Brosius, Hans-Bernd; Mangold, Roland und Schwer, Katja, 2010: Ein Mehrebenenmodell der Mediengewaltforschung. Grundlagen für eine interdisziplinäre Untersuchung der Wirkung von Mediengewalt. Schriftenreihe der Landeszentrale für Medien und Kommunikation. Band 27. Baden-Baden: Nomos Verlagsgesellschaft.

Initiative D21, 2011: (N)ONLINER Atlas. Eine Topographie des digitalen Grabens durch Deutschland. URL: www.initiative21.de/wp-content/uploads/2011/07/NOnliner2011.pdf, letzter Zugriff: 02.09.2011.

Gasser, Urs, 2011: Die Schmähungen sind wie ein Tattoo. Die Zeit vom 7.04.2011: 12.

Grimm, Petra; Rhein, Stefanie und Clausen-Muradian, Elisabeth, 2008: Gewalt im Web 2.0. Der Umgang Jugendlicher mit gewalthaltigen Inhalten und Cybermobbing sowie die rechtliche Einordnung der Problematik. Berlin: Vistas.

Grimm, Petra und Clausen-Muradian, Elisabeth, 2009: Cyber-Mobbing – psychische Gewalt via Internet: „Ja, Beleidigungen, Drohungen. So was halt." (Alba). KJug 54: 33-37.

Hackenberg, Achim, 2007: Workshop I: Jugendgewalt im Internet, Kino und Handyvideos — aus Sicht von Politik, Familie, Wissenschaft, Medienvertretern und Produktion in Deutschland, Litauen, Polen und Estland. In: Görgmeier, Dietmar (Hrsg.): Das Internet als Forum von Jugendgewalt: Herausforderung für Politik, Jugendarbeit, Eltern und Schule in Europa, Europäisches Informations-Zentrum in der Thüringer Staatskanzlei, Reihe Tagungsberichte, Bd. 59, Europe Direct: 219-224.

Hasebrink, Uwe; Livingstone, Sonia; Haddon, Leslie und Olafsson, Kjartan, 2009: Comparing Children's Online Opportunities and Risks across Europe: Cross-National Comparisons for EU Kids Online. London.

Katzer, Catarina und Fetchenhauer, Detlef, 2007: Cyberbullying: Aggression und sexuelle Viktimisierung in Chatrooms. In: Gollwitzer, Mario; Pfetsch, Jan; Schneider, Vera; Schulz, André; Steffke, Tabea; Ulrich, Christiane (Hrsg.): Gewaltprävention bei Kindern und Jugendlichen, Göttingen: Hogreve: 123-140.

Katzer, Catarina; Fetchenhauer, Detlef und Belschak, Frank, 2009: Cyberbullying in Internet-Chatrooms – wer sind die Täter? Ein Vergleich von Bullying in Internet-Chatrooms mit Bullying in der Schule aus der Täterperspektive. Zeitschrift für Entwicklungspsychologie und Pädagogische Psychologie (4)1: 33-44.

Kunczik, Michael und Zipfel, Astrid, 2010: Medien und Gewalt. Befunde der Forschung 2004 – 2009. Bericht für das Bundesministerium für Familie, Senioren, Frauen und Jugend. Kurz- und Langfassung.

Kuttner, Claudia, 2011: Soziale Online-Netzwerke als Erfahrungs- und Entwicklungsraum – Potenziale und Risiken für jugendliche Nutzerinnen und Nutzer. Kerner, Hans-Jürgen; Marks, Erich (Hrsg.): Internetdokumentation des Deutschen Präventionstages. URL: www.praeventionstag.de/Dokumentation.cms/1361, letzter Zugriff: 02.09.2011.

Landesstelle Jugendschutz Niedersachsen, 2010: Cybermobbing. Medienkompetenz trifft Gewaltprävention. Hannover.

Livingstone, Sonia; Haddon, Leslie; Görzig, Anke und Olafsson, Kjartan, 2011: Risks and Safety on the internet. The perspective of European children. Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries, URL: www.hans-bredow-institut.de/webfm_send/553, letzter Zugriff: 24.03.2011.

Medienpädagogischer Forschungsverbund Südwest (Hrsg.), 2011: JIM 2011. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-jähriger in Deutschland. Stuttgart, URL: http://www.mpfs.de/fileadmin/JIM-pdf11/JIM2011.pdf, letzter Zugriff: 10.02.2012.

Schorb, Bernd; Kießling, Matthias; Würfel, Maren und Keilhauer, Jan, 2010: Medienkonvergenz Monitoring. Soziale Online-Netzwerke-Report 2010 (MeMo). Leipzig.

Ring, Wolf-Dieter, 2007: Das Internet als Forum für Jugendgewalt: Herausforderung für Politik, Jugendarbeit, Eltern und Schule in Europa. In: Görgmeier, Dietmar (Hrsg.): Das Internet als Forum von Jugendgewalt: Herausforderung für Politik, Jugendarbeit, Eltern und Schule in Europa, Europäisches Informations-Zentrum in der Thüringer Staatskanzlei, Reihe Tagungsberichte, Bd. 59, Europe Direct: 31-38.

Steffen, Wiebke, 2011: Gutachten für den 16. Deutschen Präventionstag. Kerner, Hans-Jürgen; Marks, Erich (Hrsg.): Internetdokumentation des Deutschen Präventionstages. Hannover 2011, URL: www.praeventionstag.de/Dokumentation.cms/1310, letzter Zugriff: 02.09.2011.

Van Eimeren, Birgit und Frees, Beate, 2010: Fast 50 Millionen Deutsche online – Multimedia für alle? Ergebnisse der ARD/ZDF-Onlinestudie 2010. Media Perspektiven (7) 8: 334-379.

Wagner, Ulrike, 2008: Medienhandeln in Hauptschulmilieus. Mediale Interaktion und Produktion als Bildungsressource. München.

Willard, Nancy E., 2007: Cyberbullying and Cyberthreats. Champaign, Illinois: Research Press.

PSB/Bundesministerium des Innern und Bundesministerium der Justiz (Hrsg.), 2006: Zweiter Periodischer Sicherheitsbericht. Berlin: Eigenverlag.

BUCHTIPP

Sandro Gaycken (Hg.)
Jenseits von 1984 – Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft – Eine Versachlichung
Bielefeld 2013, (transcript) Verlag, 166 Seiten, ISBN 978-3-8376-2003-0, 19,80 €

Der Herausgeber Dr. Sandro Gaycken forscht im Fachbereich Informatik an der Freien Universität Berlin zu Datenschutz, Datensicherheit, Cyberwarfare, Cybercrime, Hacking und zu Utopien der Informationsgesellschaften. Zudem ist er derzeit Politikberater im Planungsstab des Auswärtigen Amtes. Das von ihm herausgegebene Buch „Jenseits von 1984" ist kurz vor den Enthüllungen durch Edward Snowden erschienen.

Der Sammelband mit insgesamt neun Beiträgen hat den Anspruch, zur Versachlichung der Debatte um digitale Überwachung beizutragen, was den Autoren auch gelingt. Die Artikel liefern wissenschaftliche und praktische Perspektiven auf Wahrnehmung und Realität der Überwachung, illustrieren einige wichtige Begründungen der Überwachungsbefürwortung und -kritik und beleuchten die irrationalen und agitativen Momente im Diskurs. Das Buch gliedert sich in vier Teile (Elemente sowie Konstitution des Überwachungsdiskurses, Strukturen der Überwachung und Begründung des Datenschutzes).

Der *erste Teil* stellt den Überwachungsdiskurs strukturell mit seinen argumentativen Schwächen und Problemen auf den Prüfstand und zeigt, welche Dimensionen in einem sachlichen Diskurs zu behandeln wären und welche Rollen die Vermittler in einer weiterentwickelten Informationsgesellschaft einnehmen müssten.

Sandro Gaycken bespricht zunächst die Tragfähigkeit einiger prominenter politischer Argumente. Sicherheitsbefürworter betonten, dass es keine Freiheit ohne Sicherheit geben könne, während Freiheitsbefürworter meinten, dass Sicherheit ohne Freiheit nicht lebenswert sei. Beide Positionen scheinen überzogen. Die richtige Balance sollte gefunden werden, „die detailreich und vorsichtig ermessen werden muss: […] Wie viel oder wie wenig Sicherheit darf oder muss es denn sein?" Unsicherheitsmaße, Art und Ausmaß von Freiheitseinschränkungen und die Überwachungseffektivität lassen sich feststellen. Alternativenvergleiche zwischen z. B. technischen und personalgestützten Ansätzen unter Berücksichtigung von Kosten-Nutzen-Erwägungen sind grundsätzlich möglich. Das Ausmaß an Freiheit hingegen, das benötigt wird, ist schwieriger zu bestimmen. Gaycken bringt es auf den Punkt: „Unfreiheit durch zu viel Sicherheit ist weit schwieriger zu messen als die in ihren jeweiligen Akten krimineller Handlungen konkretisierbare Unsicherheit." Mehr als die sinngemäß wiedergegebene Grundregel „Freiheitsbegrenzungen nur bei hohem Sicherheitsbedarf und Mangel an anderen milderen Eingriffsmitteln" bietet der Herausgeber zur Orientierung allerdings nicht an. Er erläutert sodann die Erkenntnis, „dass technische Überwachung nicht so effektiv

ist, wie die liefernden Firmen es versprochen hatten." Nach weiteren Erörterungen zum überschätzten Nutzen bzw. zur überschätzten Gefahr der Technik räumt er vor dem Hintergrund des noch recht neuen technologischen Fortschritts bei der Datenüberwachung ein, dass es für eine Entwarnung im Hinblick auf damit einhergehende Freiheitsverluste in den westlichen Demokratien wohl noch zu früh sei. Dennoch bleibt er bei seinem Optimismus, denn mediale und politische Kultur würden eine systematische und missbräuchliche institutionelle Kontrolle der Gesellschaft nicht erlauben. Die Informationsgesellschaft sei ausreichend aufmerksam und vorsichtig. Eine brisante Frage wird schließlich aufgeworfen: Ob die deutsche Forschungs- und Entwicklungspolitik nicht unter erhöhte Beobachtung und Kontrolle gestellt werden müsse, wenn zu befürchten stehe, dass aus dem dabei entwickelten Wissen Kontrolltechnik in totalitären Regimen entstehe und zum Einsatz komme.

Patrick Voss-de Haan legt im folgenden Beitrag dar, wie ein sachlicher Diskurs zu Überwachung eine Balance herstellen kann, die im Interesse der Gesellschaft wäre. Dazu skizziert er, welche Vermittler für eine neutrale Genese von Wissen und Meinen geeignet scheinen. Er schlägt u. a. eine neutrale Institution vor, die unterschiedliche Positionen aufbereitet und einen wirklich informierten Diskurs ermöglicht.

Im *zweiten Teil* geht es um die konstituierenden Elemente des Überwachungsdiskurses. Es wird betrachtet, wie Meinungen und Wissen real entstehen und sich entwickeln, auf welche Grundperspektiven sich einige Einstellungen zurückführen lassen und welche Rolle die Meinungsgeber haben.

Gabriel Brönnimann untersucht den Überwachungsdiskurs am Beispiel der Vorratsdatenspeicherung und verdeutlicht die Grundmotive der Streitenden anhand der jeweiligen Extrempositionen: Utopie eines Internets, das vollkommen frei von jeglicher Kontrolle ist vs. Dystopie eines Cyberspace, der bis in den letzten Winkel kontrolliert, überwacht und zensiert wird.

Kai Biermann schildert aus der Perspektive eines Fachjournalisten den Umgang der Medien mit Sicherheitsthemen, die prädestiniert seien für eine durch Sensationen getriebene Berichterstattung: „... sie wecken Emotionen ..., sie bieten Orientierung im Sinne von Gut und Böse, sie lassen sich personalisieren und skandalisieren." Dass dabei Stereotype transportiert, Konflikte geschürt und Ausgrenzung forciert werden, werde von den vielen Journalisten vielleicht bedauert, aber im Zweifel wohl in Kauf genommen. Der Beitrag illustriert die Mechanismen bundesdeutscher Medien am Beispiel der Terrorismusberichterstattung. Bezüge zum in Rede stehenden Überwachungsdiskurs müssen die Leser allerdings selbst herstellen.

Im *dritten Teil* des Bandes geht es um die Internetüberwachung: warum sie notwendig ist, unter welchen Bedingungen sie funktionieren muss und wie sie konkret eingesetzt wird.

Wendy Füllgraf beschreibt Art und Umfang der Informations- und Kommunikationskriminalität anhand des BKA-Lagebildes (Formen, Ausmaß, Täter, Opfer, Schäden). Sie weist zutreffend auf die überdurchschnittliche Dynamik und Schnelllebigkeit der IuK-Kriminalität hin und klassifiziert sie nach ihrer Zielrichtung bzw. Funktion: *Manipulative Vermögensverschiebungen* (Missbrauch von Kreditkarten, Identitätsdiebstahl/Phishing, Manipulation von Aktienkursen, Missbrauch beim Vertreiben von Waren über Datennetze, Betrugsdelikte unter Ausnutzung der Informationstechnologie und Erpressung), *Nutzungsbeeinträchtigungen* (Entstellung von Webseiten, Viren und Würmer, Systemabstürze mit Hilfe von Botnetzen), *Informationsverschaffung* (Hacking und Spionage) und *Kommunikationsdelikte* (Spams, Kommunikation missbilligter Inhalte). Mobile Endgeräte wie Handys, Smartphones, vernetzte Steuerungssysteme im Haushalt oder in Autos werden, so Füllgraf, die zukünftigen Zielobjekte der IuK-Delikte sein. Dies gehe einher mit einer Professionalisierung der Täter durch „social engineering" (Aufbau von Vertrauensverhältnissen insbesondere in sozialen Netzwerken).

Das Autorenkollektiv Andreas Dewald, Felix C. Freiling, Sven Schmitt, Michael Speitzenbarth und Stefan Vömel erklärt die heutigen und einige zukünftige Voraussetzungen und Wege der Forensik in digitalen Medien. Sie zeigen, unter welchen Umständen bestimmte Ermittlungsbefugnisse notwendig sind, um Straftaten überhaupt verfolgen zu können und wie Beweise mit den Mitteln der forensischen Informatik beschafft werden können. Dabei thematisieren sie Gefahren für Datenschutz und Freiheit und stellen vor, in welchen Konstellationen es aber keine Alternativen zu IT-forensischen Methoden gibt. Sie fragen sodann nach technikimmanenten Grenzen bei der digitalen Spurensuche und erläutern Beispiele.

Im *vierten Teil* untersuchen die Autoren, worauf Datenschutz eigentlich beruht und was davon auf welche Art und Weise argumentativ und empirisch unterlegt werden kann.

Nils Zurawski beschreibt Probleme der Messung der Bedrohung von Freiheit durch Sicherheit. Dabei stellt er an einigen Beispielen heraus, dass viele Betrachtungen zu einseitig auf technische Merkmale ausfallen und die tatsächliche Rolle der Technik bei ihrer Anwendung sowie für die Lebenswelt zu wenig herausgestellt wird.

Christian Lüdemann und Christina Schlepper stellen abschließend die Ergebnisse einer Studie vor, die verschiedene Relationen von Angst im Kontext von Überwachung untersucht. Eine Frage betrifft die direkten und indirekten Effekte der Furcht vor Kriminalität und Terrorismus auf die individuelle Bewertung bzw. Akzeptanz neuer staatlicher Kontrolltechnologien.

Der gut verständliche und nicht zu umfangreiche Sammelband ist allen Lesern/-innen zu empfehlen, die Interesse an unterschiedlichen Positionen und Argumenten haben, die ihre Meinungsbildung noch nicht als endgültig abgeschlossen sehen und daher an der ständigen Fortentwicklung einer konstruktiven Balance zwischen Kontrolle und Freiheit mitwirken wollen. Ob die Zukunft *„Jenseits von Orwell"* gestaltet werden kann, bleibt eine offene Frage und bedarf angesichts NSA intensiver medialer und zivilgesellschaftlicher Aufmerksamkeit.

Wolfgang Kahl

Veranstaltungshinweis

13. Tagung der Kriminologischen Gesellschaft (KrimG)

„Risiken der Sicherheitsgesellschaft"

26.9. bis 28.9.2013
in Fribourg/Schweiz

http://www.unifr.ch/ius/krimg2013/home