Nils Erik Flick

„Smart City" – alternativloser Selbstläufer oder abgekartetes Spiel?

Aufruf zur Diskussion

Türen, die Dich freundlich grüßen.[1] Kühlschränke, die mit Autos über Deine Gewohnheiten reden, und andere wahr gewordene Wahnvorstellungen. Straßenlaternen, die Menschen ansprechen oder welche melden, die sich komisch verhalten. Eine Umgebung, die Dich kennt. Was kann schon schiefgehen? Oder ist schon etwas schiefgegangen, wenn niemand mehr einen Schritt machen kann, ohne verfolgt, erfasst, erkannt, profiliert, von Maschinen mit dem Vornamen angesprochen und dabei hinterrücks analysiert zu werden, zum Zweck individualisierter Abrechnung, Marktforschung, Infrastrukturplanung und natürlich besserer Anpassung an die eigenen (selbstverständlich messbaren, modellierbaren und beliebig extrapolierbaren) Bedürfnisse? „The spectrum of control: A social theory of the smart city", *ein Beitrag von* Jathan Sadowski *und* Frank Pasquale *im* First Monday Peer-Reviewed Journal on the Internet *gab Anlass, die dort aufgestellten Thesen zu reflektieren und zur Diskussion zu stellen.[2]*

Was ist Überwachungskapitalismus, was ist eine Kontrollgesellschaft, und was haben beide mit dem Schlagwort *„smart"* zu tun? Ist *die Stadt der Zukunft*, in der *alles vernetzt* ist, Segen oder Desaster? Wem nutzen all die Vernetzungsvisionen? Werden hier wichtige Punkte unterschlagen? Sadowski und Pasquale üben pointierte Kritik an Plänen zur Vernetzung von Infrastrukturen, Objekten, Menschen in der Stadt. Sie zeigen, dass der Diskurs ein erhebliches Framing durch die Marketing-Rhetorik der *„Smart"*-Vertreter erfahren hat, die ihr Vorgehen gern als pragmatische Problemlösung darstellen.[3] Diese Mär wird ebenso widerlegt wie die ideologische Neutralität einer *„Smart City"*, deren Mehrwert auf einer neoliberalen Kommodifizierung persönlicher Daten beruht. Der folgende Text bezieht sich auf Sadowski und Pasquale, streut aber eigene Betrachtungen ein.

Ein unsichtbares Wurzelgeflecht

Wir leben in einem überwachungskapitalistischen System, in dem alltägliche Daten über uns gesammelt, aufbereitet und gehandelt werden.[4,5] Aus Mobilfunk-Standortdaten entstehen Bewegungsprofile,[6] Buchungen und Online-Äußerungen landen bei Kredit-Auskunfteien.[7] Auswertungen, denen niemand informiert zugestimmt hätte, werden auf Infrastrukturen gesetzt und verändern deren Charakter essenziell – *Function Creep* verwässert die Zweckbindung von Daten.[8,9] Die Industrie will mehr: sie propagiert ein *Internet der Dinge* – im Englischen noch viel treffender *internet of everything* genannt –, in dem noch mehr Daten[10] anfallen. Immer mehr Geräte funktionieren nur noch mit Internetverbindung.[11] In Politik und Verwaltung arbeitet es, „warum nicht alles effizienter machen, womöglich in öffentlich-privater Partnerschaft?". Verwaltungsdaten eignen sich zur Vermarktung.[12] So wuchert in harmonischer Symbiose mit kommerzieller Überwachung auch der Staat in die elektronischen Netze, kann der Verlockung der Macht nicht widerstehen und wird zunehmend zu einer Gefahr für sich selbst. Nach dem Willen der Branchenriesen[13] steht mehr Vernetzung bevor. Manchmal muss die Entwicklung durch Werbung, Gruppenzwang oder Verordnungen forciert werden, letzteres im Fall des *Smart Meter*, das als Teil des Wurzelgeflechts Daten ausleitet,[14] oder im Fall der *eHealth* – ein eigenes Thema.[15] Trotz mangelhafter Argumente wird die *smarte Zukunft* zur Erlösung verklärt. In ihr ist alles gut, optimiert, optimal. *Big Data* ist der große Bruder von *„Smart"*: ein Solutionismus, der mit Technik und Statistik gesellschaftliche Probleme lösen will, ohne neue zu schaffen.[16]

Jathan Sadowski, Frank Pasquale: The spectrum of control: A social theory of the smart city, München: Knaur Verlag, http://firstmonday.org/ojs/index.php/fm/article/view/5903

Wir übernehmen die Konvention aus Sadowski und Pasquale (s. o.), *„smart"* in Anführungszeichen zu setzen, weil es nie definiert wird, nur als vage positives Label dient. *„Smart City"* meint ein integriertes Informationsnetzwerk aus Objekten (und Menschen) mit einer Vielzahl möglicher Anwendungen: die Stadt als ungenutzte Datenquelle. Die typischen Szenarien wirken plastikartig, die Phrasen abgedroschen – die *„smarte Welt"*, in der „alles vernetzt" ist: Man achte auf bestimmte Artikel („*die* Stadt *der* Zukunft"). Werden diejenigen, die *nicht* wollen oder können, ausgeschlossen oder assimiliert? Eventuell sind diese Floskeln bloß rhetorische Missgriffe: die konkreten Projekte unterscheiden sich durchaus voneinander. Sadowski und Pasquale kritisieren dubiose Kosten-Nutzen-Rechnungen und die Tendenz, den Sozialvertrag durch einen Unternehmensvertrag zu ersetzen (Abschnitt III).

Die Kontrollgesellschaft und die Beziehung zwischen Verwaltung und Gesellschaft in der *„Smart City"*: ein kybernetischer Regelkreis?

Schwerer zugänglich ist vielleicht die Deleuzesche Philosophie, auf der die Kritik in den späteren Abschnitten von Sadowski und Pasquale basiert.[17] Drei Grundbegriffe werden im Text erklärt und spielen eine wichtige Rolle: *Dividuen* (*dividu-*

als), *Wurzelgeflechte* (*rhizomes*), *Passworte* (*passwords*). Ein *Dividuum* ist ein in messbare Teilaspekte zerlegtes Individuum: ein Apparat liest messbare Attribute des Individuums, versteht es eben nicht als Ganzes, das in seiner Individualität geachtet werden muss. Der auf Unsichtbarkeit getrimmte Hintergrund an Technologie, der die *„Smart City"* und ähnlich gestrickte Visionen ausmacht, ist ein *Wurzelgeflecht* – ein recht treffendes Bild. *Passworte* sind authentifizierende oder legitimierende Informationen bzw. Artefakte, über die eine Person verfügt: eine PIN, eine Schlüssel- oder Kreditkarte, eventuell auch biometrische Merkmale. Die Kontrolle liegt nicht bei dieser Person: Zugangsberechtigt ist sie von Gnaden des Systems, das ebensogut beschließen kann, sie zu delegitimieren, nicht mehr in ihr eigenes Haus zu lassen. Problematische Aspekte bleiben demnach bei technokratischen Überlegungen zum Aufbau einer *„Smart City"* außer Acht oder werden gleichsam in den AGB versteckt, die es abzunicken gilt.

Klassische Bürokratien dividualisieren gern: Bei Zensus und Mikrozensus wird dem/der Befragten keinesfalls zugestanden, selber zu entscheiden, welche der teils intimen Fragen er/sie beantworten möchte oder für relevant hält.[18] Dabei zwingen genaue Daten offensichtlich nicht zu guter Planung, angebrachter wäre die Klärung der Bedürfnisse mündiger Bürger in einem Dialog. Die *„Smart City"* wiederholt diesen Fehler: eine Gesellschaft als mess- und steuerbares System und ihre Individuen als dividualisierte Datenbündel und nicht als selbstbestimmte Subjekte anzusehen. Das ist schade, da im Volkszählungsurteil das Grundrecht auf informationelle Selbstbestimmung erkannt wurde.[19]

„Smarte" Systeme erkennen Fehlverhalten. *„Smarte"* Infrastruktur kann auf Menschen einwirken: Demonstranten werden über ihre *„Smartphones"* registriert, Anti-Demo-Drohnen sind aus der dystopischen Fiktion auf den realen Markt gewandert (Sadowski und Pasquale, Abschnitt VI). Das Spektrum der Kontrolle ist breit. Durch die digitale Vermittlung von Verrichtungen sowie die Anbindung an Server, die Identität, Legitimation, Vergangenheit prüfen können, weicht der Dialog mit der Umwelt einer strategisch geprägten Beziehung. Wie kann ich das System dazu bringen, nicht gegen mich zu arbeiten? Anders herum: Wie lassen sich vorgegebene Ziele durch Einwirkung auf die Nutzer optimieren? Die automatische Einwirkung durch eine automatisierte Infrastruktur, die das Verhalten der Bewohner im Sinne der Verwaltung und privater Partner steuert (optimiert), ist Kernaspekt der *„Smart City"*.

„Fifth Utilities" und die Selbstverständlichkeit der Überwachung; Eskalation durch Sicherheit; wem gehört die Stadt der Zukunft?

Utilities sind Versorgungsinfrastrukturen: Strom, Wasser, Gas, Telekommunikation. Ironisch werden Kameras (in Sadowski und Pasquale, Abschnitt V) zur *Fifth-Utility* erklärt – wegen der schockierenden Selbstverständlichkeit, mit der Überwachbarkeit als neue Norm etabliert wird, natürlich immer mit den besten Absichten, was aber, wie Sadowski und Pasquale bemerken, Makulatur ist: Niemand hält sich an Absichten.

Was zählt, sind geschaffene Fakten. Die *„Smart City"* wird uns wohl genau zuschauen und -hören. Der Umbau der Stadt in eine private Werbefläche,[20] euphemistisch *Stadtmöblierung*, hat ebenfalls *fifth-utility*-Charakter. Versuche mit Gesichtserkennung laufen auch schon.[21,22] Ein Dialog zwischen Gleichen sieht anders aus. Wem gehört die Stadt der Zukunft?

Nach Sadowski und Pasquale wird in der *„Smart City"* Ungerechtigkeit eher ausgebaut als gemildert. Überwachung wird komplementiert durch *Sicherheit*. Kameras mit *Intentionserkennung* und Taserpistolen – ein Sinnbild für die Implikationen der *„Smart City"* für die innere Sicherheit: Resignation entsteht, *„smarte"* Kontrolltechniken schränken die Handlungsfreiheit derart ein, dass die Frustration in Gewalt umschlagen kann: Friedlicher Protest wird erstickt. Realwelt und Internet konvergieren (*cyborg urbanization*, Sadowski und Pasquale, Abschn. VII): Eine *Infrastruktur der Unfreiheit* wird aufgebaut.[23,24]

Zurück in *die Zukunft*: wer kontrolliert wen? Die Idee des Regelkreises passt, zumal bei *„Smart"* ein naiver Effizienzgedanke im Vordergrund steht, siehe Lanier.[25] Ist die *„smarte"* Zukunft eifrigen Selbstoptimierern vorbehalten, deren Teilhabe am Leben stets über irgendeine kommerzielle Plattform vermittelt ist? Eine traurige Vorstellung. Wer kontrolliert was? Versprechen, dass die Kontrolle über die eigenen Daten beim Kunden bleibt, sind nichts wert: Nur nachprüfbare technische Umsetzungen des Prinzips sind glaubwürdig. Natürlich ist *„Smart City"*-Forschung auch durch Idealismus und Kreativität getrieben. Unterliegt die Entscheidung, was wie zum Einsatz kommt, Betriebswirtschaft und Macht, negieren diese jedoch das emanzipatorische Potenzial nützlicher Technologie. Ein Ausweg kann darin bestehen, die Beziehung zur Technologie neu zu denken: In einem freiwilligen Modell, bei dem die Kontrolle über Programmierung und Betrieb aller Endgeräte beim Nutzer liegt und kein Dienst persönlich identifizierbare Daten sammelt, ließen sich manche Vor-

Nils Erik Flick

Nils Erik Flick ist Doktorand in der Informatik an der Carl von Ossietzky Universität Oldenburg und seit 2011 FIfF-Mitglied. Seine Forschungsschwerpunkte sind Software-Verifikation und formale Sprachen, seine Interessengebiete u. a. Computer-Sicherheit und Kryptologie.
Kontakt: *flick@informatik.uni-oldenburg.de*

teile realisieren. Vernetzung ist gedanklich von allem zu trennen, das lokal realisierbar ist. Zu aggregierende Daten ließen sich dann durch datensparsame Algorithmen verknüpfen[26,27]. Proprietäre Systeme sind ebenfalls kritisch zu sehen. Eine löbliche Ausnahme vom Trend, IT-Riesen zu beauftragen, ist Barcelona:[28] Implementation in freier Software, Messdaten als *Open Data*. Die Verdrängung proprietärer *Lösungen* durch freie, selbstorganisierte Projekte ist ein richtiger Schritt und kann z. B. das Offenhalten von Sicherheitslücken verhindern. Gute Intentionen genügen aber nicht: Auch *Big Other* bedroht die informationelle Selbstbestimung.[29]

Fazit, Konklusion und Ausblick

Im Vortrag *„We lost the war"* von 2006 warnten Frank Rieger und Rop Gonggrijp vor einer bevorstehenden dunklen Zeit des Grundrechteabbaus und gaben zu bedenken, dass den wenigen AktivistInnen nicht genügend Mittel zur Verfügung stünden, um alle Schlachten zu schlagen.[30] Der Trend zum automatischen Polizeistaat hält an. Es zeigt sich, dass die Interessen staatlicher Überwacher und kommerzieller Datensammler miteinander vereinbar sind und sich im *Big Data* treffen. Das Potenzial zum Missbrauch von Scorings oder Rohdaten durch staatliche Stellen ist ein Grund, vernetzte Sensoren abzulehnen. Der Artikel von Sadowski und Pasquale liefert einen Beitrag dazu, den ideologisch verzerrten und von Schönrednerei geprägten Diskurs über *„Smart Cities"* gerade zu rücken und vor Überwachung und Kontrolle zu warnen. Viele der Referenzen, darunter weitere zum Thema *„Smart Cities"*, sind lesenswert. Sadowski und Pasquale helfen, *„Smart City"* Pläne besser einzuordnen.

Ist die Bekämpfung von *PESTs* (*Privatsphäre-erodierende „Smart"-Technologien*, im Englischen auch *Parasiten* …) eine Schlacht, die geschlagen werden muss? Ist eine Eindämmung realistisch oder muss man anders ansetzen? Lanier z. B. scheint in seinem zitierten Essay aufgegeben zu haben und fordert eine faire Vergütung als zweitschlechteste Alternative zum zentralisierten unbezahlten Datenraub. Solange eine starke Gegenbewegung fehlt, bleibt der Unmut über die Usurpation vormals freier Lebensbereiche durch *Big Data* eine müßige, solitäre Beschäftigung. Freiräume werden marginalisiert, bedrängt durch autoritäre Strömungen, die die von Sadowski und Pasquale skizzierte Version der *„Smart City"* wohl begrüßen werden. Es ist daher geboten, überwachungs- und dividualisierungsfreie Zonen zu verteidigen, und in die Offensive zu gehen. Datensparsamkeit muss *cool* werden. Abgesehen von Datenschutzbedenken wäre es auch gar nicht dumm (geradezu *smart*!), die wachsende Abhängigkeit von Computersystemen zu überdenken, nicht zu intensivieren.

Anmerkungen

1 Vorweggenommen von Douglas Adams in „Per Anhalter durch die Galaxis", wo eine solche Funktion ungeahnte Konsequenzen hat. Douglas Adams, „Life, the Universe and Everything" (1982, ISBN 0-345-39182-9).

2 Jathan Sadowski and Frank Pasquale, The spectrum of control: A social theory of the smart city. First Monday Peer-Reviewed Journal on the Internet, http://www.firstmonday.org/ojs/index.php/fm/article/view/5903

3 R. Kitchin, 2014. "The real-time city: Big data and smart urbanism," GeoJournal, vol. 79, no. 1, pp. 1–14.

4 John Bellamy Foster and Robert W. McChesney, Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. Monthly Review, http://monthlyreview.org/2014/07/01/surveillance-capitalism/

5 Shoshana Zuboff, 2015. „Big Other: Surveillance Capitalism and the Prospects of an Information Civilization". Journal of Information Technology (2015) 30, 75–89. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

6 Nach zaghaften Modellversuchen in der Branche beschliesst die Telekom 2015, alle Mobilfunkkunden zu tracken und die Erkenntnisse zu verkaufen. https://netzpolitik.org/2015/data-analytics-deutsche-telekom-rastert-mobilfunk-vorratsdaten-zu-kommerziellen-zwecken/

7 Kreditech: „The Kreditech Group uses big data algorithms and automated processes to score everyone worldwide, also the 4bn [4 Milliarden] unbanked that do not have a credit score." https://www.datenschutz.de/news/detail/?nid=5905

8 Mordini, Emilio. „Ethics and Policy of Biometrics." Handbook of Remote Biometrics. Springer London, 2009. 293-309.

9 Wright, David, et al. „Sorting out smart surveillance." Computer Law & Security Review 26.4 (2010): 343-354.

10 Am Datenschutz krankt es schon in den unteren Netzwerkschichten: Der IPv6-Standard [RFC 4862, „stateless autoconfiguration"] sieht auch für mobile Geräte zunächst eine eindeutige und unveränderliche Netzwerkschnittstellen-Kennnummer vor, die in der globalen IPv6-Adresse des Gerätes eingebaut ist. Erweiterungen wie das Würfeln der Geräteadresse [RFC 4941] sind in billigen Chips kaum zu erwarten. Schon heute haben etwa WLAN-Chips in mobilen Geräten die problematische Eigenschaft, eine weitgehend eindeutige Hardware-Adresse (MAC) zu nutzen, die oftmals nur unter Schwierigkeiten temporär geändert werden kann. Damit lassen sich Bewegungsprofile, zunächst der Dinge, davon abgeleitet natürlich auch der Besitzer erstellen. Dies gehört, ebenso wie die Frage, welche Datenverarbeitung lokal geschieht und welche auf den Servern eines „Cloud"-dienstleisters, zu den unsichtbaren Eigenschaften der Technologie, die aber als essenziell zu betrachten sind und nur in einer unehrlichen oder fehlinformierten Abstraktion ignoriert werden können.

11 Z. B. Fitnessmessgeräte von der Firma OMRON, http://www.omron-healthcare.de/. Zum Herunterladen der Daten auf den PC wird offenbar eine Anmeldung nebst Zustimmung zu Datensammel-AGB in einem Online-Portal verlangt. Der Treiber liegt nicht bei, und die Verpackung warnt nicht. Marketing-Claim auf der OMRON-Homepage: „Wir stellen den Mensch vor die Technologie" (sic, mit Deppenbeugung).

12 Meldegesetz: https://www.datenschutzbeauftragter-info.de/neues-meldegesetz-der-staat-als-adresshaendler/

13 Samsung möchte das „Internet of Things" vorantreiben: http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/; IBM: „Smarter Planet"-Kampagne

14 http://www.zeit.de/digital/datenschutz/2013-11/smart-meter-teuer-daten-vermarkten

15 Siehe Beiträge zur eGK in früheren Ausgaben der FIfF-Kommunikation.

16 Evgeny Morozov, 2014. „To Save Everything, Click Here: The Folly of Technological Solutionism", ISBN 978-1610393706

17 Gilles Deleuze, 1995. „Negotiations, 1972–1990". (Transl.: Martin Joughin), Columbia Univ. Press, ISBN 978-0231075817

18 www.devianzen.de/2014/12/31/das-recht-in-ruhe-gelassen-zu-werden/

19 Volkszählungsurteil von 1987: http://www.servat.unibe.ch/dfr/bv065001.html. Zugleich wurden im Urteil Grenzen für das Recht auf informationelle Selbstbestimmung vorgesehen, falls das „öffentliche Interesse überwiegt".

20 Straßenkunst oder kreative Verfremdungen oder Richtigstellungen der Werbung können als Vandalismus verfolgt werden, während andersherum ziemlich viel Narrenfreiheit herrscht: die Anregung zum Überkonsum hat eine privilegierte Stellung inne. Sieht so Fortschritt aus? Die Stadt als kommunikative Einbahnstraße? Wird sich die „Smart City"-Entwicklung in diese Kette von Entfremdungen einreihen?

21 TESCO-Tankstellen missbrauchten Gesichtserkennung für Werbung, http://www.bbc.co.uk/news/technology-24803378

22 Keine Konzessionen bei kommerzieller Gesichtserkennung: https://firstlook.org/theintercept/2015/06/16/privacy-advocates-resign-protest-u-s-facial-recognition-code-conduct-2 – Es stellt sich ohnehin die Frage, mit welcher Legitimation datensammelnde und -verarbeitende Industrie überhaupt zum *Stakeholder* in der Privatsphäre anderer erklärt wird.

23 Eben Moglen (siehe Endnote 24) – mit dem Unterschied, dass die Datenspuren in der realen Welt sehr viel breiter und sehr viel schlechter zu verschleiern sind, wenn einmal eine ähnliche Überwachungsdichte erreicht wird. Es ist unmöglich, der Überwachung in der realen Welt durch Kryptographie zu entkommen. Daher führt der Ausbau hier in eine noch sehr viel unfairere Lage als theoretisch im *Cyberspace*. Die Konvergenz läuft natürlich auch anders herum, etwa durch realweltliche Verbote sicherer Endgeräte (oder deren pervasive Kompromittierung http://www.ceu.edu/article/2015-01-19/real-world-battles-will-be-won-or-lost-internet-doctorow-says).

24 Eben Moglen, Snowden and the Future, http://snowdenandthefuture.info/ (4 Vorträge)

25 Lanier, Jaron. Who owns the future? Penguin, 2014, ISBN 978-0-241-95721-9 [S. 42 ff.]

26 *Secure Multiparty Computation* erlaubt es, beliebige Funktionen auf Datensätzen zu berechnen, ohne jedoch zusätzliche Information über den Inhalt zu verraten.

27 Yehuda Lindell, Benny Pinkas, 2009. „Secure multiparty computation for privacy-preserving data mining". Journal of Privacy and Confidentiality 1, no. 1, pp. 59–98

28 Open Source, Open Data Barcelona: http://smartcity.bcn.cat/en/sentilo.html; anderes Projekt: https://smartcitizen.me/

29 Shoshana Zuboff, 2015. „Big Other: Surveillance Capitalism and the Prospects of an Information Civilization". Journal of Information Technology (2015) 30, 75–89. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

30 „We lost the war". Vortrag von Rop Gonggrijp und Frank Rieger (CCC) auf dem 22c3, https://events.ccc.de/congress/2005/fahrplan/events/920.en.html

vor*gänge* – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

Cybersecurity

Der NSA-Überwachungsskandal hat deutlich gemacht, in welchem Umfang und mit welcher Reichweite westliche Geheimdienste die Überwachung der Kommunikationsnetze betreiben. Der damit verbundene finanzielle, technische und personelle Aufwand lässt erahnen, dass es dabei keineswegs nur um die Ausforschung der Privatsphäre mehr oder weniger ahnungsloser Bürger.innen geht. Die Zeiten, in denen der Cyberspace nur dem Gedankenaustausch diente, sind längst vorbei; die Datennetze sind zur zentralen Infrastruktur unserer Gesellschaft geworden. Ihre Überwachung zielt deshalb nicht nur auf jene, die per E-Mail, Chat oder Onlineplattformen kommunizieren, sondern kann buchstäblich jede.n treffen: ob am Bankautomaten, in der Arztpraxis, bei der Arbeit oder im vernetzten Heim. Der „Cyberspace" ist zu einem Ort geworden, an dem sich neue Formen der Kriminalität, des Krieges und der terroristischen Bedrohung entwickeln, aber auch neue Strategien der Sicherheit erprobt werden. Diese Ausgabe der **vor*gänge*** widmet sich dem Thema Cybersecurity, der zunehmenden sicherheitspolitischen Durchdringung des digitalen Raumes.

*aus dem Editorial der **vor**gänge 209 (Heft 1/2015) von Claudia Krieg und Sven Lüders*