Christian Meyer

Digitale Disziplin
Zur Transformation der inneren Sicherheit

Ausnahmezustand in Frankreich und der Türkei, internationale Vernetzung von Polizeien und Geheimdiensten, Diskussionen über Anonymität im Kontext von Informations- und Kommunikationstechnologien (IKT), intelligente Kamerasysteme zur Überwachung des öffentlichen Raums – spätestens seitdem Europa mit den Anschlägen in den vergangenen Jahren seine ganz eigenen, traumatisierenden Erfahrungen mit Terrorismus gemacht hat, läuft die Maschinerie „innerer Sicherheit" in vielen Ländern wieder auf Hochtouren. Dabei scheinen technologische Antworten auf soziale Verhältnisse immer öfter als Mittel der Wahl. Mit digitaler Datenerhebung und -auswertung versuchen Sicherheitsbehörden, sich einen Reim auf komplexe Verhältnisse und Bedrohungen zu machen. Erstmals zeigte sich einer breiteren Öffentlichkeit das Ausmaß staatlicher Datensammlung im Zusammenhang mit IKT, als 2013 Edward Snowden die Praktiken der US-amerikanischen und britischen Geheimdienste publik machte. Hinzu kommen Diskussionen um den Zugriff auf persönliche Daten von Internetunternehmen wie Facebook oder Google. Überwachung und Datenschutz sind nicht länger nur in Bürgerrechtskreisen Thema. Eine Perspektive, die, trotz der Vielseitigkeit des Themas, die Zusammenhänge im Blick hat, ist hingegen selten und die Fülle an Technologien erschwert die Debatte zusätzlich. Klar ist nur, dass diverse Praktiken, sei es Kameraüberwachung oder die Ortung Verdächtiger, ohne das Internet heute nicht denkbar sind.

Die vorliegende Analyse geht der Frage nach, wie sich das Dispositiv der inneren Sicherheit über die letzten Jahre verändert hat und wie es aktuell verfasst ist. Dafür wird zunächst der Dispositivbegriff erläutert sowie relevante Sicherheitsdiskurse vorgestellt. Am EU-Forschungsprojekt INDECT wird beispielhaft die zentrale Rolle von Technologien und Digitalisierung für die innere Sicherheit gezeigt und anhand der foucaultschen Machttypen diskutiert. Schließlich wird das Dispositiv zeitdiagnostisch im Kontext neoliberaler Politik verortet.

PROKLA. Verlag Westfälisches Dampfboot, Heft 186, 47. Jg. 2017, Nr. 1, 63 – 81

Dispositiv, Disziplin und gouvernementale Sicherheit

Innere Sicherheit wird hier im Anschluss an Michel Foucault (1978) als *Dispositiv* gefasst. Ein Dispositiv ist zunächst „eine Gesamtheit von Praxen, Kenntnissen, Maßnahmen und Institutionen, deren Ziel es ist, das Verhalten, die Gesten und die Gedanken der Menschen zu verwalten, zu regieren, zu kontrollieren und in eine vorgeblich nützliche Richtung zu lenken" (Agamben 2008: 24). Foucault (1978: 119f.) selbst betont dabei „das Netz, das zwischen diesen Elementen geknüpft werden kann" und diesen seine Funktion zuweist. Ein Dispositiv ist eine strategische Formation, die „auf einen Notstand" (ebd.: 120) reagiert. Dabei ist es nicht statisch, sondern kann sich auch auflösen, zergliedern und neu zusammensetzen (Bührmann/Schneider 2008: 53). Der Vorteil, innere Sicherheit als Dispositiv zu denken, besteht darin, die Elemente in ihrer strategischen Formierung zu erfassen, was bei einseitiger Fokussierung, auf beispielsweise Entwicklungen im Bereich des Rechts, nicht gelingt. Das Dispositiv umfasst Diskurse, Technologien, polizeiliche Praktiken und Entwicklungen der Sicherheitsforschung, ferner Gesetze und Subjektivierungsweisen. Zudem hat es eine politische Dimension (Kunz 2005: 359).

Begriff, Gedanke und Konzept des Dispositivs hängen eng mit Foucaults Analysen von Machttypen zusammen, wonach diese „an ihren äußersten Punkten, in ihren letzten Andeutungen, in den Praktiken, in denen sie über Rechtsregeln hinausgeht, sich in Institutionen einlässt, in Techniken verkörpert oder sich Instrumente für materielle Eingriffe verschafft" (Demirović 2008: 28) analysiert werden soll. Michel Foucault unterscheidet zwischen zwei Machttypen, die in diesem Kontext relevant sind. Im 17. Jahrhundert etabliert sich die *Disziplinarmacht*. Als „'Mikrophysik' der Macht" (Foucault 1977: 178), stellt sie die Kontrolle ins Zentrum und hat den individuellen Körper zum Gegenstand (Foucault 1999: 279), wobei Kontrolle und Vereinzelung der Individuen im Kloster, im Militär, in der Schule und schließlich im Gefängnis perfektioniert werden. Symbol für die Logik dieser Institutionen ist das von Jeremy Bentham (1748-1832) konzipierte Panoptikum, in dem die Eingesperrten wissen, dass sie permanent überwacht werden. Sie verinnerlichen diesen Umstand und verhalten sich normkonform (Foucault 1977: 258ff.), denn ein permanentes Überwacht-werden-können kommt einem ständigen Sanktioniert-werden-können gleich (Opitz 2004: 33). Diese Form der Disziplinierung breitet sich in der gesamten Gesellschaft aus. Einen wesentlichen Beitrag dazu liefert die Polizei (Foucault 1977: 277).

Die *Gouvernementalität*, der zweite Machttyp, zielt dagegen auf die „Vielfalt der Menschen" (ebd.: 280) und ermittelt Abweichungen von einer statistisch ermittelten Norm (Foucault 2006: 96f.). Der Übergang von Disziplin zu Gouvernementalität ist auch einer von Normierung zu Normalisierung. Die Bevölkerung

erscheint als ein „Naturphänomen" (ebd.: 110), das man verstehen muss und welches sich nicht „per Dekret" (ebd.) ändern lässt. Es gibt jedoch Transformationskräfte, denen die Bevölkerung zugänglich ist, vorausgesetzt, dass diese „analytisch, wohlberechnet, vorausschauend" (ebd.) sind. Statistische Methoden sollen Aussagen über die Zukunft ermöglichen, um „dem Rechnung [zu] tragen, was geschehen kann" (ebd.: 39). Die Gouvernementalität steht damit auch für ein neues Verhältnis von Staatlichkeit zu Wissen. Die „Entstehung und Fortdauer des modernen Staates [ist] undenkbar ohne die permanente Generierung, Verbreitung, Speicherung und Unterdrückung von Wissen" (Lemke 2007: 53). Es geht darum, mit ausreichend Abstand zu beobachten, was sich ereignet (Foucault 2006: 75). Mit einer Haltung des laissez faire ist die Gouvernementalität nicht an hundertprozentiger Sicherheit in allen Details orientiert, sondern verfolgt ein ökonomisches Interesse, das nach einem optimalen Verhältnis zwischen Aufwand und Nutzen sowie nach der Minimierung gesellschaftlicher Kosten sucht (ebd.: 17).

Diskurse innerer Sicherheit: Bedrohung (aus) der Zukunft

Dem Dispositiv „innere Sicherheit" liegt ein Bedrohungsszenario zugrunde, „das von Terrorismus, organisierter Kriminalität bis zu illegaler Immigration reicht" (Kaufmann 2011: 102). Seit den 1980er Jahren, vor allem aber seit dem 11. September 2001, werden immer mehr Gesellschaftsbereiche vornehmlich unter Gefahrenaspekten behandelt (ebd.: 101). Dieser Umstand wird unter dem Begriff der *Securitization* (Versicherheitlichung) gefasst. „‚Sicherheit' ist der Akt, der Politik dazu verhilft, sich über die etablierten Spielregeln hinwegzusetzen. [...] Securitization kann dementsprechend als extremere Version der Politisierung eines Themas verstanden werden" (Buzan u.a. 1998: 23f.; Übers.: C.M.). *Securitization* findet aber nur erfolgreich statt, wenn ein gesellschaftlicher Bereich auch als sicherheitsrelevant anerkannt wird. Das heißt jedoch nicht, dass diese Anerkennung Resultat eines herrschaftsfreien Diskurses ist, vielmehr ist sie auf Konsens und Zwang angewiesen (ebd.: 25). Wird auf Strategien der *Securitization* zurückgegriffen, rechtfertigt das auch die Übertretung des liberalen Rahmens, die Missachtung geltender Gesetze und Akte der Autorität. *Securitization* ist damit auch die „Produktion von Ausnahmesituationen, in denen sich Souveränität manifestiert" (Opitz 2008: 220) und eine selbstreferenzielle Praxis, die Sicherheitsinteressen schafft, indem sie diese als solche benennt (Buzan u.a. 1998: 24). Die Politik der nationalen Sicherheit ist jedoch kein Selbstzweck, sondern hilft unter anderem, Opposition mundtot zu machen (ebd.: 29). Seit den 1970er Jahren ist die bundesdeutsche Debatte über innere Sicherheit zudem dadurch geprägt, dass

auf akute Bedrohungen verwiesen wird, um kurzfristige Entscheidungen treffen zu können (Kunz 2005: 360). Wird ein normativ aufgeladener Bezugspunkt, wie „die freiheitliche Ordnung" oder „unsere Lebensweise", bedroht, wird ein „rechtlich entkoppelte[r] Möglichkeitsraum" eröffnet (Opitz 2008: 220). Die Frage, *ob überhaupt* mehr Sicherheit nötig ist, kann im Diskurs der *Securitization* gar nicht gestellt werden. So ist der Diskurs grundsätzlicher Kritik unzugänglich und es ist äußerst schwierig, beispielsweise neue Technologien zu problematisieren.

Damit einher geht die steigende Popularität *ziviler Sicherheit*. Sie „konstituiert sich als Schnittfläche zwischen den klassischen Aufgabenbereichen innerer Sicherheit sowie den Kriegs- und Friedensaufgaben des Katastrophenschutzes" (Kaufmann 2011: 102). Diese Zusammenführung verändert auch das Dispositiv innerer Sicherheit. Verschiedenste Abhängigkeiten fallen ins Auge, wenn unterstellt wird, dass sämtliche Infrastrukturen (Energie, Trinkwasser, Transportwege usw.) gefährdet sind, egal ob „physikalisch, virtuell, geographisch [oder] logisch" (ebd.: 112). Diese Abhängigkeiten sind nicht von umfassender Digitalisierung zu trennen, insbesondere da „Informationsinfrastrukturen als Infrastrukturen von weiteren Infrastrukturen gelten" (ebd.: 105).[1] Tendenziell wird alles als bedroht imaginiert. Die Gesellschaft gilt als verletzlich. Die politischen Sicherheitsstrategien richten deshalb den Blick in die Zukunft. Bereits in den 1980er Jahren wird eine „'vorbeugende Bekämpfung' von Straftaten" (Pütter et al. 2005) in deutsche Polizeigesetze übernommen. Unter dem Leitbild der *Prävention* finden weitere tiefgreifende Veränderungen statt. Präventionsmaßnahmen geben sich nicht mehr bloß mit einer Interpretation zufrieden, sondern entwerfen eine Zukunft, die sie dann in die gewünschte Richtung zu beeinflussen suchen. Ob diese Vorstellungen der Realität nahekommen, ist irrelevant. Politisch entscheidend ist vielmehr, „welche Konsequenzen sie zeitigen" (Krasmann 2011: 53). Dazu gehört zweifellos, dass Menschen mittels einer Präventionslogik regiert werden, die nicht nur ihr Bewusstsein prägt, sondern auch bestimmte Alltagspraktiken hervorbringt (ebd.). Der Prävention wird auch die Unschuldsvermutung, die das bürgerliche Recht auszeichnet, geopfert: Alle Daten müssen zur Verfügung stehen, weil alle verdächtig sind (Opitz 2008: 223). Mit dem Blick in die Zukunft und dem damit verbundenem *predictive policing*, dem Versuch Verbrechen mittels Statistik und umfassenden Sozialdaten zu Leibe zu rücken bevor sie begangen werden, verän-

1 In der Sicherheitssparte des aktuellen europäischen Forschungsrahmenprogramms Horizon 2020 gehen der Schutz kritischer Infrastrukturen und Cybersecurity Hand in Hand (Europäische Kommission 2016). Auch das Konzept zur zivilen Verteidigung der Bundesregierung nennt Cyberangriffe als ernsthafte und wahrscheinliche Bedrohung. Das Internet gilt als *die* kritische Infrastruktur und wird mit fortschreitender Digitalisierung (Internet der Dinge, Industrie 4.0 etc.) auch in Sicherheitsfragen noch an Relevanz gewinnen.

dert sich der gesellschaftliche Umgang mit Zeit grundlegend. Während bisher Erfahrungen aus der Vergangenheit als Orientierung für ein Handeln in der Gegenwart dienten, wird heute die Gegenwart zunehmend unter der Imagination einer düsteren Zukunft umstrukturiert.

Das Forschungsprojekt INDECT

Rationalitäten wie die der Prävention schreiben sich in vernetzten Praktiken und Technologien ein (Krasmann/Opitz 2007: 133). Die gesellschaftliche Realität ist ihrerseits aber auch „immer schon der Effekt von Technologien der Erfassung, Auswertung und Verarbeitung von Daten" (ebd.: 136). Der „Präventionsstaat" (Krasmann 2011) steht mit seiner technischen Praxis auf dem Boden „des elektronischen Zeitalters und dieser Wandel ist irreversibel" (Rauer 2012: 87). Dabei besteht eine Koevolution von Technologien und Diskursen innerhalb des Dispositivs (vgl. Krasmann/Opitz 2007: 133ff.).

Zeitgenössische Sicherheitstechnologien sollen Polizeien und Geheimdiensten ein möglichst optimales Lagebild verschaffen und den Schritt zu einer *proaktiven*, also nicht nur vorausschauenden, sondern voraushandelnden Praxis erleichtern. Der Begriff des Dispositivs zeigt an, dass sich via *Securitization* illiberale Regierungsweisen in Techniken einschreiben und so eine eigenständige Materialität bekommen (Opitz 2008: 218). Für eine vernetzte Sicherheit sind vernetzte Technologien nötig. Überwachung ist heute dementsprechend komplex und verwoben; es geht um Daten und Metadaten (Bauman u.a. 2014: 123). Neben eher klassischen Technologien, wie Kameras oder der Telekommunikationsüberwachung (TKÜ) sind neue, wie Data-Mining[2] und Mustererkennung, getreten. Letztere basieren auf Software, deren Einsatz auch die klassischen Techniken stark verändert. Die IKT-Entwicklung hat so Massenüberwachung erst ermöglicht (Marx 2011: 91); andererseits ist Technik immer von sozialen Prozessen mitbestimmt (Lyon 1994: 54). Technischen Systemen liegen aber nicht nur gesellschaftliche Verhältnisse zugrunde, sondern sie „produzieren eine politische Wirklichkeit, bilden bestimmte historisch bedingte Sinnzusammenhänge ab und heben diese in Versprechen technischer Funktionalität auf" (Hempel 2011: 129).

INDECT (*Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment*) wurde im Zuge

2 Data-Mining bedeutet, Informationen aus den Untiefen des Internets zu Tage zu bringen und mittels Statistik, Muster und Zusammenhänge aus großen Datenmengen zu gewinnen.

des siebten Forschungsrahmenprogramms (FP7) der EU durchgeführt. In der Sparte „Sicherheit der Bürger" lief es von 2009 bis 2014 und hatte ein Budget von knapp 15 Millionen Euro, wovon knapp 11 Millionen von der EU kamen (CORDIS n.d.c). An dem Projekt beteiligen sich 17 Institutionen aus neun Staaten, darunter elf Universitäten, vier Privatfirmen und zwei Polizeien als potenzielle Endnutzer (INDECT n.d.b)[3]. Es befasste sich mit der Bündelung unterschiedlicher Überwachungstechnologien zur computergestützten, proaktiven Verbrechensbekämpfung. INDECT verfolgte eine zweigleisige Strategie, im Rahmen derer die städtische und die virtuelle Umwelt (v.a. Internet) überwacht werden soll (INDECT n.d.b). Dazu wurde an einem integrierten Informationssystem geforscht, das Bedrohungen präventiv bearbeiten sollte, um so die Polizeiarbeit zu unterstützen (CORDIS n.d.b). Schwerpunkt des Projekts war, in städtischen Umgebungen Video- und Audiodaten mit dem Zweck zu erheben, Bedrohungslagen und kriminelles Verhalten durch Mustererkennung automatisch zu identifizieren. Um gefährliche Situationen und „abnormales Verhalten" näher zu bestimmen, wurden zu Beginn des Projekts Polizeikräfte aus Nordirland und Polen befragt (CORDIS n.d.c). Als Verdachtsmomente für die Erhebung galt, wenn Autos auf Straßen beschleunigt werden, Menschen auf öffentlichen Straßen rennen, in öffentlichen Verkehrsmitteln auf dem Boden sitzen, sich häufig umsehen (ob sie beobachtet werden) oder sich länger an einem Platz aufhalten (INDECT n.d.a: 16ff.). Auch Menschenansammlungen werden als Verdachtsmomente behandelt, sobald eine bestimmte kritische Anzahl von Personen an einem Ort auftaucht (INDECT 2012: 26). Parallel wurde, insbesondere durch die beteiligte Universität York, an konstanter Überwachung von Internetressourcen (*Monitoring*), *Relationship-Mining*, *Social Network Analysis* (University of York n.d.a) sowie an einer semantischen Suchmaschine geforscht (University of York n.d.b). Hinzu kamen Werkzeuge zur Observation mobiler Objekte (Drohnen) und eine neuartige Suchmaschine für Bilddaten (CORDIS n.d.a; vgl. Rauer 2012). In INDECT wurde versucht, das ganze Spektrum zeitgenössischer Sicherheitstechnologie zusammenzuführen. Dementsprechend war zentraler Gegenstand des Projekts, unterschiedliche Datensorten, wie Videos, Texte oder biometrische Daten (Fingerabdrücke, Bewegungsmuster) technisch zu bündeln und bearbeitbar zu machen.[4]

---

3 Im *End Users Requirements Board* erweiterte INDECT gegen Ende des Projekts den Kreis beteiligter Polizeien auf Vertreter von insgesamt neun Staaten (CORDIS 2016).

4 INDECT war ein sehr anwendungsorientiertes Forschungsprojekt und hat angeblich über 50 „funktionierende Prototypen" (CORDIS 2016) entwickelt. Darunter befindet sich Software zum Prozessieren verschiedener Datensorten und zum Auffinden verdächtiger Websites, zahlreiche Tools zur Audio- und Videoanalyse, Gefahrenerkennung und

Das INDEC-Projekt zeichnet letztlich aus, dass Überwachung des öffentlichen Raums und Internet-Monitoring nicht getrennt voneinander behandelt werden, sondern dass beide Dimensionen miteinander vernetzt und integriert werden. Situationen im öffentlichen Raum sollen unter Einbeziehung von Erkenntnissen aus dem Internet oder Datenbanken beurteilt und kategorisiert werden. Durch die Kombination technologischer Strategien verknüpfte INDECT somit disziplinare und gouvernementale Rationalitäten, indem es Monitoring, Kameras und Datenbanken zusammenführte.

Gouvernementale und disziplinare Technologien

Das Internet wird zunehmend zum Terrain staatlicher Sicherheit. Dabei herrscht die schillernde Auffassung vor, das Internet als einerseits gefährdet und andererseits selbst als Gefährdung zu verstehen – nicht nur bei INDECT. Polizeien und Geheimdienste vernetzen sich mit Unternehmen wie Facebook und Google (Monroy 2015a). Europol klagt über verschlüsselte Kommunikation und strebt seinerseits Kooperationen an, um „Zugang zur Kommunikation jener Personen zu bekommen, die unsere Gesellschaft beschädigen wollen" (ebd.). Das können Kriminelle, vermeintliche Terrorist_innen oder auch Fluchthelfer_innen sein (Monroy 2015b).[5] Zudem beteiligt sich Europol im Rahmen von Horizon 2020 an Forschungen zur „Auswertung offener Quellen im Internet" (Monroy 2016a), also Data-Mining. 2015 wurde die *European Union Internet Referral Unit* (EU IRU), eine Meldestelle für Internetinhalte, ins Leben gerufen, vor allem um soziale Medien zu überwachen, da jihadistische Gruppen dort Nachwuchs rekrutieren und Gewalt propagieren (Europol 2015). Mit der EU IRU soll die Zusammenarbeit staatlicher Stellen mit großen Internetunternehmen weiter institutionalisiert und technisch umgesetzt werden. Neben automatisierter Bilderkennung nutzt die Stelle auch ein zentrales Register, um Internetseiten aufzulisten, bei denen bereits Verstöße gemeldet wurden (Monroy

---

Entscheidungsfindung sowie Drohnen zur weitgehend autonomen Verfolgung verdächtiger Objekte (ebd.). Insgesamt wurden zu den Forschungen über 400 Artikel veröffentlicht. Einige Ergebnisse wurden „erfolgreich" von Polizeikräften getestet. Als Nachfolgeprojekt ist unter anderem ein Spin-off-Unternehmen zur kommerziellen Vermarktung der Ergebnisse angedacht (CORDIS 2016).

5 Auch spanische Forscher von INDECT haben das Internet als besonders kriminellen Ort erkannt: „Kriminelle nutzen immer öfter das Internet, um Verbrechen zu planen. Die Polizei muss deshalb mit wirkmächtigen Werkzeugen zum Aufspüren von Bedrohungen ausgestattet werden, um Verbrechen zu verhindern bevor sie begangen werden" (Gacimartín et al. 2010; Übers. CM).

2015b). Die Beispiele verdeutlichen eine zunehmende Kooperation zwischen staatlichen und privaten Akteuren und deren Interesse an „vorausschauender" Kriminalitätsbekämpfung.

Monitoring, also kontinuierliche Überwachung und systematisches Erfassen von Aktivitäten im Internet oder im öffentlichen Raum, ist ein gouvernementaler, massenkonstituierender Machttypus (vgl. Foucault 1999: 280). Bei der Korrelation verschiedener Daten und Prognostik geht es um eine „Anordnung der Dinge" (Foucault 2006: 150): Mit diesen Methoden versuchen Polizeien und Geheimdienste, Auffälligkeiten zu entdecken (vgl. Marx 2011: 88f.), Ordnung ins vermeintliche Chaos zu bringen und aus unstrukturierten Datenmassen mittels Informationsverdichtung nützliche Ressourcen werden zu lassen, zu fördern und abzubauen. Dabei spielt Statistik eine große Rolle, sie „stellt demographische Informationen bereit, die eine bestimmte Form von administrativer Kontrolle nach sich ziehen" (Opitz 2004: 50). Die Begriffe, die nach Foucault im Rahmen der gouvernementalen Sicherheitsdispositive wichtig werden – Fall, Risiko und Gefahr (Foucault 2006: 94f.) – sind davon nicht zu trennen. Es geht um Vorhersagen und Messungen (Foucault 1999: 284). Migration von Arbeitskräften beispielsweise ist für den zeitgenössischen Kapitalismus in Europa notwendig. Eine unkontrollierte Zuwanderung läuft Standortinteressen jedoch entgegen. Ähnliches gilt für Datenströme: Sie müssen fließen, da sie nicht nur ökonomisch relevant sind, sondern auch Sicherheitsbehörden ein komplexes Lagebild bieten, dass von den Nutzer_innen selbst gezeichnet wird. Werden soziale Medien zur Fluchthilfe und für die Koordinierung unregulierter Grenzübertritte genutzt, besteht aus Perspektive gouvernementaler Sicherheit Handlungsbedarf, sobald ein kritischer Wert überschritten wird. Das permanente Scannen auf verdächtigen Inhalt und brisante Verbindungen bedeutet eine Verstaatlichung des Internets im foucaultschen Sinne (vgl. Demirović 2008: 9f.).

Die populärste und zugleich am häufigsten kritisierte Technologie, die mit innerer Sicherheit assoziiert wird, sind Überwachungskameras, die nicht nur bei INDECT eine zentrale Rolle spielen. Mittels Kameras breitet sich das panoptische Prinzip in die Gesellschaft aus (Lyon 1994: 63). Die technische Entwicklung führt derweil zu kleineren, mobileren, hochauflösenden, schwenkbaren und lichtempfindlicheren Kameras, die ein engmaschiges Netz bilden und zusätzlich mit anderen Technologien (Datenbanken, Mikrofone) verbunden werden können (s.o.). Die Herstellung eines permanenten Sichtbarkeitszustandes (Foucault 1977: 258) soll tendenziell flächendeckend hergestellt werden. So werden dem an sich statischen Konzept des Panoptikums dynamische Qualitäten verliehen. Durch Digitalisierung kommen Techniken der Bild- oder Mustererkennung, der biometrischen Identifizierung sowie die Möglichkeiten der Objektverfolgung in

Kamerabildern hinzu. Damit einher geht „die Möglichkeit einer detaillierten Kontrolle und pünktlichen Intervention" (ebd.: 206). Universitäten, andere Forschungseinrichtungen, Unternehmen und Polizeien arbeiten in zahlreichen Projekten sogenannter intelligenter Videotechnik (Monroy 2016b). Im Zentrum der Bemühungen steht dabei meist, verdächtige Personen, Verhaltensweisen oder Gegenstände zu identifizieren, „ohne dass die anfallenden Videoströme permanent von menschlichen BedienerInnen beobachtet werden müssen" (ebd.).[6] Allein das Bundesministerium für Bildung und Forschung (BMBF) fördert Forschungsprojekte zur Mustererkennung mit Millionenbeträgen (Bundesregierung 2013). Neben Algorithmen der Mustererkennung sind mit Kameras verknüpfte Datenbanken unerlässlich, beispielsweise zur Identifizierung von Menschen durch Gesichtserkennung. Während Kameras oft noch sichtbar sind, gehört es zum Wesen der Datenbanken, unsichtbar zu sein (Hempel/Metelmann 2005: 13). Sie dienen der Speicherung und Kategorisierung von personenbezogenen und sonstigen Daten und werden von unterschiedlichsten Institutionen verwaltet und genutzt. Kameras überwachen nicht länger anonyme Subjekte, sondern identifizierbare Personen (Cameron 2005: 108). Mit einer Vielzahl von vernetzten Datenbanken scheint zugleich der Idealfall des „nie abzuschließende[n] Dossier[s]" (Foucault 1977: 291), wie er von der Disziplinarmacht angestrebt wird, möglich. Beim Rückgriff auf die Panoptikum-Metapher steht oft der kontrollierende Blick im Zentrum. Was hingegen meist unter den Tisch fällt, ist die Kategorisierung durch die Macht (beispielsweise in Risikostufen) (Lyon 2005: 25). Kategorisierung und Klassifikation zeigen die Relevanz von Datenbanken voller personenbezogener Informationen, die zum Teil völlig belanglos erscheinen, bis sie in Beziehung gesetzt werden (Cameron 2005: 118). Dies geschieht, indem Informationen entlang von bestimmten Kategorien geclustert werden, die wiederum in einen statistischen oder algorithmischen Zusammenhang gebracht werden. Datenbanken ergeben nur dann Sinn, wenn die gespeicherten Informationen auch systematisch nutzbar sind. Weil aber so unterschiedliche Datensorten (Bilder, Telefonnummern, biometrische Daten etc., vgl. Hempel 2011: 135) nebeneinanderstehen, ist eine semantische oder graphische Datenaufbereitung besonders wichtig. Um die Datenbanken durchsuchen zu können, wird deshalb intensiv zu Suchmaschinen gearbeitet (vgl. INDECT n.d.a.; Europäische Kommission 2016). Liegen einmal alle Informationen in digitaler Form vor, ist die Verknüpfung und integrierende Nutzung verschiedener Daten ein lösbares Problem.

6 Auch bei INDECT war diese erhoffte Entlastung ein wichtiges Motiv.

Die Beispiele zeigen, dass das Dispositiv innerer Sicherheit gegenwärtig durch die Integration unterschiedlicher Technologien charakterisiert wird (vgl. Rauer 2012: 82f.; Europäische Kommission 2016).[7] Im sogenannten Informationszeitalter ist die Grenze zwischen Kommunikation und Überwachung jedoch unscharf geworden (Marx 2011: 85), da bei digitaler Kommunikation und IKT fast zwangsläufig Datenspuren hinterlassen werden, die sich auch zu Kontrollzwecken nutzen lassen (vgl. Bigo 2008: 109). Die Polizei nutzt soziale Medien (facebook, Twitter etc.), fast jedes Mobiltelefon verfügt über eine hochauflösende Kamera und fungiert als Peilsender. Die Digitalisierung geht so mit einer Konvergenz unterschiedlicher Technologien einher. Darin begründet sich auch der „Zugriff auf die Zukunft" (Hempel/Metelmann 2005: 12), dem technischen Äquivalent zur vorbeugenden Präventionslogik in der Sicherheitspolitik (s.o.). So werden disziplinare und gouvernementale Logiken integriert, das heißt, die Bevölkerung als Ganzes *und* das einzelne Individuum werden überwacht. Der Dispositivcharakter der inneren Sicherheit bei Projekten wie INDECT zeigt sich in der Vernetzung der Datensätze, da das eigentliche Novum in der Interaktion der mehr oder weniger bereits bekannten Einzeltechnologien liegt. Bei der Sicherheit wird an einer Verschränkung von virtueller und realer Welt gearbeitet, ganz ähnlich wie bei der industriellen Produktion unter dem Schlagwort Industrie 4.0.

Um das Verhältnis von Sicherheitsdiskurs und Technologien zu verstehen, lohnt ein Rückgriff auf die Akteur-Netzwerk-Theorie (ANT). Diese geht davon aus, dass soziale Praxis immer von Artefakten mitbestimmt wird (Degele 2002: 139) und Technik als Stabilisator sozialer Verhältnisse fungiert (Latour 1991). Im Zentrum von ANT steht der Gedanke, dass sich soziale Praxis ausdehnt und verfestigt, auf Dauer gestellt wird und nicht mehr so einfach hinterfragt werden kann. Durch die *Delegation* von Handlungen an und *Inskription* von Diskursen in technische Artefakte entstehen *hybride* Akteure, die sich aus Menschen und Technik zusammensetzen.[8] Polizeiliche Praktiken und Sicherheitsdiskurse werden in Technologien überführt. Dadurch gewinnen diese an Handlungsmacht und objektivieren auch implizite Strategien von Akteuren und Bedrohungssze-

7 „In naher Zukunft wird die beste Strategie für die Informationsgewinnung aus Kommunikationsdaten, um Terrorismus zu begegnen, Krisen zu managen und in Gefahrenlagen zu agieren, darin liegen, die Vorzüge künstlicher Intelligenz, Biometrie im weiteren Sinn und IKT mit menschlicher Erfahrung zu kombinieren." (INDECT 2009: 38; Übers.: C.M.)

8 Die Idee der Inskription ist bereits bei Foucault angelegt, wenn er in Bezug auf Benthams Panoptikum von der Institutionalisierung des ärztlichen Blicks und dessen Einschreibung in den Raum spricht (Foucault 2003: 250).

narien (Hempel 2011: 125). Technik ist aber weder allmächtig, noch neutrales Werkzeug, vielmehr verändert sie Handlung und Kontext (ebd.). Wenn Mensch und Technik verschmelzen, entsteht ein Hybrid und es ändert sich mitunter auch das eigentliche Ziel der Technik und der polizeilichen Praktiken (ebd.: 216f.). Die Kamera zum Beispiel sollte nur aufnehmen, was ihr vor die Linse kommt, der Polizist wollte nur Verdächtige kontrollieren, aber der Hybrid-Akteur kontrolliert alle, die vor die Linse kommen und behandelt sie als verdächtig. Foucault beschreibt die Disziplinarmacht immer wieder als Maschine, die unabhängig vom Überwachungspersonal funktioniert und damit unpersönlich wird (Foucault 1977: 229). In den hier vorgestellten Projekten wird die Macht buchstäblich zur Maschine und „[e]s sind nicht die menschlichen Akteure, die eine Gefahr definieren, sondern es sind maschinelle Praktiken" (Rauer 2012: 85f.). Diese hochtechnisierte Praxis innerer Sicherheit wird auch als *Technopolicing* bezeichnet (Lyon 1994: 113). Der Versuch mittels nicht-menschlicher Akteure gesellschaftliche Ordnungen auf Dauer zu stellen, ist nicht unproblematisch und ruft immer „neue Unschärfen und Kontingenzen" (Rauer 2012: 71) hervor. Neben dem Problem des „categorial suspicion" (Lyon 1994: 113), sieht Lyon Paradoxa bei der Abhängigkeit der Polizei von Daten, die den Anschein der Objektivität erheben, sobald sie auf Bildschirmen erscheinen (ebd.). Subjektive Urteile gelangen beispielsweise über Freitextfelder in Datenbanken und werden von da an nicht mehr hinterfragt. Bei INDECT war geplant, Hinweise aus der Bevölkerung über ein sogenanntes Portal aufzunehmen und diese dann der Polizei für ein komplexeres Lagebild zur Verfügung zu stellen. Das Dispositiv der inneren Sicherheit verändert sich so durch den Einsatz digitaler Technologien. Es wäre jedoch falsch, von einem bloßen Technikdeterminismus auszugehen.

Innere Sicherheit im Neoliberalismus

Der inneren Sicherheit kommt im Rahmen neoliberaler Politik eine zentrale Rolle zu, denn ein wichtiger Aspekt ist die Verlagerung von sozialer auf innere Sicherheit. Das zeigt sich bei der Struktur des öffentlichen Budgets (Butterwegge 2007: 189; vgl. Wacquant 2012). Permanent werden Ausschlüsse wie Arbeitslosigkeit, Wohnungslosigkeit oder Illegalisierung produziert (Kannankulam 2008: 417), wobei die Ausgeschlossenen im neoliberalen Präventionsstaat per se als deviant stigmatisiert werden und unter Kontrolle gehalten werden müssen (ebd.: 421). Sie erfahren die harten Aspekte ausschließender und bestrafender Überwachung (Lyon 1994: 61). Neoliberalismus und Gouvernementalität erschöpfen sich damit nicht in Strategien der Selbstregierung und -optimierung – zumindest nicht für die Subalternen. Der Rückgriff auf Repression stellt im

Kapitalismus immer eine Option dar, rückt aber „in Zeiten der Krise vermehrt in den Vordergrund" (Buckel/Kannankulam 2002: 5). Es stellt sich in diesem Kontext die Frage, vor wem die Gesellschaft geschützt werden muss und wer dazugehört. Die Gefahr scheint jedenfalls von außen zu drohen, etwas Fremdes zu sein.[9] Die Ausgeschlossenen selbst gelten nicht als Teil der schützenswerten Gemeinschaft, sondern sind „Repräsentationen der Unsicherheit" (Krasmann/Opitz 2007: 143) und werden oft „entlang der Kategorien Alter, Geschlecht, soziale Herkunft, ethnischer Hintergrund und Wohnumfeld unterschieden" (Stenson 2007: 184). Diese Rasterung geht einher mit einer sinkenden Toleranzschwelle gegenüber kleinen Störungen der öffentlichen Ordnung, etwa Ruhestörung durch Jugendliche (ebd.). Bei vielen der neuen Sicherheitstechnologien entscheiden Algorithmen, wer genug Risikomerkmale oder Verdachtsmomente auf sich vereint und einer weiteren Überprüfung bedarf (vgl. INDECT 2010: 41; INDECT n.d.a: 23ff.).

Durch Sozialabbau weiten sich Phänomene des Ausschlusses tendenziell aus. Den Folgen stellt sich der Sicherheitsstaat als neuer starker Staat, der die in Bewegung gesetzte Gesellschaft aufmerksam im Auge behält, damit nichts aus dem Ruder läuft. Auf staatlicher Ebene herrscht eine „funktionale Verknüpfung" (Wacquant 2012: 680) von Deregulierung und Autorität, die auf eine Kriminalisierung von Armut hinausläuft (ebd.).[10] Nicht zuletzt werden in dieser Logik Kameras programmiert, die auf dem Boden sitzende Personen als verdächtig markieren und die Polizei alarmieren (vgl. Monroy 2016b). Liberalisierung von Markt und Sozialpolitik führt zu steigenden Spannungen und sinkender Legitimität des Staates. Ein autoritärer Staat antwortet auf beides (Wacquant 2012: 692f.).

Staatliche Sicherheitsapparate werden seit den Krisen der 1970er Jahre ausgebaut (Dawson 2011). Die Studie *Policing The Crisis* (Hall u.a 1982) zeigt, wie im Rahmen der starken Rezession in den 1970ern Schwarze Arbeitnehmer_innen in Großbritannien auch zu den ökonomisch am stärksten unterdrückten werden und es zu einer „Synchronisierung der ethnischen und klassenbezogenen Aspekte der Krise" (ebd.: 332, Übers.: C.M.) kommt. Ab 1974 setzt in Großbritannien

9 Nicht zufällig fallen in neu-rechtem Denken imaginierte Bedrohungen der Bevölkerung durch etwas ihr Äußerliches oder Fremdes (EU, Migration, Wertewandel) mit dem Einfordern eines starken Staates, der für Recht und Ordnung sorgt und davor schützt, zusammen.

10 Beispiele finden sich zuhauf: sogenannter Warnschussarrest, Intensivtäter-Debatte oder Vertreibung von Obdachlosen aus Innenstädten, Hartz IV-Gesetzgebung; bei letzteren zeigt sich auch das produktive „Prinzip des Nicht-Müßiggangs" (Foucault 1977: 197) der Disziplinarmacht.

eine regelrechte Hetze gegen Migrant_innen ein, die sich sehr ähnlicher Topoi – Flutmetapher, „Sozialschmarotzer" etc. – bedient, wie die in Deutschland Anfang der 1990er Jahre und heute in weiten Teilen Europas stattfindende (vgl. ebd.: 335). Hall u.a. identifizieren Rassismus und verschärften Klassenkampf als direkte Krisenfolgen, in denen ausgehandelt wird, wer die Lasten zu tragen hat. Auch diese Zuspitzung bleibt nicht ohne Konsequenzen: „Krisen müssen behoben, ihre schlimmsten Effekte abgemildert werden. Sie müssen zudem unter Kontrolle gebracht werden. Um es direkt zu sagen, sie müssen polizeilich beantwortet werden" (ebd.: 339; Übers.: C.M.). Dabei dient ein „autoritärer Konsens" (ebd.) als gesellschaftliche Basis. Ausgrenzung im Namen der Sicherheit wird von der Mehrheit akzeptiert, da (wie bei *Securitization*) die zu schützende Bevölkerung als Ganzes angesprochen und einbezogen wird. Dabei werden die Ränder der Gesellschaft „abnormalisiert", um die Sicherheit der statistisch gesehen „normalisierten" Mehrheit zu schaffen. Es entsteht eine Dynamik, die ständig neue (Un)Sicherheit (Bigo 2008: 108) und Ausschlüsse produziert. Der Sicherheitsdiskurs produziert so eine imaginäre Zukunft der Homogenität, in der es keine Randgruppen, Widersprüche und Kämpfe mehr gibt und die er umzusetzen versucht.

Angesichts der Aufstände von Tottenham im August 2011 (vgl. PROKLA 175) zeigt sich, dass die Studie mit den Jahren nichts an Aussagekraft eingebüßt hat (vgl. Dawson 2011). Wenn während und nach den Aufständen Verdächtige mittels Formen digitaler Überwachung überführt werden, beispielsweise durch die Veröffentlichung von Kamerabildern in sozialen Medien, kombiniert mit Aufrufen zur Denunziation, ist das der aktuelle Ausdruck des „autoritären Konsenses". Die Londoner Polizei bemüht sich seither verstärkt darum, sich unter Zuhilfenahme sozialer Medien ein Lagebild zu verschaffen (vgl. Metropolitan Police Service 2012). Abwechselnde Phasen von „more than usual alarm" und „more than normal control" (Hall u.a. 1982: 185f., Afz. i.O.) tauchen meist in Zeiten tiefgreifender sozialer Unruhen, ökonomischer Krisen und historischer Brüche auf (ebd.). Die historische Formation samt ihren hegemonialen Verhältnissen, die Hall u.a. untersuchen und die bis heute andauert, nennen sie „post *laissez-faire* Welfare State form" (ebd., Herv. i.O.). In dieser sind die Innenministerin und sonstige mit Sicherheitsfragen Betraute stets darum bemüht, weitere Diskursverschiebungen zu erreichen. Sie initiieren Panikdynamiken und beantworten sie unter Rückgriff auf Zuschreibungszyklen, welche meist die stigmatisierende Zusammenführung von Begriffen enthalten („convergence") (ebd.). Dabei werden negativ konnotierte Begriffe mit an sich unproblematischen verknüpft, um auch diese mit einer Bedrohung zu assoziieren (ebd.). Beispiele für solche Zusammenführungen sind „islamischer Terrorismus" oder „Internetkriminalität". Der Islam

und das Internet werden so zum Gegenstand polizeilichen Handelns. Aktuell wird mit dem Begriff der „Schleuserkriminalität" und der Bedrohung durch angeblich eingewanderte Djihadist_innen, Migration als Sicherheitsproblem gelabelt. Letztendlich beschreibt die Studie von Hall u.a. nicht nur anschaulich, wie es zu *Securitization* und proaktiver Polizeiarbeit kommt, sondern gibt auch Aufschluss darüber, wie mit Stereotypen Politik der inneren Sicherheit betrieben wird. In den heutigen Technologien steckt die jüngere Geschichte der Sicherheitsstrategien und Polizeiarbeit. In ihnen ist die Beantwortung der erzeugten Paniken objektiviert.

Seit dem 11. September 2001 haben sich Sicherheitsdiskurse weiter verschärft und es ist davon auszugehen, dass diese Entwicklung nach den jüngeren Anschlägen in Europa anhält. Die Technologien, die seither eingesetzt werden (vgl. Cameron 2005: 115), vereinen Elemente disziplinarer und gouvernementaler Macht und verändern diese. Mittels „intelligenter" Kameras ist der panoptische Blick nicht mehr an geschlossene Institutionen gebunden. Die Disziplinen „deinstitutionalisieren" (Foucault 1977: 271, Anfz. i.O.) sich somit auch in ihrer restriktiven Ausprägung. Gouvernementalität und Disziplin stehen jetzt in einem neuen Verhältnis. Während sich die gouvernementale Sicherheit ursprünglich gegenüber der Disziplinarmacht durch eine gewisse Distanz zum Objekt auszeichnete, und es nicht mehr darum ging, die Überwachungsmethoden auszuschöpfen und die Beherrschten für den Souverän ständig sichtbar zu halten und gefügig zu machen (Foucault 2006: 102f.), bemühen sich Projekte wie INDECT um kleinteilige Überwachung und permanente Sichtbarmachung durch modernste Kommunikationstechnologien. Die vielleicht wichtigste Neuheit ist, dass die Individuen selbst wieder verstärkt von Interesse sind, um etwas über die Bevölkerung zu erfahren (vgl. Foucault 2006: 69f.). Diese zukunftsorientierte, technologiebasierte Sicherheit ist dann etwas anderes als Disziplin: „Überwachung ist nicht das gleiche wie Disziplin. Foucault hat nicht verstanden, dass Überwachung das vereint, was er mit der Differenzierung von Sicherheit auf der einen und Disziplin auf der anderen Seite getrennt hat" (Bigo 2008: 109; Übers.: C.M.). An Bigo anschließend ließe sich also sagen, es liegt in der Natur der Sache, dass Überwachung und deren Technologien, Disziplin und Sicherheit vereinen. Die einzelnen Technologien verkörpern zwar unterschiedliche Machttypen. Sie wirken aber alle zusammen und ergänzen sich. Die gouvernementale Totalerfassung, Statistik und Suche nach Normabweichungen, wird teilweise zur Voraussetzung disziplinarer Einzelüberwachung. Dennoch kann gouvernementale Statistik „mit einer Katastrophe umgehen aber nicht mit dem Armageddon" (Bigo 2008: 112; Übers.: C.M.; vgl. Kaufmann 2011: 109). Spätestens seit 9/11 ist deshalb jeder Einzelfall wieder von Interesse, weil im Worst-case-Denken jedes einzelne aus dem

Ruder gelaufene Individuum Schaden von gesellschaftlich relevantem Ausmaß anrichten kann. Ein Sicherheitsdenken des Laissez-faire kann es damit nicht mehr geben, sondern Elemente der Disziplinarmacht müssen eine panoptische Situation bis in die Ritzen der Gesellschaft etablieren, um wenigstens die Illusion von Schutz gegen das Unbekannte aufrechtzuerhalten, „gegen die Atombombe im Rucksack" (ebd.). Durch den technischen Fortschritt ist das Panoptikum ohne Einsperrung nicht länger Science-Fiction und Dystopie, sondern tatsächlich möglich. Dennoch lässt sich die Gesellschaft nicht zur Disziplinaranstalt umbauen. Verkehr, Handel, Mobilität und Datenaustausch müssen möglich sein. Deshalb bestehen liberale Elemente der Gouvernementalität weiter, die sich jedoch weitgehend auf die Ökonomie im engeren Sinn beschränken, während bürgerliche Freiheiten eingeschränkt werden oder zumindest nicht für alle gelten (vgl. Krasmann/Opitz 2007: 140).

Das Dispositiv innerer Sicherheit ist die Orchestrierung von Technologien, Diskursen, Praktiken, Gesetzen und Subjektivierungsweisen. Doch was sind die Probleme, auf die das Dispositiv der inneren Sicherheit antwortet? Sowohl Securitization, als auch deren technowissenschaftliche Verkörperungen sind „ihrer Herkunft nach Emergenzprodukte, die aus historischen Konstellationen hervorgegangen sind" (Richter 2011: 63). Die Situation, auf die sich die innere Sicherheit neu einzustellen versucht, ist geprägt von einer neoliberalen Formation und digitaler Technologie. Die angestrebte lückenlose Überwachung erinnert an die Pestverordnungen des 17. Jahrhunderts (Foucault 1977: 251f.). Doch jene beruhten auf Einschluss und einer Ausnahmesituation und galten nur für begrenzte Zeit. Heute ist die Überwachung räumlich und zeitlich entgrenzt. Die Disziplinarmacht ist damit wieder stärker in den Vordergrund getreten. Dafür gibt es vor allem drei Gründe: Erstens führt Neoliberalismus zu Ausschlüssen und sozialen Konflikten. Als Krisenfolgen müssen diese „policed" werden. Zweitens kann jeder Einzelfall relevant sein. Folglich müssen alle überwacht werden, um potenzielle Terrorist_innen oder Kriminelle herausfiltern zu können. Und drittens erlaubt der Stand der Technologie individuelle Überwachung auf gesellschaftlicher Ebene und das ohne Einsperrung. Dafür wird sowohl der öffentliche Raum wie auch das Internet überwacht. Letzten Endes können staatliche Akteur_innen de jure auf fast sämtliche Daten zugreifen, auch wenn sie von privater Seite erhoben wurden, seien es Kamerabilder von Verkehrsbetrieben oder Daten und Metadaten von Mobilfunkanbietern. Hinzu kommen zahlreiche Beispiele für direkte Kooperationen (vgl. Monroy 2016b; Hempel/Metelmann 2005). Daten werden also von verschiedensten Akteur_innen und auch zu unterschiedlichen Zwecken erhoben, doch werden sie mittels neuester Technologien, in Projekten wie INDECT, auf staatlicher Seite für polizeiliche

oder geheimdienstliche Zwecke wieder zusammengeführt. Es findet eine *Reintegration* verteilter Überwachung statt. Der Streit zwischen FBI und Apple um die Entschlüsselung eines Chatprotokolls war rühmliche Ausnahme und fand zudem außerhalb des europäischen Kontextes statt (vgl. Gruber/Reinhold 2016). Wo der Staat keinen Zugriff hat, bemüht er sich, die Informationslücken zu schließen (vgl. Monroy 2015a). Mit Technologien der inneren Sicherheit wird versucht, soziale Verwerfungen einzuhegen, kritische Milieus unter Kontrolle zu halten und unkontrollierte Migration einzuschränken. Sie sind dabei mitunter sehr kleinteilig und auf Hotspots wie Innenstädte, Infrastrukturen oder Grenzen beschränkt. Andererseits ist die Überwachung des Internets grenzenlos. Proaktive Sicherheitstechnologien antworten im Dienst einer autoritären Politik auf nationale wie internationale Krisenfolgen. Gesellschaftliche Widersprüche werden sie nicht beseitigen.

Literatur

Agamben, Giorgio (2008): *Was ist ein Dispositiv?* Zürich-Berlin.

Bauman, Zygmunt u.a. (2014): After Snowden: Rethinking the Impact of Surveillance. In: *International Political Sociology* 8(2): 121-44.

Bigo, Didier (2008): Security: A Field Left Fallow. In: Dillon, Michael/Neal, Andrew W. (Hg.): *Foucault on Politics, Security and War*. Basingstoke: 93-114.

Buckel, Sonja/John Kannankulam (2002): Bevölkerungsvermessung und Sicherheitsdispositive nach dem „11. September". In: *Das Argument* 244. ULR: links-netz.de/K_texte/K_buckel_sicherheit.html, Zugriff: 20.8.2013.

Bührmann, Andrea D./Werner Schneider (2008): *Vom Diskurs zum Dispositiv. Eine Einführung in die Dispositivanalyse*. Bielefeld.

Bundesregierung (2013): *Drucksache 17/13056. Antwort der Bundesregierung auf die kleine Anfrage der Abgeordneten Herbert Behrens, Andrej Hunko, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/12704 – Forschungen zum Einsatz automatisierter Mustererkennung und Biometrie zum Aufspüren von sogenanntem bedrohlichem Verhalten.*

Butterwegge, Christoph (2007): Rechtfertigung, Maßnahmen und Folgen einer neoliberalen (Sozial-)Politik. In: Lösch, Bettina/Ptak, Ralf (Hg.): *Kritik des Neoliberalismus*. Wiesbaden: 135-219.

Buzan, Berry u.a. (1998): *Security. A New Framework for Analysis*. London

Cameron, Heather (2005): The Next Generation. Visuelle Überwachung im Zeitalter von Datenbanken und Funk-Etiketten. In: Hempel, Leon/Metelmann, Jörg (Hg.): *Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels*. Frankfurt/M: 106-121.

CORDIS (2016): Final Report Summary – INDECT. URL: cordis.europa.eu/result/rcn/175782_de.html, Zugriff: 20.3.2016.

– (n.d.a): CORDIS Indect. URL: cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_LANG=EN&PJ_RCN=10374914&pid=52&q=FD8A9BBC079BD5FCECD584ADBD3CE6A7&type=adv, Zugriff: 2.7.2012.

– (n.d.b): Indect Periodic Report 12.10. URL: cordis.europa.eu/search/index.cfm?fuseaction=result.document&RS_LANG=EN&RS_RCN=11481605&q=FD8A9BBC079BD5FCECD584ADBD3CE6A7&pid=52&type=adv, Zugriff: 2.7.2012.

– (n.d.c): INDECT Sheet CORDIS. URL: cordis.europa.eu/fp7/security/fp7-project-leaflets_en.html, Zugriff: 2.7.2012.

Dawson, Ashley (2011): Policing the Crisis. URL: counterpunch.org/2011/08/11/policing-the-crisis/print, Zugriff: 14.12.2012.

Degele, Nina (2002): *Einführung in die Techniksoziologie*. München.

Demirović, Alex (2008): Das Problem der Macht bei Michel Foucault, *IPW Working Paper* 2/2008.

Europäische Kommission (2016): *Work Programme 2016-2017. 14. Secure Societies – Protecting Freedom and Security of Europe and Its Citizens* URL: ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf, Zugriff: 16.8.2016.

Europol (2015): Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda. URL: europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda, Zugriff: 29.8.2016.

Foucault, Michel (1977): *Überwachen und Strafen. Die Geburt des Gefängnisses*. Frankfurt/M.

– (1978): Ein Spiel um die Psychoanalyse. Gespräch mit Angehörigen des Département de Psychoanalyse der Universität Paris VIII in Vincennes. In: *Dispositive der Macht. Über Sexualität, Wissen und Wahrheit*. Berlin: 118-175.

– (1999): *In Verteidigung der Gesellschaft*. Frankfurt/M.

– (2003): Das Auge Der Macht. Gespräch Mit J.-P. Barou und M. Perrot. In: *Dits et Ecrits. Schriften 3*. Frankfurt/M: 250-271.

– (2006): *Sicherheit, Territorium, Bevölkerung. Geschichte Der Gouvernementalität I*. Frankfurt/M.

Gacimartín, Carlos u.a. (2010): On Detecting Internet-Based Criminal Threats with XplicoAlerts: Current Design and next Steps. In: *Universidad Carlos III de Madrid Papers*. URL: it.uc3m.es/~muruenya/papers/MCSS10XplicoAlerts.pdf, Zugriff: 22.10.2012.

Gruber, Angela/Reinhold, Fabian (2016): „Streit zwischen FBI und Apple. iPhone geknackt – Duell verschoben", spiegel.de (29.03.2016).

Hall, Stuart u.a. (1982): *Policing the Crisis. Mugging, the State, and Law and Order*. London-Basingstoke.

Hempel, Leon (2011): Das Versprechen der Suchmaschinen. Der europäische Sicherheitsraum als Sichtbarkeitsregime. In: Hempel, Leon u.a. (Hg.): *Sichtbarkeitsregime. Überwachung, Sicherheit Und Privatheit Im 21. Jahrhundert. Leviathan Sonderheft 25/2010*. Wiesbaden: 124-142.

Hempel, Leon/Metelmann, Jörg (2005): Bild – Raum – Kontrolle. Videoüberwachung Als Zeichen Gesellschaftlichen Wandels. In: Hempel, Leon/Metelmann, Jörg (Hg.): *Bild – Raum – Kontrolle. Videoüberwachung Als Zeichen Gesellschaftlichen Wandels*. Frankfurt/M: 9-21.

INDECT (2009): Evaluation of Components, D9.4 WP9. URL: project-indect.eu/, Zugriff: 31.8. 2012.

– (2012): D1.1. Report on the Collection and Analysis of User Requirements. URL: indect-project.eu/, Zugriff: 31.8.2012.

– (2010): D9.47. Report on the Outcomes of the First Conference Related to Security of Citizens in Urban Environment. URL: project-indect.eu/, Zugriff: 31.8.2012.

– (2009): D 9.4. Evaluation of Components WP9. URL: project-indect.eu/, Zugriff: 31.8.2012.

– (n.d.a): Deliverable 1.1 (alte Fassung). URL: files.piratenpartei.de/indect/INDECT_Deliverable_D1.1_v20091029.pdf, Zugriff: 22. 8.2013.

– (n.d.b): Welcome to INDECT Homepage. URL: indect-project.eu/, Zugriff: 2.7.2012.

Kannankulam, John (2008): Konjunkturen der inneren Sicherheit. In: *PROKLA* 38(3): 413-427

Kaufmann, Stefan (2011): Zivile Sicherheit: Vom Aufstieg Eines Topos. In: Hempel, Leon u.a. (Hg.): *Sichtbarkeitsregime. Überwachung, Sicherheit Und Privatheit Im 21. Jahrhundert. Leviathan Sonderheft 25/2010*. Wiesbaden: 101-123.

Krasmann, Susanne (2011): Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend akzeptiert werden. In: Hempel, Leon u.a. (Hg.): *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25/2010*. Wiesbaden: 53-70.

Krasmann, Susanne/Opitz, Sven (2007): Regierung und Exklusion. Zur Konzeption des Politischen im Feld der Gouvernementalität. In: Krasmann, Susanne/Volkmer, Michael (Hg.): *Michel Foucaults „Geschichte Der Gouvernementalität" in Den Sozialwissenschaften. Internationale Beiträge*. Bielefeld: 127-155.

Kunz, Thomas (2005): *Der Sicherheitsdiskurs. Die Innere Sicherheit und ihre Kritik*. Bielefeld.

Latour, Bruno (1991): Technik ist stabilisierte Gesellschaft. In: Belliger, Andrea/Krieger, David J. (Hg.): *ANThology. Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie*. Bielefeld: 369-397.

Lemke, Thomas (2007): Eine unverdauliche Mahlzeit? Staatlichkeit, Wissen und die Analytik der Regierung. In: Krasmann, Susanne/Volkmer, Michael (Hg.): *Michel Foucaults „Geschichte der Gouvernementalität" in den Sozialwissenschaften. Internationale Beiträge*. Bielefeld: 47-73.

Lyon, David (2005): Interview mit David Lyon: „Wir Haben gerade erst begonnen". Überwachen zwischen Klassifikation und Ethik des Antlitzes. In: Hempel, Leon/Metelmann, Jörg (Hg.): *Bild – Raum – Kontrolle. Videoüberwachung Als Zeichen Gesellschaftlichen Wandels*. Frankfurt/M: 22-32.

– (1994): *The Electronic Eye. The Rise of the Surveillance Society*. Cambridge.

Marx, Gary T. (2011): The New Surveillance. Some Concepts and Some Implications for Privacy and Stratification. In: Hempel, Leon u.a. (Hg.): *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25/2010*. Wiesbaden: 85-98.

Metropolitan Police Service (2012): 4 Days in August. Strategic Review into the Disorder of August 2011. URL: content.met.police.uk/cs/Satellite?blobcol=urldata&blobheadername1=Content-Type&blobheadername2=Content-Disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22145%2F595%2Fco553-114DaysInAugust.pdf%22&blobkey=id&blobtable=MungoBlobs&blobwhere=1283551523589&ssbinary=true, Zugriff: 17.9.2013.

Monroy, Matthias (2015a): „Dauerhaft Angespannte Bedrohungslage": Europol und Interpol wollen Verschlüsselung umgehen und Geheimdienstdaten verarbeiten, *Netzpolitik.org*, 7.5.2015. URL: netzpolitik.org/2015/dauerhaft-angespannte-bedrohungslage-europol-und-interpol-wollen-verschluesselung-umgehen-und-geheimdienstdaten-verarbeiten/, Zugriff: 6.6.2016.

– (2015b): Automatisiertes „Erkennen von Propaganda": Meldestelle für Internetinhalte bei Europol soll weiter wachsen, Netzpolitik.org, 22.9.2015. URL: netzpolitik.org/2015/automatisiertes-erkennen-von-propaganda-meldestelle-fuer-internetinhalte-bei-europol-soll-weiter-wachsen/, Zugriff: 6.6.2016.

– (2016a) Frankreich und Deutschland verabreden Sicherheitsforschung zu „gezielter Gewalt in Städten", Netzpolitik.org, 9.2.2016. URL: netzpolitik.org/2016/frankreich-und-deutschland-verabreden-sicherheitsforschung-zu-gezielter-gewalt-in-staedten/, Zugriff: 6.6.2016.

– (2016b): An Bahnhöfen lieber nicht rennen oder herumlungern: Bundespolizei erprobt Videoüberwachung mit Mustererkennung', Netzpolitik.org, 12.5.2016. URL:/netzpolitik.org/2016/lieber-nicht-rennen-oder-herumlungern-bundespolizei-erprobt-musterkennung-an-bahnhoefen/, Zugriff: 6.6.2016.

Opitz, Sven (2004): *Gouvernementalität im Postfordismus. Macht, Wissen und Techniken des Selbst im Feld unternehmerischer Rationalität*. Hamburg.

– (2008): Zwischen Sicherheitsdispositiven und Securitization: Zur Analytik illiberaler Gouvernementalität. In: Purtschert, Patricia u.a. (Hg.): *Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault*. Bielefeld: 201-228.

Pütter, Norbert u.a. (2005): Bekämpfungs-Recht und Rechtsstaat. Vorwärtsverrechtlichung in gebremsten Bahnen? In: *Cilip. Polizei & Bürgerrechte* 82: 6-15.

Rauer, Valentin (2012): Interobjektivität: Sicherheitskultur aus Sicht der Akteur-Netzwerk-Theorie. In: Daase, Christopher u.a. (Hg.): *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*. Frankfurt/M: 69-91.

Richter, Norbert Axel (2011): Foucaults Theorie Der Ordnung. In: Heidenreich, Felix (Hg.): *Technologien der Macht. Zu Michel Foucaults Staatsverständnis*. Baden-Baden: 53-65.

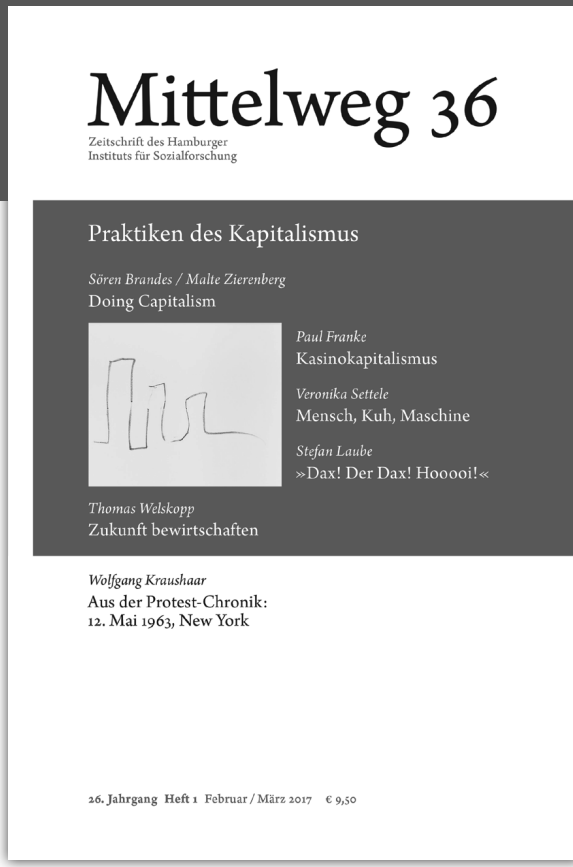
University of York (n.d.a): INDECT Home Page. URL: cs.york.ac.uk/aig/projects/indect/, Zugriff: 22.10.2012.

– (n.d.b): Suresh Manandhar's Home Page. URL: users.cs.york.ac.uk/~suresh/-Projects-.html, Zugriff: 22.10.2012.

Stenson, Kevin (2007): Staatsmacht, Biopolitik Und Die Lokale Regierung von Kriminalität in Großbritannien. In: Krasmann, Susanne/Volkmer, Michael (Hg.): *Michel Foucaults „Geschichte der Gouvernementalität" in den Sozialwissenschaften. Internationale Beiträge*. Bielefeld: 181-209.

Wacquant, Loïc JD (2012): Der neoliberale Leviathan. Eine historische Anthropologie des gegenwärtigen Gesellschaftsregimes. In: *PROKLA* 42(4): 677-698.

Alle Wissenschaft wäre überflüssig, wenn die Erscheinungsform und das Wesen der Dinge unmittelbar zusammenfielen. *Karl Marx*



Heft 1/2017, 108 Seiten

Praktiken des Kapitalismus

Print € 9,50– / E-Journal € 7,99

25 Jahre

Mittelweg 36

Zeitschrift des Hamburger
Instituts für Sozialforschung

www.mittelweg36.de