Bettina Paul und Simon Egbert

Zur Einführung in das Themenheft: Über den Mehrwert soziotechnischer Perspektiven für die Kriminologie

An introduction to the special issue: about the added value of sociotechnical perspectives for criminology

Viele kriminologisch relevante Praktiken – wie beispielsweise *predictive policing*, biometrische und Video-Überwachungssysteme – können als soziotechnische Interaktionen charakterisiert werden, da sie sich grundsätzlich aus einem Zusammenspiel von menschlichen und nicht-menschlichen Akteur_innen konstituieren. So wäre der präemptive[1] Wandel von Sicherheitspraktiken ohne die systematische Einbindung von technischen[2] Artefakten und Systemen gar nicht möglich bzw. durchsetzbar gewesen, da vorausschauende Sicherheitsstrategien auf Technologien zurückgreifen müssen, um gesellschaftlich akzeptierte Vorhersagen für die Zukunft erstellen zu können.

Die derzeitigen Kriminal- und Sicherheitspraktiken könnten in ihrer neuen Qualität (z. B. Hybridität) und hinsichtlich ihrer Genese, Praxis und Implikation umfassender analysiert werden, wenn – so die leitende Kernthese des vorliegenden Themenhefts – sich die Kriminologie um eine eingehende Be-

1 Unter Präemption verstehen wir jene Sicherheitspraktiken, die konkrete Kontroll- bzw. Überwachungsinterventionen auch dann schon beinhalten, wenn sich die zugrunde liegende Bedrohung noch nicht voll entfaltet hat bzw. deren Aufkommen räumlich und zeitlich noch nicht feststeht und lediglich eine Entstehungsmöglichkeit existiert (Massumi 2015: 9 ff.; Opitz 2012: 287 ff.; Amoore spricht deshalb auch von einer „possibilistischen" Logik, 2013: 12). Eine solche Neuorientierung präventiver Politiken wurde zwar bereits vor den Terroranschlägen vom 11. September 2001 beobachtet (z. B. Legnaro 1997: 276 f.; Lepsius 2004: 83), und doch ist sie seitdem deutlich verbreiteter und es wird gegenwärtig deutlich mehr auf (technologisch gestützte) Imaginations- und Prognosetechniken zurückgegriffen, um mögliche, kaum antizipierbare zukünftige Sicherheitsrisiken bereits in der Gegenwart bearbeiten zu können (vgl. a. McCulloch/Wilson 2016).

2 Unter dem Begriff „Technik" verstehen wir ein Instrument, das sowohl materialisiert – in Gestalt eines Artefakts – als auch virtuell – z. B. in Form einer Software oder eines Algorithmus – auftreten kann. Als „Technologie" wiederum werden darüber hinaus die mit Techniken zusammenhängenden Praktiken, Wissensbestände und gesellschaftlichen Kontexte begriffen (vgl. Lösch 2012: 252).

rücksichtigung der soziotechnischen Charakteristik bemühen und dafür auf die Annahmen der *Science and Technology Studies* (STS) beziehen würde.[3]

Kernannahmen der Science and Technology Studies

Die STS sind eine soziologische Denkrichtung, die sich im Kern damit auseinandersetzt, dass, *erstens,* Gesellschaft und Technologie untrennbar miteinander verbunden sind (s. z. B. Latour 2010; Bijker/Pinch 2012). Soziologie ist danach nicht nur das Studium der Gesellschaft, sondern jenes des „seamless web" zwischen gesellschaftlicher und technologischer Welt (Hughes 1986). Die Besonderheit der unter dem Rubrum STS versammelten Ansätze besteht, *zweitens,* in der Aufmerksamkeit, die der eigenmächtigen Rolle technischer Artefakte und Systeme zukommt. Dies ist die gedankliche Konsequenz aus dem methodologischen Diktum der Symmetrie, demzufolge alle Akteur_innen eines Kontextes betrachtet werden sollen (insb. Latour 1996, 2002). Dieses Prinzip induziert, dass alle an einer analysierten Praxis beteiligten Entitäten – seien sie nun menschlich oder nicht-menschlich – in eine Untersuchung Eingang finden sollten. Für die Qualifizierung als relevante_r Partizipant_in einer Praxis ist nicht die (menschliche) Intentionalität Voraussetzung, stattdessen zählt, ob die Entitäten Einfluss auf andere auszuüben im Stande sind: „[…] jedes Ding, das eine gegebene Situation verändert, indem es einen Unterschied macht, (ist) ein Akteur" (Latour 2010: 123). Die jeweils genutzten technologischen Artefakte und Systeme sind demnach nicht als passive Vermittler zu verstehen, sondern als agierende Akteure bzw. Aktanten (Latour 2002: 219). Als solche transformieren sie ihre Einsatzkontexte und bestimmen über ihre Materialität die dortige Praxis mit. *Drittens* heben die STS-Ansätze die soziale Dimension von technologischen Artefakten hervor: Vor allem der *Social Construction of Technology* (SCOT) Ansatz verweist auf die Bedeutung der gesellschaftlichen Dimension des materiellen Ergebnisses technologischer Entwicklungen, indem er auf die involvierten Gruppen im technologischen Entwicklungsprozess blickt (Bijker 1993). Dabei arbeitet diese STS-Schule die verschiedenen, sozial geformten Interessen mit ihrem direkten Einfluss auf die Ausgestaltung der jeweiligen Technologie heraus und bildet ein theoretisches Fundament für die Kritik von Objektivitätsfiktionen wissenschaftlich-technologischer Apparaturen, da letztere immer auch als sozial konstruiert – und damit als ebenso kontingent wie fehlbar – zu beschreiben sind. Gesellschaftliche Interessen, Hoffnungen und Hypothesen schreiben dabei Visionen der Welt in den materialisierten Inhalt und seine Formen der Technik ein, so-

3 Wir befassen uns vorliegend allein mit jenen Ansätzen, die mehr oder minder konkret den STS und ihrer techniksoziologischen Ausrichtung zugerechnet werden. In der Tat gibt es noch viele weitere techniksoziologische Ansätze (Überblick: Lengersdorf/Wieser 2014), insbesondere auch deutschsprachige, die ähnlich argumentieren, aber aus Platzgründen nicht näher besprochen werden können (z. B. Rammert 2016).

dass Technologien spezifische „Skripte“ aufweisen (Akrich 1992). Diese reproduzieren und aktualisieren sich schließlich in der Anwendung des Artefaktes.

Mit Übernahme einer solchen soziotechnischen Perspektive können Praktiken und soziale Kontexte, die für die Kriminologie von Interesse sind, auf eine neue Weise erfasst und analysiert werden. So werden Fragen, wie jene nach der Delegation von Verantwortung an Technologien aufgeworfen (s. z. B. Egbert et al. 2016). Andere betreffen die neuen Handlungsmöglichkeiten, die über Prozesse der Technifizierung entstehen, ob auf Seiten der Strafverfolgung – wie am Beispiel der Körperkameras zu sehen ist (Timan 2016) – oder auf Seiten der Normbrüche – wie das Beispiel der Cyberkriminalität zeigt (Leman-Langlois 2008: 2 f.). Die Kriminologie sollte daher verstärkt nach der spezifischen Rolle der Technologie in den entsprechenden Interaktivitätskontexten fragen sowie danach, welche praktischen und diskursiven Effekte diese nach sich ziehen. Von Interesse ist u.E. dabei vor allem, wie Technologien intervenieren und welche Funktionen sie übernehmen.

Im Folgenden werden wir einen Überblick über die bisherige kriminologische Beschäftigung mit Technologien geben und aufzeigen, an welchen Stellen durch einen STS-gestützten Blick Fragen und Perspektiven erweiterungsfähig wären. Danach stellen wir vor, wie die grundlegenden Annahmen der STS für die Kriminologie nutzbar gemacht werden können. Das Ganze schließt mit einer Zusammenschau der Beiträge dieses Themenheftes und ihrer Bedeutung für den vorliegend besprochenen Schwerpunkt.

Über die bisherige Rolle von Technologien in der Kriminologie

In kriminologischen Analysen wurde sich bisher durchaus vielfach mit Technologien auseinandergesetzt. Allerdings ist, und das ist hier der wesentliche Punkt, nur in Einzelfällen eine systematische Übernahme von STS-Gedanken erkennbar. Viele dieser Werke sind für sich genommen und an der eigenen Zielsetzung gemessen analytisch unbestritten fruchtbar. Unser Anliegen ist es vielmehr herauszustellen, dass eine Beschäftigung mit Technologien an analytischer Schärfe und überhaupt an neuen Untersuchungsperspektiven gewinnen könnte, wenn sie gerade mit Annahmen der STS arbeiten würde.

Widmet man sich den Ansätzen, die aus einem kriminologischen Forschungsinteresse heraus Technologien zum expliziten Thema machen, ohne dabei ausdrücklich auf techniksoziologische Arbeiten Bezug zu nehmen, so sind für den deutschsprachigen Diskurs insbesondere die Arbeiten von Detlef Nogala zu nennen. Er stellt, wie es im Kern solcher ausgerichteten Arbeiten zumeist der Fall ist, vor allem auf die technologische Entwicklung und deren Einfluss auf die Maximierung von Überwachungsmöglichkeiten ab (1998, 2000). Eine seiner Kernthesen – heute gültiger als je zuvor – lautet, dass „ausgefeiltere Überwachungssysteme“ den Trend zu einer proaktiven und

zunehmend vorfeldorientierten Kontrollpolitik überhaupt erst ermöglicht haben (2000: 151). Er geht jedoch nicht so weit, die Öffnung der technischen *black boxes* selbst vorzunehmen sowie ihre materialen Widerständigkeiten aufzuzeigen. Analysen dieser Ausrichtung nehmen folgerichtig das sich anbietende analytische Potenzial nicht in Gänze auf. Stattdessen liegt ihr Fokus auf der Systematisierung unterschiedlicher Überwachungstechnologien (Nogala 2000: 143; vgl. a. Bowling/Marks/Murphy 2008: 55) oder der gesteigerten Kontrollfähigkeit durch neue Technologien (Marx 2016: 63 ff.; so auch z. B. Eisenberg/Puschke/ Singelnstein 2005).

Ein weiterer Fokus gilt den Veränderungen von Strafpraxen, die durch das Aufkommen neuer elektronischer Technologien vermehrt auch auf der Basis von neuen Informationsverarbeitungssystemen (Datenbanken) und von technologisch vermittelten Prima-facie-Belegen von Normbrüchen – z. B. per elektronischer Fußfessel – bedingt sind. Richard Jones (2000: 11) z. B. verweist in diesem Kontext darauf, dass die entsprechende Detektion des Normbruchs automatisch bzw. algorithmisch erfolgt (*digital rule*): Im Falle der Fußfessel auf Basis eines elektronischen Signals am Computer, das z. B. auf die Missachtung der Ausgangssperre hinweist, die wiederum schematisch in entsprechende Sanktionen – z. B. die Verschärfung von Bewährungsauflagen – übersetzt wird. Damit sei laut Jones eine besondere Form der sozialen Regulation verbunden, die wesentlich die Verbindung von kontrollierenden und strafenden (weil z. B. unmittelbar exkludierenden) Praktiken beinhaltet, die letztlich erst durch technologische Unterstützung ermöglicht wird (vgl. a. Aas 2004). Die Nutzung von STS-Literatur hätte, so unsere These, die Analysen noch fruchtbarer gemacht, da sie einen detaillierteren Blick auf die Technologie selbst und ihre Konstitution sowie Wirkmächtigkeit bietet. Ähnliches gilt für die wirkmächtige Rolle von Technologien im Kontext von Sicherheitspraktiken, wie sie von Lucia Zedner betont wird, die völlig korrekt von der „socially situated nature of technology" (2009: 259) spricht, ohne dies jedoch weiter zu vertiefen.[4]

Einen ähnlichen Schwerpunkt vertreten Kevin D. Haggerty und Richard V. Ericson in ihrer mittlerweile klassischen Analyse der *surveillant assemblages* (2000). Diese sind durch dominante technologische Anteile und die Abstrahierung vom menschlichen Körper sowie die Bildung von entsprechenden „Datendoublen" gekennzeichnet (2000: 606). Technologien machen die Übersetzung des menschlichen Körpers in „pure information" erst möglich (2000: 613). Deutlicher auf Mikropraktiken fokussiert, aber ähnlich offen für die aktive Rolle von Technologien ist wiederum die Arbeit, die Michalis Lianos und Mary Douglas (2000) vorgelegt haben, in der sie die Charakteristika automatischer Kontrollsysteme, so genannter *Automated Socio-Technical Environments* beschreiben und Effekte für die Kontrollpraxis herausarbeiten. Am prägnantesten ist dabei ihre These, dass Verhandlungen mit Maschinen nicht möglich sind und auch z. B. bei einer

4 Siehe dazu auch die anderen Beiträge in Aas/Gundhus/Lomell (2009).

fehlerhaften Zutrittsverweigerung der Technologie eine unmittelbare Aufklärung des Irrtums bzw. des Defekts nicht möglich ist (2000: 264).

Ein gemeinsames Merkmal dieser Arbeiten ist die Hervorhebung, dass Überwachungstechnologien keineswegs neutral oder objektiv sind, da sie von Beginn an sozial codierte Verdachtskonstruktionen generieren und verdoppelte Typisierungsschemata anbieten (vgl. für die Videoüberwachung Wehrheim 2014). In eine ähnliche Stoßrichtung argumentieren jene Arbeiten, die unter dem Stichwort „sicherheitsindustrielle(r) Komplex" (Busch 2010) bzw. „surveillance-industrial complex" (Hayes 2012; Ball/Snider 2014) die praktischen Verquickungen von wirtschaftlichen und sicherheitsbezogenen Interessen veranschaulichen (vgl. auch schon Lindenberg 1997) und auf die zunehmende Privatisierung von Sicherheit hinweisen. In diesem Rahmen spielen seit jeher Technologien eine wesentliche Rolle, da über den Vertrieb von kommerziellen Sicherheitsprodukten (Taser, Videokameras, Software-Systeme wie *CompStat*, Körperkameras etc.) zunehmend nicht-staatliche Akteur_innen an der Sicherheitsproduktion beteiligt sind (Kreissl 2011: 270 f.).

Des Weiteren existieren kriminologische Arbeiten, die explizit auf techniksoziologische Annahmen zurückgreifen, dabei aber weitestgehend auf der Ebene des Verweises bleiben. Stellvertretend für viele (z. B. Heinrich 2007; Kroener 2014) seien hier Reinhard Kreissl und Lars Ostermeier genannt (2011), die auf Thesen der Akteur-Netzwerk-Theorie (ANT) verweisen, deren Entgrenzungsdiktum aber alleine für die begriffliche Dekonstruktion von bekannten terminologischen Bipolaritäten wie „Öffentlichkeit" und „Privatsphäre" oder „konform" versus „deviant" nutzen (2011: 291 ff.). In der Tat verdeutlichen sie dabei indes treffend die technische Mediatisiertheit moderner Kontrollverfahren und deuten einige der damit zusammenhängenden Folgen an – wie z. B. die Nicht-Verhandelbarkeit von Exklusionsentscheidungen (2011: 293 f.).

Darüber hinaus gibt es vereinzelte Arbeiten, die techniksoziologische Annahmen explizit in kriminologische Fragestellungen inkorporieren *und* systematisch in Rechnung stellen.[5] Allen voran ist Sheila Brown zu nennen, die bereits 2006 mit Rückgriff auf Kerngedanken der ANT eine *Criminology of Hybrids* formulierte. Ihr Aufruf, sich mit den theoretischen Herausforderungen und Möglichkeiten der ANT bzw. STS zu beschäftigen, wurde jedoch bislang von der Kriminologie nicht nachhaltig aufgegriffen. Brown stellt vor allem heraus, dass sich die bisherige Kriminologie stets an einer Binarität von Natur und Gesellschaft abarbeitet, selbst wenn sie sich mit soziotechnischen Handlungskontexten beschäftigt (2006: 225). Technologien bleiben in der Kriminologie, so Brown, stets dem menschlichen Tun unter- und nachgeordnet. Wir sind aber unabänderlich in der Technosozialität angekommen, weswegen Brown

5 Dominique Linhardt (2000) ist z. B. einer der wenigen, der grundlegende Überlegungen anstellte, die danach jedoch nicht weiter aufgegriffen wurden. So legte er eine detaillierte empirische Analyse von Rationalen der Flughafensicherheit vor, die aufzeigt, wie Maschinen die Menschen in Handlungsformate zwingen (2000: 84).

moniert, dass es überfällig sei, sich dem hybriden Charakter kriminologisch relevanter Praktiken zu stellen. Vor allem im Rückgriff auf Latours Netzwerkbeschreibungen sowie Haraways postfeministisch-kybernetische Perspektive skizziert sie programmatisch neue Forschungsfelder und Fragen für die Kriminologie, die jenseits exklusiver menschlicher Handlungsträgerschaft angesiedelt sind. Ein Hauptaugenmerk liegt dabei auf dem menschlichen Körper, der untrennbar mit technosozialen Bezügen verknüpft ist. Unser Körper wird z. B. zu Daten zerlegt und neu zusammengesetzt, wenn es darum geht, Menschen via elektronischem Monitoring zu verfolgen, ihre Identitäten mittels Fingerabdrücken festzustellen etc. Die vielfältigen Fragen juristischer, empirischer, theoretischer, aber eben auch ethischer Natur (z. B. nach der Zuschreibung von Schuld) (vgl. a. Aas 2015: ix ff.) werden von Brown in eine disziplinäre Herausforderung an die Kriminologie zusammengeführt. Diese habe sich eben nicht nur mittels einer anderen Ätiologie den Erklärungen menschlicher Handlungen in ihrer simultanen Konstitution als technischer Begebenheit zu widmen (2006: 236),[6] sondern auch das Kontrollsystem auf ihre „technological properties of the body politic, and of the institutional landscape of control, as inseparable from their form" (2006: 236) hin zu analysieren.

Mit dem Sammelband von Dominique Robert und Martin Dufresne (2015) liegt zudem ein Überblickswerk über die Anwendungspotenziale der ANT für die kriminologische Analyse vor. Das analytische Potenzial der ANT sehen Robert und Dufresne in den folgenden Prinzipien: In deren Betonung der Performativität des Sozialen, in ihrer antihumanistischen bzw. artefaktemanzipativen Stoßrichtung und in der Fokussierung von menschlichen und nicht-menschlichen Aktanten als relationale Entitäten (Robert/Dufresne 2015: 1). Die zahlreichen Fallstudien des Bandes stellen dieses Potenzial exemplarisch dar. So untersucht Bertrand Renard Praktiken der genetisch-forensischen Analyse in Belgien und wendet dabei das alte methodische Diktum der ANT an: *following the actors* – indem er der DNA-Spur am Tatort bis in den Gerichtssaal nachgeht (2015: 113). Diesen auch als Übersetzung bezeichneten Prozess teilt er in drei wesentliche Bereiche auf: jenen Zeitpunkt, als die DNA-Analyse als Idee in den juristischen Kontext eingeführt wurde, die technische Arbeit selbst, also den Weg vom Tatort zum Gutachten, und schließlich die juristische Arbeit, also die gerichtliche Bewertung und Bearbeitung des Gutachtens (2015: 114). Renard beschreibt auf diese Weise, was passiert, wenn DNA-Spuren als neue Aktanten in den juristischen Kontext eingeführt werden, welche Assoziationen damit gebildet werden und welche Effekte damit verbunden sind.

---

6 Beispielhaft ist für eine diesbezügliche Einzelfallstudie der Text von Wytske van der Wagen und Wolter Pieters (2015) zu nennen, die sich dem Internetbetrug per automatisierter Schadprogramme (Botnets) zuwenden und als „hybrid criminal network" rekonstruieren. Sie zeigen auf, dass der Normbruch nicht mehr allein durch Ansätze analysiert werden kann, die alleinig auf die menschliche Handlungsfähigkeit abstellen (2015: 581). Damit verdeutlichen sie, wo die rechtlichen Schwierigkeiten der Zuschreibung von Handlungsverantwortung liegen, wenn nicht mehr nur Menschen mit Maschinen, sondern letztere selbstständig agieren.

Öffnet man den Blick für die der Kriminologie nahestehenden *Surveillance Studies*[7] wie auch die *Critical Security Studies*, finden sich weitere Arbeiten, die einen expliziten Rückgriff auf techniksoziologische Ansätze beinhalten. Einen programmatisch intendierten Überblick zum Nexus Techniksoziologie und *Surveillance Studies* haben Inga Kroener und Daniel Neyland (2012) vorgelegt. Sie werfen anhand des Beispiels der Videoüberwachung die Frage auf, in welcher Weise neue Technologien relevant für die Einführung neuer Risikoszenarien sind und wie wiederum diese Narrative in die Systeme selbst eingeschrieben werden (2012: 143 f.). Ein verstärkter Blick mit STS bei der Analyse von Sicherheits- und Überwachungspraktiken würde laut Kroener und Neyland eine vierfache Sensibilisierung schaffen können (2012: 145 f.): Dafür, dass, *erstens,* die Auswirkungen von Technologien niemals von vornherein feststehen, sondern entlang ihrer soziotechnischen Einbettung generiert werden; *zweitens* die aus Technologien gespeisten Informationen nie für sich selbst stehen und ‚reine' Daten seien, sondern stets komplexe Interpretationsspielräume beinhalten; *drittens* Technologien als erstarrte gesellschaftliche Beziehungen zu verstehen sind, denen spezifische politische Werte und Normen inhärent sind und *viertens* technologische Artefakte und Systeme immer multiple Ontologien besitzen, da sie nicht für sich selbst stehen, sondern ihre Bedeutung je nach Perspektive und Anwendungspraktik erlangen (wie z. B. im Falle der Wasserflasche, die mittlerweile in Flugzeugen nur noch eingeschränkt akzeptiert wird und die sich von einem banalen Objekt zu einem riskanten Gegenstand gewandelt hat) (2012: 146 f.; vgl. a. Neyland 2009).

Und erst kürzlich hat Stefan Kaufmann (2016) einen Brückenschlag zwischen techniksoziologischen Kerngedanken und sozialwissenschaftlichen Analysen technologisierter Sicherheitspraktiken vorgelegt. Dabei situiert er die Technologien als relationale Elemente soziotechnischer Praktiken und betont deren fluiden, nicht-determinierbaren Charakter (siehe dazu auch Altenhain in diesem Band) und die Unmöglichkeit, per technologischer Assistenz absolute Sicherheit herzustellen (vgl. a. Rauer 2012).

Welchen Beitrag können die STS für die Kriminologie leisten?

Wie also könnte die Verwertung von STS-Ansätzen für kriminologisch relevante Fragen fruchtbar gemacht werden? Wir wollen dies an fünf Beispielen aufzeigen:

---

7 Für die *Surveillance Studies* gilt ähnliches wie für die Kriminologie. Zwar spielen hier Technologien eine vergleichsweise große Rolle (überblickend: Zurawski 2015), sie werden aber nur selten in den Status eigenmächtiger Interaktionspartizipanten gerückt (s. z. B. Lyon 2003; Monahan 2006). Der am meiste rezipierte Vertreter ist hier Gary T. Marx, der seit langem die Rolle von technologischer Entwicklung in der Beeinflussung von Kontrollpraktiken analysiert (zuletzt 2016).

Erstens weist die These der sozialen Konstruktion von Technologien auf die Aushandlungs- und Stabilisationsprozesse der verschiedenen Akteur_innen und deren Interessen im Produktions- bzw. Entwicklungsprozess – also der Genese – von Technologien hin.

Am Beispiel der Drogentests lässt sich das analytische Potential für die Kriminologie dabei gut aufzeigen: Drogentests als verbreitete gesellschaftliche Alltagspraxis sind vor allem aufgrund der Entwicklung von Schnelltests möglich geworden. Die Tests bilden eine Kompromisslösung zwischen verschiedenen Bedürfnissen der Anwender_innen: hinreichende analytische Validität, Praktikabilität vor Ort, schnelle und günstige Ergebnisse (Paul/Egbert 2016). Diese Rationale der Entwicklungs- und Implementationsphasen sind in die Artefakte eingeschrieben und bestimmen damit die Art wie die Tests angewendet werden (können). Andere Fragen beziehen sich z. B. auf die politische Qualität, die dem Artefakt inhärent ist (vgl. Winner 1980) und darauf, wie die Technologie die Sichtweisen über jene Phänomene formt, die es bearbeiten soll (hier z. B. auf unerwünschten Drogenkonsum und die Vorstellungen über seine Konsument_innen als Sicherheitsgefahr) und inwieweit die Technologieentwicklung in gesellschaftliche und ökonomische Zusammenhänge eingebettet ist.[8]

Damit kann beispielsweise die bisherige kriminologische Diskussion um die ökonomische Lenkung von Straf- und Überwachungspolitiken aktualisiert und expandiert werden. Während z. B. Lindenberg bereits 1997 mit der Analyse des bestrafungsindustriellen Komplexes am Beispiel der elektronischen Fußfessel eingehend zeigt, welche wirtschaftlichen Interessen der Initiierung von Straftechnologien inhärent sind, vermag ein STS-informierter Blick bereits die konkrete Stabilisierung und Ausformung der Technologie selbst durch die Analyse der Aushandlung der verschiedenen gesellschaftlichen, insbesondere ökonomischen, Interessen festzustellen. Dabei werden nicht nur die Interessen identifiziert, sondern auch die hinter ihnen stehenden Rationalitäten und die jeweils damit verbundenen sozialen Gruppen, die mit der Entwicklung und Ausgestaltung einer Technologie konkrete Versprechungen und Motive verbinden. Diesen Übertrag bis hin zur Analyse der Einschreibungen in der Ausgestaltung der Technologie bildet einen Mehrwert für die kriminologische Analyse, indem die These, dass hinter Kontroll- und Bestrafungspraktiken eben nicht nur präventive oder strafende Intentionen stehen, noch präziser und vielschichtiger ausgestaltet werden kann.

Ein *zweites Beispiel* ist die Hervorhebung der *agency* von Technologien. Fasst man diese im Sinne von (vermittelnder) Befähigung zur Handlung, so lässt sich der spezifische Einfluss von Artefakten auf die Interaktion zwischen Menschen und nicht-menschlichen Entitäten analysieren. Am Beispiel der Videoüberwachung im öffentlichen Raum lässt sich so zeigen, wie diese

8 Für das Beispiel der biometrischen Technologien und deren ökonomische Einbettung vgl. Kühne/Wehrheim (2013).

Kontroll-Interaktion soziotechnisch durchdrungen ist (beispielhaft siehe auch die Studie von Timan 2013): Die Operator_innen hinter den Bildschirmen sind nur das zu sehen im Stande, was hinsichtlich Bildauflösung, Sicht- bzw. Schwenkbereich für sie einsehbar ist. Gleichzeitig gehen indes mit bildlichen- bzw. filmischen Darstellungen per se Evidenzzuschreibungen einher, die eine ungefilterte Repräsentation der Realität nahelegen. Zentral ist hierbei auch die Rolle, die die Auffassung der Technologie als mechanische Objektivität produzierende Apparatur spielt (Daston/Galison 2010), die über den Prozess des *black boxing* (Latour 2002: 373) gestützt wird, bei dem nur der In- und Output eines Geräts verfolgt, jedoch der Funktionsprozess selbst nicht hinterfragt wird.

Insofern kann eine STS-informierte Analyseperspektive den bisherigen kriminologischen Studien zur Videoüberwachung (z. B. Norris/Armstrong 1998) weiterführende Erkenntnisse zur soziotechnischen Ausgestaltung dieser Kontrollpraktik hinzufügen: Die detaillierte Wiedergabe des Überwachungsbildes gilt es hierbei zu dechiffrieren, die Auswahl und Herstellung desselben sowie seiner Interpretation. All das ist untrennbar mit den multiplen, grundständig sozialen Einschreibungen in die Apparaturen und Aufzeichnungsparameter verbunden, was insbesondere für den Verdachtskonstruktionsprozess gilt (vgl. a. Wehrheim 2014).

Drittens gilt es den schon angeschnittenen Punkt der Mensch-Maschine-Hybridität zu betrachten. Das bereits erwähnte Beispiel der Körperkameras bei Polizist_innen eröffnet exemplarisch ein neues Feld für die Kriminologie, in dem die technische Erweiterung des Körpers zum Gegenstand der Analyse wird. Bislang wird der Körper in der Kriminologie als einzelne Entität im Verhältnis zur Kontrollpraxis verhandelt (z. B. als Gegenstand der Disziplinierung). Wird diese Begrenzung aufgehoben, findet dies noch am ehesten mit Blick auf die digitale Erweiterung des Menschen statt, d. h. dessen Aktivitäten in virtuellen Räumen (z. B. McGuire 2007: 79 ff.). Diese Erweiterung öffnet sich bereits für Fragen der Subjektivierungsformen und spezifischen Vulnerabilitäten oder Haftbarmachung (vgl. Brown 2006). Durch Hybridität gekennzeichnete Kontrollinteraktionen wie der polizeiliche Einsatz von Körperkameras zieht jedoch eine ganz eigene Einflussnahme auf die Interaktion der Beteiligten nach sich, die neue Fragen aufwirft: Worin konkret besteht die Einflussnahme der Technologie auf das Handeln und die Performanz in der Kontrollsituation, auf die Identität als Polizist_in, auf ihre Körperwahrnehmung? Wie verändert sich (Selbst-)Kontrolle der Protagonist_innen gegenüber der bildbasierten Aufzeichnung? Und auf einer abstrakteren gesellschaftlichen Ebene: Wie verändern diese hybriden Konstellationen unsere Beziehung zu Kontrolle und Kontrollinstitutionen?

Die damit verbundenen Fragen nach der Verortung von Subjektivität und Entscheidungen wird einmal mehr im *vierten* Beispiel aufgeworfen. Dabei gilt es, nach den Netzwerken, den Übermittlungen zu fragen, die eine Kontroll-Praxis formen. Blickt man z. B. auf die Praktiken des *predictive policing*,

so ist konkret die Spezifik der Algorithmen, die in die Technologie mit der die Polizei arbeitet, eingespeist werden, zu beachten. Bei dieser Auszeichnung von Risiko-Quartieren für zukünftige Einbrüche z. B. (Legnaro/ Kretschmann 2015; Belina 2016), entscheidet die Software nicht gänzlich autonom, welches Gebiet als riskant tituliert wird, sondern auf Basis entsprechender, von Menschenhand programmierter algorithmischer Risikofaktoren und anhand polizeilicher Daten, die sich in den Verdachtskonstruktionsprozess der Technologie einschreiben. Eine Perspektive, die gerade die Faktoren der Geschwindigkeit wie auch der Datencharakteristika in den Blick nimmt, d. h. eben auch danach fragt, wie die spezifischen Entscheidungsparameter konfiguriert sind, kann analysieren, welchen (technischen) Einflüssen die Polizeipraxis konkret unterlegen ist und welche Veränderungen in der polizeilichen Verdachtskonstruktion damit verbunden sind. Damit würde sie über die bisherigen kriminologischen Analysen ergänzend hinausgehen, in dem z. B. die Einschätzung, dass die im Zuge von Predictive Policing genutzten Daten gemeinhin als „wertfrei und moralisch neutral (gelten)“ und die dabei genutzten Karten eine spezifische „Performativität“ aufweisen, die ihren konstruierten, kontingenten Charakter unsichtbar werden lässt (Belina/Germes 2016: 32) zum einen mit konkretem Blick auf die soziotechnische Herstellung und Aufbereitung der Daten rekonstruiert werden kann, zum anderen in ihrer praktischen Realisierung wiederzugeben ist: Welche Daten werden konkret eingespeist, wie werden sie verarbeitet und aufbereitet, mit welchem Evidenzanspruch werden sie versehen und inwieweit hat dies einen Effekt auf den praktischen Umgang mit den Prognosen der Technologien?

Als *fünftes* Beispiel sei hier die Hervorhebung der Reziprozität von Diskurs und Praktik bzw. Artefakt betont. Nicht nur das Artefakt ist in seiner Entwicklung durch soziale Einflüsse geformt (siehe Beispiel eins), sondern eben auch der gesellschaftliche bzw. politische Diskurs wird durch die Existenz des Artefaktes spezifisch tangiert und in seinem Fortgang beeinflusst (Egbert/Paul 2014; Walters 2014). Fragen nach der spezifischen technosozialen Ordnung, die so über die Existenz eines Artefakts gestiftet wird, lassen sich z. B. an empirischen Feldern wie der Lügendetektion im „war of terror“ aufzeigen. Durch die Existenz neuer avancierter Verfahren der *deception detection* (wie bildgebende Verfahren der Neurowissenschaft) wirken die Technologien, ihre Materialität etc. auf den Diskurs um anti-terroristisch motivierte Kontrollpraktiken zurück und prägen z. B. die Erwartungshaltung und die Legitimitätszuschreibung an die Technologie und den damit verbundenen Eingriff, da sie als vermeintlich objektive diskursive Referenz und somit verführerische symbolische Figur fungieren (können). Die Technologie, hier das hirnbildgebende Verfahren, wird damit zum „Diskursaktant“ und prägt die politisch wahrgenommenen bzw. prophezeiten Sicherheitsversprechungen und die dort antizipierten legitimen Anwendungskontexte (Egbert/Paul i.E.). Mit diesem STS-inspirierten Blick von Technologien als Diskursaktanten lässt sich z. B. der bisherige kriminologische Diskurs um die Akzeptanz biometrischer Identifizierungsverfahren (z. B. Bennett et al. 2014: 151 ff.) insofern treffend er-

gänzen, als das an gesellschaftlich-politischen Kontrolldiskursen beteiligten Partizipantenensemble substanziell erweitert wird und auf diese Weise die diskursive Dynamik gegenstandsnäher zugänglich gemacht werden kann. Denn die jeweils für bestimmte (sicherheitspolitische) Ziele vereinnahmten Technologien lassen bestimmte, gemeinhin positiv konnotierte Adressierungen zu – wie z. B. Objektivität, Fairness, Unparteilichkeit – die als wirkmächtige Referenzen bei der Legitimierung von Überwachungsmaßnahmen dienen (s. dazu bereits Bright 2011; Krasmann/Kühne 2014).[9]

Die Beiträge des Heftes

Die Beiträge in diesem Heft widmen sich auf unterschiedlichem Wege den meisten der vorstehend angesprochenen Ebenen:

Emily Troshynski widmet sich im Auftaktbeitrag der Frage, wie Sexualstraftäter, die in den USA ihre lebenslange Bewährungsstrafe mittels GPS-Monitoring absolvieren, diese Situation wahrnehmen. Für ihre hier vorgestellte Studie nimmt sie eine technofeministische Perspektive ein, um herauszustellen, wie die neue Hybridität von Mensch und Maschine – im Haraway'schen Cyborg-Sinne – auf die Haftentlassenen wirkt. Der Rückgriff auf die Cyborg-Metapher von Haraway hilft, so Troshynski, sowohl technologische Determinismen wie einen Gender-Essentialismus zu vermeiden, da die Beziehung zwischen Geschlecht und Technologie dynamischer wie situationsbezogen analysiert werden kann. Mit ihrem Beitrag gelingt es Troshynski zum einen die Konstitution der soziotechnischen Überwachung von Menschen auf Bewährung pointiert in den Blick zu nehmen. Zum anderen kann sie mittels einer gendersensiblen STS-Perspektive auf die cyborgsche Konstellation durch die am Körper angebrachte Technologie aufzeigen, wie sich die Körperwahrnehmung der betroffenen Subjekte re-konstituiert, sich deren Körper neu reproduziert und wie dieser somit diszipliniert wird.

Benedikt Lehmann widmet sich dem Subjektstatus in soziotechnischen Bezügen auf eine andere Art: Bei ihm geht es um den algorithmischen Hochfrequenzhandel („high-frequency trading", HFT) an den modernen Finanzmärkten, der mittels technischer Neuerungen in der Datenverarbeitung Geschwindigkeit und Automatisierung des Wertpapier-Handels vorantreibt und so Wege findet, sich seiner Regulierung zu entziehen. Lehmann blickt auf einen klassischen Diskussionspunkt der kriminologischen Beschäftigung mit *White-Collar-Crime*, nämlich der Frage, wo und wie die Subjekte in die illegitimen Tätigkeiten des Handels individuell eingebunden sind. In seiner anomischen Ausprägung funktioniert der HTF durch die Transformation der Menschen zu rein passiven Bediener_innen der Handelsalgorithmen, die ihr Nicht-Wissen und sogar ihren Entscheidungsverzicht strategisch einzusetzen

9 Für das Beispiel Videoüberwachung im öffentlichen Raum siehe Kroener (2014).

wissen. Zugleich bedient sich die Regulation des Handels auch der Algorithmen und verweist damit auf neue Anpassungserfordernisse der Kontrolle. Lehmann stellt heraus, wie das Verlangen nach Subjektlosigkeit in der Kapitalakkumulation wie auch in den Notwendigkeiten der Kontrolle neue kriminologisch relevante Fragen der Verantwortungsdiffusion aufwirft und was das für eine soziotechnische Analyseperspektive bedeuten kann.

Stefano Mazzilli-Daechsel macht den Versuch, die kritische Kriminologie davon zu überzeugen, sich auf eine ontologische Neuorientierung hin zu einer Objekt-Orientierung einzulassen. Er bedient sich dafür einer Lesart Bruno Latours als „objekt-orientiertem Denker" (nach Graham Harman), wobei der Begriff des „Objekts" für menschliche wie nicht-menschliche Entitäten genutzt wird, solange sie imstande sind, sich zu vernetzen oder eben einer solchen Vernetzung zu widerstehen. Mazzilli-Daechsels entspricht damit Browns Kritik des veralteten Binaritätsdenken (von technisch/sozial; Natur/Kultur oder menschlich/nicht-menschlich), dass im Zeitalter des technisch erweiterten wie vernetzten Menschen kaum mehr hilfreich ist. Er widmet sich vor allem den Konsequenzen, die das Umdenken mit sich bringt und erörtert das veränderte Verständnis von Kernkonzepten wie Schadensverursachung (statt einer Orientierung an Kriminalität) und Widerstand für die Kriminologie.

Claudio Altenhain beschreibt in seinem Forschungsbericht die „Migration" einer polizeilichen *Big Data*-Software von New York nach São Paulo und die damit zusammenhängenden Transformationsprozesse und diskursiv-politischen Friktionen. Er plädiert dafür, sich nicht nur auf Phänomene des globalen Nordens zu konzentrieren, da der spezifische soziale Kontext in Ländern des globalen Südens für die jeweiligen Sicherheitstechnologien von höchster Relevanz ist. Altenhain zeigt in Anschluss an Annemarie Mol (2002), dass Technologien keine feste ontologische Realität besitzen, sondern fluide Gebilde sind, die von unterschiedlichen Anwender_innen und in differenten Kontexten jeweils andere Formen und Funktionen zugewiesen bekommen. Damit verdeutlicht er auch die spezifische Wechselwirkung zwischen Technologien und (Sicherheits-)Diskursen, da nicht nur Technologien als spezifische Ergebnisse von Diskursen verstanden werden können, sondern sie auch umgekehrt auf Diskurse zurückwirken und gleichsam als eigenständige Diskursaktanten auftreten.

Dieses Themenheft zeigt, wie STS-Ansätze für kriminologisch relevante Themen und Forschung nutzbar gemacht werden können. Durch die Sensibilisierung für die soziale Konstruktion von technologischen Artefakten auf der einen und die materiellen Effekte von Technologien auf der anderen Seite erlaubt die Integration von STS-Annahmen eine detaillierte Analyse von gegenwärtigen Kontroll-, Sicherheits- oder Überwachungspraktiken. Dabei können insbesondere Diskussionslinien um die (zunehmende) Ökonomisierung sozialer Kontrolle in wichtigen Punkten vertiefend ergänzt werden, indem bereits der Geneseprozess der jeweiligen Überwachungstechnik zum Gegenstand der kriminologischen Analyse wird und dabei die jeweils beteiligten Interes-

sensgruppen in ihrer wirkmächtigen Rolle rekonstruiert werden. Insgesamt kann die Integration von Perspektiven der *Science and Technology Studies* eine grundlegende Erweiterung kritisch-kriminologischer Herangehensweisen und ihrer Palette an Fragestellungen und Untersuchungsgegenständen leisten. So sind technologisch mediatisierte Kontroll-, Überwachungs-, Präventions- oder Bestrafungspraktiken nicht nur en detail zu analysieren, sondern die damit zusammenhängenden Praktiken gleichsam in Raum und Zeit auszudehnen, indem die vorgängigen Entscheidungsprozesse und Selektionen in den Fokus der Analyse rücken.

Je mehr kriminologisch relevante Praktiken technologisch vermittelt sind, umso wertvoller ist die hier vorgeschlagene Erweiterung der Analyse mithilfe einer STS-Perspektive. Dies sollte in der Kritischen Kriminologie in Zukunft deutlich stärker im Fokus stehen, will sie in Lehre, Theoriebildung und Forschung, aber eben auch in der Kriminal- und Sicherheitspolitik eine (kritische) Einflussgröße bleiben (vgl. a. Haggerty 2004).

Literatur

Aas, Katja Franko (2004): From narrative to database: Technological change and penal culture, in: Punishment & Society 6 (4), 379-393.

Aas, Katja Franko (2015): Preface, in: Robert, Dominique/Dufresne, Robert (Hg.): Actor-Network Theory and Crime Studies, Farnham/Burlington, ix-xiii.

Aas, Katja Franko/Gundhus, Helene Oppen/Lomell, Heidi Mork (2009) (Hg.): Technologies of InSecurity. The surveillance of everyday life, Abingdon/New York, 257-270.

Akrich, Madeleine (1992): The De-Scription of technical objects, in: Bijker, Wiebe E./Law, John (Hg.): Shaping technology/building society, Cambridge, MA, 205-224.

Amoore, Louise (2013): The politics of possibility: risk and security beyond probability. Durham/London.

Ball, Kristie/Snider, Laureen (Hg.) (2013): The Surveillance-Industrial Complex. A Political economy of surveillance, London/New York: Routledge.

Belina, Bernd (2016): Predictive Policing, in: Monatsschrift für Kriminologie und Strafrechtsreform 99 (2), 85-100.

Belina, Bernd/Germes, Mélina (2016): Kriminalitätskartierung als Methode der Kritischen Kriminologie?, in: Kriminologisches Journal 48 (1), 24-46.

Bennett, Colin J./Haggerty, Kevin D./Lyon, David/Steeves, Valerie (2014) (Hg.): Transparent Lives. Surveillance in Canada. Edmonton.

Bijker, Wiebe E. (1993): Do not Despair: There is Life after Constructivism, in: Science, Technology, & Human Values 18 (1), 113-138.

Bijker, Wiebe E/Pinch, Trevor (2012): Preface to the Anniversary Edition, in: Bijker, Wiebe E/Hughes, Thomas P./Pinch, Trevor (Hg.): The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology, Anniversary Edition, Cambridge, xi-xxxiv.

Bowling, Ben/Marks, Amber/Murphy, Cian C. (2008): Crime Control Technologies, in: Brownsword, Roger/Yeung, Karen (Hg.): Regulating Technology, Oxford/Portland, 51-78.

Bright, Jonathan (2011): Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology, in: Surveillance & Society 9 (1/2), 233-247.

Brown, Sheila (2006): The criminology of hybrids: Rethinking crime and law in technosocial networks, in: Theoretical Criminology 10 (2), 223-244.

Busch, Heiner (2010): Vom Militärisch- zum Sicherheitsindustriellen Komplex – eine Einleitung, in: Bürgerrechte & Polizei/CILIP 94 (3), 3-13.
Daston, Lorraine/Galison, Peter (2010): Objectivity, New York.
Egbert, Simon/Paul, Bettina (i.E.): Moderne Verfahren der Lügendetektion als sicherheitspolitische Innovationen – Technikgenese zwischen diskursiven Versprechungen und materialer Intervention, in: Bosančić, Saša/Böschen, Stefan/Schubert, Cornelius (Hg.): Diskursive Konstruktion und schöpferische Zerstörung. Begegnungen von Innovationsforschung und Diskursanalyse, 2. Beiheft der Zeitschrift für Diskursforschung, Weinheim.
Egbert, Simon/Paul, Bettina (2014): Lügendetektion per Neuroimaging – Visuelle Verdachtstechnologien als soziotechnische Ensembles, in: Kriminologisches Journal 46 (3), 153-167.
Egbert, Simon/Thane, Katja/Urban, Monika/Schmidt-Semisch, Henning (2016): Technologisierung des Vertrauens. Zu Drogentestpraktiken im Pflegekinderwesen, in: Neue Praxis (3), 251-262.
Eisenberg, Ulrich/Puschke, Jens/Singelnstein, Tobias (2005): Ubiquitäres Computing = ubiquitäre Kontrolle?, in: Kriminologisches Journal 37 (2), 93-108.
Haggerty, Kevin D. (2004): Displaced expertise: Three constraints on the policy-relevance of criminological thought, in: Theoretical Criminology 8 (2), 211-231.
Haggerty, Kevin D./Ericson, Richard V. (2000): The surveillant assemblage, in: British Journal of Sociology 51 (4), 605-622.
Hayes, Ben (2012): The surveillance-industrial complex, in Ball, Kristie/Haggerty, Kevin D./Lyon, David (Hg.): Routledge Handbook of Surveillance Studies. London/New York, 167-175.
Heinrich, Stephan (2007): Innere Sicherheit und neue Informations- und Kommunikationstechnologien, Münster.
Hughes, Thomas P. (1994): 'Technological Momentum', in: Smith, Merritt Roe/Marx, Leo (Hg.): Does Technology Drive History?, Cambridge, 101-114.
Jones, Richard (2000): Digital Rule: Punishment, Control and Technology, in: Punishment & Society 2 (1), 5-22.
Kaufmann, Stefan (2016): Security Through Technology? Logic, Ambivalence and Paradoxes of Technologised Security, in: European Journal for Security Research 1 (1), 77-95.
Krasmann, Susanne/Kühne, Sylvia (2014): 'My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology, in: Surveillance & Society 12 (1), 1-14.
Kreissl, Reinhard (2011): Privatisierung von Sicherheit, in: Zoche, Peter/Kaufmann, Stefan/Haverkamp, Rita (Hg.): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld, 267-277.
Kreissl, Reinhard/Ostermeier, Lars (2011): Wer hat Angst vorm Großen Bruder?, in: Hempel, Leon/Krasmann, Susanne/Bröckling, Ulrich (Hg.): Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25, 281-298.
Kroener, Inga (2014): CCTV. A Technology Under the Radar?, Farnham/Burlington.
Kroener, Inga/Neyland, Daniel (2012): New technologies, security, and surveillance, in: Ball, Kirstie/Haggerty, Kevin D./Lyon, David (Hg.): Routledge Handbook of Surveillance Studies, London/New York, 141-148.
Kühne, Sylvia/Wehrheim, Jan (2013): Versicherheitlichung und Biometrie. Zur Verbreitung einer Kontrolltechnologie im Spannungsfeld von Staat, Ökonomie und Alltag, in: Klimke, Daniela/Legnaro, Aldo (Hg.): Politische Ökonomie und Sicherheit, Weinheim und Basel, 303-318.
Latour, Bruno (1996): Der Berliner Schlüssel, Berlin.
Latour, Bruno (2002): Die Hoffnung der Pandora, Frankfurt a.M.
Latour, Bruno (2010): Eine neue Soziologie für eine neue Gesellschaft, Frankfurt a.M.
Legnaro, Aldo (1997): Konturen der Sicherheitsgesellschaft: Eine polemisch-futurologische Skizze, in: Leviathan 25, 271-284.

Legnaro, Aldo/Kretschmann, Andrea (2015): Das Polizieren der Zukunft, in: Kriminologisches Journal 47 (2), 94-111.
Leman-Langlois, Stéphane (2008): Introduction: technocrime, in: Ders. (Hg.): Technocrime. Technology, crime and social control, Cullompton/Devon/Portland, 1-13.
Lengersdorf, Diana/Wieser, Matthias (Hg.) (2014): Schlüsselwerke der Science & Technology Studies, Wiesbaden.
Lepsius, Oliver (2004): Freiheit, Sicherheit und Terror. Die Rechtslage in Deutschland, in: Leviathan 43(1), 64-88.
Lianos, Michaelis/Douglas, Mary (2000): Dangerization and the end of deviance, in: The British Journal of Criminology 40 (2), 261-278.
Lindenberg, Michael (1997): Ware Strafe. Elektronische Überwachung und die Kommerzialisierung strafrechtlicher Kontrolle, München.
Linhardt, Dominique (2000): Demokratische Maschinen?, in: Kriminologisches Journal 32 (2), 82-107.
Lösch, Andreas (2012): Techniksoziologie, in: Maasen, Sabine/Kaiser, Mario/Reinhart, Martin/Sutter, Barbara (Hg.): Handbuch Wissenschaftssoziologie, Wiesbaden, 251-264.
Lyon, David (2003): Surveillance Technology and Surveillance Society, in: Misa, Thomas J./Brey, Philip/Feenberg, Andrew (Hg.): Modernity and Technology, Cambridge/London, 161-183.
Marx, Gary T. (2016): Windows into the Soul. Surveillance and Society in an Age of High Technology, Chicago/London.
Massumi, Brian (2015): Ontopower: War, Powers, and the State of Perception. Durham/London.
McCulloch, Jude/Wilson, Dean (2016): Pre-crime. Pre-emption, precaution and the future, London et al.
McGuire, Mike (2007): Hypercrime. The New Geometry of Harm. Abingdon/New York.
Monahan, Torin (2006) (Hg.): Surveillance and Security. Technological Politics and Power in Everyday Life, New York/London.
Neyland, Daniel (2009): Mundane terror and the threat of everyday objects, in: Aas, Katja Franko/Gundhus, Helene Oppen/Lomell, Heidi Mork (Hg.): Technologies of InSecurity. The surveillance of everyday life, Abingdon/New York, 257-270.
Nogala, Detlef (1998): Moderne Überwachungstechnologien, in: Bürgerrechte & Polizei 60 (2), 6-11.
Nogala, Detlef (2000): Der Frosch im heißen Wasser, in: Schulzki-Haddouti, Christiane (Hg.): Vom Ende der Anonymität: Die Globalisierung der Überwachung, Hannover, 139-155.
Opitz, Sven (2012): An der Grenze des Rechts: Inklusion/Exklusion im Zeichen der Sicherheit. Weilerswist.
Paul, Bettina/Egbert, Simon (2016): Drug Testing for Evidence? A Sociotechnical Practice, in: O'Gorman, Aileen/Potter, Gary/Fountain, Jane (Hg.): Evidence in Social Drug Research and Drug Policy, Lengerich, 99-112.
Rammert, Werner (2016): Technik – Handeln – Wissen. Zu einer pragmatistischen Technik- und Sozialtheorie, 2., akt. Aufl., Wiesbaden.
Rauer, Valentin (2012): Interobjektivität: Sicherheitskultur aus Sicht der Akteur-Netzwerk-Theorie, in: Daase, Christopher/Offermann, Philipp/Rauer, Valentin (Hg.): Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr, Frankfurt a.M./New York, 69-91.
Renard, Bertrand (2015): The Relevance of Actor-Network-Theory (ANT) for Research on the Use of Genetic Analysis for Identification in Criminal Justice, in: Robert, Dominique/Dufresne, Martin (Hg.): Actor-Network Theory and Crime Studies, Farnham/Burlington, 113-126.
Robert, Dominique/Dufresne, Martin (Hg.) (2015): Actor-Network Theory and Crime Studies, Farnham/Burlington.
Robert, Dominique/Dufresne, Martin (2015): Introduction: Thinking through Networks,

Reaching for Objects and Witnessing Facticity, in: Dies. (Hg.): Actor-Network Theory and Crime Studies, Farnham/Burlington.
Timan, Tjerk (2013): Surveillance in Urban Nightscapes. A STS-Informed Perspective, in: Tecnoszienca 4 (2), 93-124.
Timan, Tjerk (2016): The body-worn camera as a transitional technology, in: Surveillance & Society, 14 (1), 145-149.
Wagen, Wytske van der/Pieters, Wolter (2015): From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks, in: The British Journal of Criminology 55 (3), 578-595.
Verbeek, Peter Paul (2005): What Things Do? Philosophical Reflections on Technology, Agency, and Design, University Park.
Walters, Williams (2014): Drone strikes, dingpolitik and beyond: Furthering the debate on materiality and security, in: Security Dialogue 45 (2), 101-118.
Wehrheim, Jan (2014): Definitionsmacht und Selektivität in Zeiten neuer Kontrolltechnologien, in: Schmidt-Semisch, Henning/Hess, Henner (Hg.): Die Sinnprovinz der Kriminalität. Wiesbaden, 137-153.
Winner, Langdon (1980): Do Artifacts Have Politics?, in: Daedalus 109 (1), 121-136.
Zedner, Lucia (2009): Epilogue: The inescapable insecurity of security technologies?, in: Aas, Katja Franko/Gundhus, Helene Oppen/Lomell, Heidi Mork (Hg.): Technologies of InSecurity. The surveillance of everyday life, Abingdon/New York, 257-270.
Zurawski, Nils (2015): Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung, Berlin.

Bettina Paul, Universität Hamburg, Institut für Soziologie, Allende Platz 1, 20146 Hamburg, bettina.paul@uni-hamburg.de

Simon Egbert, Universität Hamburg, Institut für Kriminologische Sozialforschung, Allende Platz 1, 20146 Hamburg, simon.egbert@wiso.uni-hamburg.de