren «Objektivität» ab. Das heute bereits existierende Kontrollsystem weist seltsame Lücken auf. Aus irgendeinem Grund werden Wirtschaftskriminelle kaum überwacht oder ganz selten bestraft. Dagegen wird Otto-Normal-Verdiener durch den rhizomatischen Apparat zunehmend dividualisiert, weil sich ein Dividuum besser analysieren, durchdringen und kontrollieren lässt. Wie Johnathan Crary (2014) in seinem Buch «24/7: Schlaflos im Kapitalismus» aufgezeigt hat, ist die militärische Logik, dauernd wachsam sein zu müssen, inzwischen auch in den kapitalistischen Alltag eingedrungen und beeinflusst Annahmen über Erwerbstätigkeit und existenzsichernde Löhne. Sollte sich herausstellen, dass «Intelligenz-Initiativen» städtischen Regierungen lediglich die technokratische Rechtfertigung dafür bieten, sich vermeintlichen ökonomischen Zwängen zu unterwerfen und unternehmerische Formen der urbanen Governance einzuführen oder weiter zu stärken (Harvey 1989), dann verdienen sie entsprechenden Widerstand. Und vieles spricht dafür, dass es so ist. Manche vermuten, dass es sich bei den Sensoren der «Smart City» um nichts anderes als «politisch-technologische Instrumente handelt, mit denen vor allem neue Anlage- und Zirkulationsmöglichkeiten für das

Kapital geschaffen und legitimiert werden sollen» (Vanolo 2014: 884). Damit wären sie nichts anderes als die Wiedereinführung altbekannter Ketten in Gestalt von modernen Technologien.

Es gibt eine Reihe von Hinweisen, dass wir es gegenwärtig mit der Wiederbelebung frühkapitalistischer Akkordarbeit in Form einer «Gig-Wirtschaft» zu tun haben. Wir sollten auch endlich anerkennen, dass es sich bei der Sklaverei nicht um eine Abweichung von kapitalistischen Imperativen handelt(e), sondern vielmehr um eine bestimmte Variante der Ausbeutung von Arbeitskraft, auf die aggressive Führungskräfte aus Staat und Wirtschaft jederzeit zurückgreifen können, wenn sie noch mehr aus den Menschen herauspressen wollen (Baptist 2014). Cory Doctorow (2015) hat es ein wenig provokativ folgendermaßen auf den Punkt gebracht:

«Unsere Netzwerke haben den Eliten einen enormen Informationsvorsprung verschafft, und solange wir den nicht einholen, steuern wird auf ein durch Informations- und Kommunikationstechnologien angetriebenes langes Zeitalter des Feudalismus zu, in dem Eigentum das Vorrecht der Superreichen ist und in dem das mit Überwachungssystemen überfrachtete Internet der Dinge dich wie einen armen Schlucker und Pachtbauern behandelt, dessen Rechte nicht von der Verfassung, sondern einem Lizenzvertrag bestimmt werden.»

Es sollte eines unserer maßgeblichen Ziele sein, zu einer gerechteren Verteilung des Wertes zu kommen, der aus den neuen massiven Datenströmen erwächst. Die Arbeit, die darin besteht, beobachtet zu werden (Andrejevic 2004), wird nicht angemessen vergütet (Scholz 2013). Sich im städtischen Netzwerk als

menschliche Informationsknotenpunkte zu gerieren wird zu einer weiteren bürgerschaftlichen und aus wirtschaftlichen Gründen gebotenen Pflicht, die Smart-City-BewohnerInnen zu erfüllen haben. Jennifer Gabrys schreibt dazu: «Die Überwachung und Verwaltung von Daten, die dann in städtische Informationssysteme eingespeist werden, wird mehr und mehr für den Bürgerstatus konstitutiv. Aus Bürgerrechten wird die Erkundung von anderen Bürgern. Diese drückt sich zunehmend in Praktiken aus, die auf informatikgestützte Umfelder und Technologien reagieren (und mit diesen kommunizieren).» (Swarts 2013: 16 f.) Da immer mehr Unternehmen mit solchen Daten wirtschaftliche Profite erzielen, müssen unbedingt Vorkehrungen zu einem gerechteren Vorteilsausgleich getroffen werden (Lanier 2011). Sonst werden zu Dividuen degradierte Menschen lediglich die Macht anderer vermehren, die die rhizomatischen Verbindungen ausbeuten, indem sie den Datenfluss in den Netzwerken stetig steigern.

Gegenwärtig überwiegt unter Smart-City-Anhängern die Ansicht, die von ihnen propagierten Netzwerke aus Sensoren und Kontrollmechanismen verfügten vor allem über eine «gutmütige» Intelligenz, vor der man sich nicht zu fürchten bräuchte. Daran sind Zweifel angebracht. Jonathan Swarts spricht in diesem Zusammenhang von einer beschränkten «neoliberalen politökonomischen Vorstellungswelt», in der es bestimmte «Grundwerte, Orientierungen und unausgesprochene (wenn nicht gar unbewusste) Annahmen und Ansichten darüber gibt, wie politische und wirtschaftliche Systeme strukturiert sein müssen und welche Rollen bestimmte Akteure in diesen spielen können oder sollten». Ein großes

Problem ist dabei ein mangelndes Reflektionsvermögen, was nicht wirklich überrascht. Es wird nicht ausreichen, eine hochgradig normative Agenda zu vertreten und gleichzeitig nur geringfügige Anpassungen der existierenden Objekt- und Datenstrukturen vorzunehmen. Genauso wenig hilfreich ist eine freischwebende Form des Utopismus, bei der Governance als eine selbsttätige Maschine begriffen wird. Wir haben uns bemüht, mit unserer kritischen Analyse eine Grundlage zu schaffen, mit der das emanzipatorische Potenzial der «Smart City» für die gesamte Bevölkerung und nicht nur für die Elite (das heißt die meist männlichen Personen, die hinter dem Vorhang des Sensorenapparats stehen) freigelegt werden kann. Alle Bestrebungen, die Städte «intelligenter» zu machen, müssen an diesem Ziel – bei dem es um mehr Demokratie, das Ideal der Gleichheit und eine gerechtere Verteilung von Nutzen und Kosten geht – gemessen werden.

Aus dem Englischen von Max Henninger.

Jathan Sadowski ist Doktorand an der Arizona State University, wo er am Consortium for Science, Policy and Outcomes forscht und lehrt. Er interessiert sich vor allem für die gesellschafts- und gerechtigkeits-theoretischen sowie politökonomischen Aspekte von Informations- und Kommunikationstechnologien, insbesondere in «Smart Cities», mit denen er sich in seiner Dissertation befasst.

Frank Pasquale ist Professor für Rechtswissenschaft an der Francis King Carey School of Law der Universität Maryland. Er forscht zu den informationsrechtlichen Herausforderungen, die sich aus dem rapiden technologischen Wandel ergeben, insbesondere in den Bereichen der Gesundheitsversorgung, des Internets und der Finanzindustrie. Jüngste Veröffentlichung: «The Black Box Society: The Secret Algorithms that Control Money and Information», Cambridge 2015.

Die englische Originalfassung ist am 6. Juli 2015 im Journal First Monday unter dem Titel «The spectrum of control: A social theory of the smart city» erschienen (<http://firstmonday.org/ojs/index.php/fm/article/view/5903/4660>).

LITERATUR

- Agamben, Giorgio (2010):** Nacktheiten, Frankfurt am Main.
- Andrejevic, Mark (2004):** The work of watching one another: Lateral surveillance, risk, and governance, in: *Surveillance & Society*, 2, 4, S. 479–497, unter: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3359>.
- Angwin, Julia (2014):** Has privacy become a luxury good?, in: *New York Times*, 3.3.2014, unter: www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html.
- Arnsdorf, Isaac (2010):** The museum is watching you: Galleries quietly study what people like, or skip, to decide what hangs where, in: *Wall Street Journal*, 18.8.2014, unter: www.wsj.com/articles/SB10001424052748704554104575435463594652730.
- Bady, Aaron (2013):** The MOOC moment and the end of reform, in: *Liberal Education* 4/2013, S. 6–15, unter: <http://theneuwinquiry.com/blogs/zunguzungu/the-mooc-moment-and-the-end-of-reform/>.
- Balko, Radley (2013):** Rise of the Warrior Cop: The Militarization of America's Police Forces, New York.
- Baptist, Edward A. (2014):** The Half Has Never Been Told: Slavery and the Making of American Capitalism, New York.
- Baum, Dan (2011):** The ultimate jam session: While Singapore succeeds with an iron fist, the United States waits for the invisible hand, in: *Wired Magazine*, 1.11.2011, unter: <http://archive.wired.com/wired/archive/9.11/singapore.html>.
- Bobo, Kim (2011):** Wage Theft in America: Why Millions of Working Americans Are Not Getting Paid – And What We Can Do About It, New York.
- Bogard, William (1996):** The Simulation of Surveillance: Hypercontrol in Telematic Societies, New York.
- Campbell-Dollaghan, Kelsey (2014):** Police are testing a «live Google Earth» to watch crime as it happens, in: *Gizmodo*, 14.4.2014, unter: <http://gizmodo.com/police-are-testing-a-live-google-earth-to-watch-crime-1563010340>.
- Carpenter, Daniel/Moss, David A. (Hrsg.) (2013):** Preventing Regulatory Capture: Special Interest Influence and How to Limit It, Cambridge.
- Castle Press (2010):** Personix life stage clusters, unter: www.castlepress.net/cp_assets/CP_Lifestyle.pdf.
- Chambers, John/Elfrink, Wim (2014):** The Future of Cities: The Internet of Everything Will Change How We Live, in: *Foreign Affairs*, 31.10.2014, unter: www.foreignaffairs.com/articles/142324/john-chambers-and-wim-elfrink/the-future-of-cities.
- Citron, Danielle Keats/Pasquale, Frank A. (2011):** Network accountability for the domestic intelligence apparatus, in: *Harvard Law Journal* 1/2011, S. 1441–1494.
- Cohen, Julie E. (2012):** Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, New Haven.
- Cotterell, Roger (2006):** Law, Culture and Society: Legal Ideas in the Mirror of Social Theory, Hampshire.
- Crary, Jonathan (2014):** 24/7: Schlaflos im Kapitalismus, Berlin.
- Deleuze, Gilles (1993):** Unterhandlungen, 1972–1990, Frankfurt am Main.
- Democracy now! (2011):** Police crackdowns on Occupy protests from Oakland to New York herald the «new military urbanism», 16.11.2011, unter: www.democracynow.org/2011/11/16/police_crackdowns_on_occupy_protests_from.

- Doctorow, Cory (2014):** Riot control drone that fires paintballs, pepper-spray and rubber bullets at protesters, in: Boing Boing, 17.6.2014, unter: <http://boing-boing.net/2014/06/17/riot-control-drone-that-paintb.html>.
- Doctorow, Cory (2015):** Technology should be used to create social mobility – Not to spy on citizens, in: The Guardian, 10.3.2015, unter: www.theguardian.com/technology/2015/mar/10/nsa-gchq-technology-create-social-mobility-spy-on-citizens.
- Foucault, Michel (1986):** Sexualität und Wahrheit 1: Der Wille zum Wissen, Frankfurt am Main.
- Fraser, Nancy (1995):** From redistribution to recognition? Dilemmas of justice in a «post-socialist», in: New Left Review 212, S. 68–93.
- Friedersdorf, Conor (2014):** Eyes over Compton: How police spied on a whole city, in: The Atlantic, 21.4.2014, unter: www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/.
- Gabrys, Jennifer (2014):** Programming environments: Environmentality and citizen sensing in the smart city, in: Environment and Planning D: Society and Space 1/2014, S. 30–48, unter: <http://dx.doi.org/10.1068/d16812>.
- Gandy, Matthew (2005):** Cyborg urbanization: complexity and monstrosity in the contemporary city, in: International Journal of Urban and Regional Research 1/2005, S. 26–49; unter: <http://dx.doi.org/10.1111/j.1468-2427.2005.00568.x>.
- Geertz, Clifford (1973):** The Interpretation of Cultures: Selected Essays, New York.
- Gieryn, Thomas F. (2006):** City as truthspot: Laboratories and field-sites in urban studies, in: Social Studies of Science 1/2006, S. 5–38, unter: <http://dx.doi.org/10.1177/0306312705054526>.
- Goldsmith, Steven/Crawford, Susan (2014):** The Responsive City: Engaging Communities Through Data-Smart Governance, San Francisco.
- Graham, Stephen (2002):** CCTV: The stealthy emergence of a fifth utility?, in: Planning Theory & Practice 2/2002, S. 237–241, unter: <http://dx.doi.org/10.1080/14649350220150116>.
- Graham, Stephen (2009):** The urban «battlespace», in: Theory, Culture & Society 7–8/2009, S. 278–288, unter: <http://dx.doi.org/10.1177/0263276409349280>.
- Graham, Stephen (2011):** Cities Under Siege: The New Military Urbanism, London.
- Greenfield, Adam (2013):** Against the Smart City, New York.
- Habermas, Jürgen (1987):** Theorie des kommunikativen Handelns 1: Handlungsrationalität und gesellschaftliche Rationalisierung, Frankfurt am Main.
- Habermas, Jürgen (2014):** Faktizität und Geltung: Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats, Frankfurt am Main.
- Halpern, Orit/LeCavalier, Jesse/Calvillo, Nerea/Pietsch, Wolfgang (2013):** Test-bed urbanism, in: Public Culture 2/2013, S. 273–306, unter: <http://dx.doi.org/10.1215/08992363-2020602>.
- Haraway, Donna (1991):** A cyborg manifesto: Science, technology, and socialist-feminism in the late twentieth century, in: dies.: Simians, Cyborgs, and Women: The Reinvention of Nature, New York, S. 149–181.

- Harcourt, Bernard E. (2012):** Political disobedience, in: *Critical Inquiry* 1/2012, S. 33–55, unter: <http://dx.doi.org/10.1086/668049>.
- Harvey, David (1989):** From managerialism to entrepreneurialism: The transformation in urban governance in late capitalism, in: *Geografiska Annaler. Series B, Human Geography* 1/1989, S. 3–17, unter: <http://dx.doi.org/10.2307/490503>.
- Harvey, David (2008):** The right to the city, in: *New Left Review* 53, S. 23–40, unter: <http://newleftreview.org/II/53/david-harvey-the-right-to-the-city>.
- Hollands, Robert G. (2008):** Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?, in: *City* 3/2008, S. 303–320, unter: <http://dx.doi.org/10.1080/13604810802479126>.
- Hollands, Robert G. (2015):** Critical interventions into the corporate smart city, in: *Cambridge Journal of Regions, Economy and Society* 1/2015, S. 61–77, unter: <http://dx.doi.org/10.1093/cjres/rsu011>.
- Hoofnagle, Chris Jay (2003):** Big brother's little helpers: How Choicepoint and other commercial data brokers collect and package your data for law enforcement, in: *North Carolina Journal of International Law & Commercial Regulation* 1/2003, S. 595–637, unter: www.law.unc.edu/journals/ncilj/issues/volume29/number-4-summer-2003/big-brothers-little-helpers-how-choicepoint-and-other-commercial-data-brokers-collect-and-package-your-data-for-law-enforcement/.
- Jurgenson, Nathan (2012):** When atoms meet bits: Social media, the mobile Web and augmented revolution, in: *Future Internet* 1/2012, S. 83–91, unter: <http://dx.doi.org/10.3390/fi4010083>. 2015).
- Kitchin, Rob (2014):** The real-time city: Big data and smart urbanism, in: *GeoJournal* 1/2014, S. 1–14, unter: <http://dx.doi.org/10.1007/s10708-013-9516-8>.
- Kitchin, Rob/Dodge, Martin (2011):** *Code/Space: Software and Everyday Life*, Cambridge.
- Krieger, Nancy (1994):** Epidemiology and the web of causation: Has anyone seen the spider?, in: *Social Science & Medicine* 7/1994, S. 887–903, unter: [http://dx.doi.org/10.1016/0277-9536\(94\)90202-X](http://dx.doi.org/10.1016/0277-9536(94)90202-X).
- Lanier, Jaron (2011):** *You Are Not a Gadget: A Manifesto*, New York.
- Lessig, Lawrence (1999):** *Code and Other Laws of Cyberspace*, New York.
- Lévi-Strauss, Claude (2010):** *Das wilde Denken*, Frankfurt am Main.
- Magnet, Shoshana Amielle (2011):** *When Biometrics Fail: Gender, Race, and the Technology of Identity*, Durham.
- Manzi, Jim (2012):** *Uncontrolled: The Surprising Payoff of Trial-and-Error for Business, Politics, and Society*, New York.
- McCoy, Alfred W. (2009):** Welcome home, war! How America's wars are systematically destroying our liberties, in: *TomDispatch*, 12.11.2009, unter: www.tomdispatch.com/blog/175154/tomgram%3A_alfred_mccoy,_surveillance_state,_u.s.a.
- Merton, Robert K. (1968):** On sociological theories of the middle range, in: ders.: *Social Theory and Social Structure*, New York, S. 39–53.
- Mirowski, Philip (2013):** *Never Let a Serious Crisis Go to Waste: How Neoliberalism Survived the Financial Meltdown*, London.

Monahan, Tarin (2010): Surveillance as governance: Social inequality and the pursuit of democratic surveillance, in: Haggerty, Kevin D./Samatas, Minas (Hrsg.): *Surveillance and Democracy*, New York, S. 91–110.

Morozov, Evgeny (2014): Every little byte counts, in: *New York Times*, 16.5.2014, unter: www.nytimes.com/2014/05/18/books/review/the-naked-future-and-social-physics.html.

Neirotti, Paolo/De Marco, Alberto/Cagliano, Anna Corinna/Mangano, Giulio/Scorrano, Francesco (2014): Current trends in smart city initiatives: Some stylised facts, in: *Cities* 38, S. 25–36, unter: <http://dx.doi.org/10.1016/j.cities.2013.12.010>.

Newsom, Gavin (2013): *Citizenville: How to Take the Town Square Digital and Reinvent Government*, New York.

Palmisano, Samuel (2010): Building a smarter planet: The time to act is now. Rede im Chatham House, London, 12.1.2010, unter: www.ibm.com/smarterplanet/us/en/events/sustainable_development/12jan2010/.

Pasquale, Frank (2015): *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge.

Peppet, Scott R. (2011): Unraveling privacy: The personal prospectus and the threat of a full disclosure future, in: *Northwestern University Law Review* 3/2011, S. 1153–1204, unter: <http://www.northwesternlawreview.org/issues/105/3>.

Purcell, Mark (2002): Excavating Lefebvre: The right to the city and its urban politics of the inhabitant, in: *GeoJournal* 2–3/2002, S. 99–108, unter: <http://dx.doi.org/10.1023/B:GEJO.0000010829.62237.8f>.

Reuters (2015): IBM says to invest \$3 billion in «Internet of things» unit«, unter: www.reuters.com/article/2015/03/31/us-ibm-investment-idUSKBN0MROBS20150331.

Roderick, Leanne (2014): Discipline and power in the digital age: The case of the US consumer data broker industry, in: *Critical Sociology* 5/2014, S. 729–746, unter: <http://dx.doi.org/10.1177/0896920513501350>.

Rosen, Christine (2012): The machine and the ghost, in: *New Republic*, 12.6.2012, unter: www.newrepublic.com/article/books-and-arts/magazine/104874/rosen-verbeek-technology-morality-intelligence.

Rothkopf, David (2009): *Superclass: The Global Power Elite and the World They Are Making*, New York.

Sadowski, Jathan (2014a): Insurance vultures and the Internet of things, in: *Baffler*, 11.6.2014, unter: www.thebaffler.com/blog/insurance-vultures-and-the-internet-of-things/.

Sadowski, Jathan (2014b): Biometrics are coming for you, in: *Al Jazeera America*, 6.7.2014, unter: <http://america.aljazeera.com/opinions/2014/7/biometrics-big-datamining.html>.

Sadowski, Jathan/Pasquale, Frank (2014): Creditors use new devices to put squeeze on debtors, in: *Al-Jazeera America*, 9.11.2014, unter: <http://america.aljazeera.com/opinions/2014/11/debt-collection-technologystarterinterruptdevicesubprime.html>.

Sadowski, Jathan/Selinger, Evan (2014): Creating a taxonomic tool for technocracy and applying it to Silicon Valley, in: *Technology in Society* 38, S. 161–168, unter: <http://dx.doi.org/10.1016/j.techsoc.2014.05.001>.

- Salinas, Brenda (2013):** High-end stores use facial recognition tools to spot VIPs, unter: www.npr.org/blogs/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips.
- Santus, Brenda (2014):** Hackers claim they can copy fingerprints from photos, in: Mashable, 29.12.2014, unter: <http://mashable.com/2014/12/29/fingerprint-photo-copy/>.
- Schneier, Bruce (2014):** The Internet of things is wildly insecure – and often unpatchable, unter: www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html.
- Scholz, Trebor (Hrsg.) (2013):** Digital Labor: The Internet As Playground and Factory, New York.
- Shay, Lisa/Hartzog, Woodrow/Nelson, John/Larkin, Dominic/Conti, Gregory (i.E.):** Confronting automated law enforcement, in: Calo, Ryan/Froomkin, Michael A./Kerr, Ian (Hrsg.): Robot Law, Northampton, unter: <http://robots.law.miami.edu/wp-content/uploads/2012/01/Shay-EtAl-Confronting-AutomatedLawEnf.pdf>.
- Shelton, Taylor/Zook, Matthew/Wiig, Alan (2014):** The «actually existing smart city», in: Cambridge Journal of Regions, Economy and Society, 1/2014, S. 13–25, unter: <http://dx.doi.org/10.1093/cjres/rsu026>.
- Söderström, Ola/Paasche, Till/Klauser, Francisco (2014):** Smart cities as corporate storytelling, in: City 3/2014, S. 307–320, unter: <http://dx.doi.org/10.1080/13604813.2014.906716>.
- Solum, Lawrence B. (2014):** Artificial meaning, in: Washington Law Review 1/2014, S. 69–86, unter: www.law.uw.edu/wlr/print-edition/past-issues/vol-89/1/artificial-meaning/.
- Star, Susan Leigh (1999):** The ethnography of infrastructure, in: American Behavioral Scientist 3/1999, S. 377–391, unter: <http://dx.doi.org/10.1177/00027649921955326>.
- Sterling, Bruce (2014):** The Epic Struggle of the Internet of Things, Moskau.
- Swarts, Jonathan (2013):** Constructing Neoliberalism: Economic Transformation in Anglo-American Democracies, Toronto.
- Taylor, Charles (1971):** Interpretation and the sciences of man, in: Review of Metaphysics 1/1971, S. 3–51.
- Townsend, Anthony (2014):** Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia, New York.
- U.K. Department for Business, Innovation & Skills (2013):** The smart city market: opportunities for the UK. BIS Research Paper 136, unter: www.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217-smart-city-market-opportunities-uk.pdf.
- Unger, Roberto Mangabeira (2004):** Plasticity into Power: Comparative-Historical Studies on the Institutional Conditions of Economic and Military Success, London.
- Vanolo, Alberto (2014):** Smartmentality: The smart city as disciplinary strategy, in: Urban Studies 5/2014, S. 883–898, unter: <http://dx.doi.org/10.1177/0042098013494427>.
- Verchick, Robert R. M. (2010):** Facing Catastrophe: Environmental Action for a Post-Katrina World, Cambridge.

Virilio, Paul (1989): Der negative Horizont. Bewegung, Geschwindigkeit, Beschleunigung, München.

Virilio, Paul (2009): The state of emergency, in: Rosa, Hartmut/Scheuerman, William E. (Hrsg.): High-Speed Society: Social Acceleration, Power, and Modernity, University Park, S. 201–214.

Walker, Shaun/Grytsenko, Oksana (2014): Text messages warn Ukraine protesters they are «participants in mass riot», in: The Guardian, 21.1.2014, unter: www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot.

Wasik, Bill (2013): In the programmable world, all our objects will act as one, in: Wired Magazine, 14.5.2013, unter: www.wired.com/2013/05/internet-of-things-2/all/.

Winner, Langdon (1977): Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought, Cambridge.

Winters, Jeffrey A. (2011): Oligarchy, New York.

Wacquant, Loïc (2008): The militarization of urban marginality: Lessons from the Brazilian metropolis, in: International Political Sociology 1/2008, S. 56–74, unter: <http://dx.doi.org/10.1111/j.1749-5687.2008.00037.x>.

IMPRESSUM

ANALYSEN Nr. 23

wird herausgegeben von der Rosa-Luxemburg-Stiftung

V. i. S. d. P.: Stefan Thimmel

Franz-Mehring-Platz 1 · 10243 Berlin

www.rosalux.de

ISSN 2194-2951 · Redaktionsschluss: Dezember 2015

Layout/Herstellung: MediaService GmbH

Druck und Kommunikation

Lektorat: TEXT-ARBEIT, Berlin

Gedruckt auf Circleoffset Premium White,
100% Recycling

«Angesichts der vielen Versprechen und hoffnungsvollen Visionen, die mit «Smart Citys» verknüpft sind, verwundert es nicht, dass dabei die politischen Inhalte und Vorgaben häufig aus den Augen verloren werden, die in die miteinander verbundenen Technologien und Initiativen wie ein Code eingeschrieben sind.»

JATHAN SADOWSKI UND FRANK PASQUALE

