Constantin Goschler, Christopher Kirchberg, Jens Wegener

Sicherheit, Demokratie und Transparenz

Elektronische Datenverbundsysteme in der Bundesrepublik und den USA in den 1970er und 1980er Jahren

DOI (Artikel): 10.14765/zzf.dok-2619

In: Frank Bösch (Hg.), Wege in die digitale Gesellschaft. Computernutzung in der Bundesrepublik 1955-1990, Göttingen 2018, S. 64–85.

DOI (Band): 10.14765/zzf.dok-2642

Digitaler Reprint des ursprünglich in der ZZF Schriftenreihe **Geschichte der Gegenwart** im Wallstein Verlag im September 2018 erschienenen Sammelbandes:
https://zzf-potsdam.de/de/publikationen/wege-die-digitale-gesellschaft

https://doi.org/10.14765/zzf.dok-2619

Wege in die digitale Gesellschaft

Computernutzung in der Bundesrepublik 1955 – 1990

Herausgegeben von
Frank Bösch

https://doi.org/10.14765/zzf.dok-2619

Inhalt

https://doi.org/10.14765/zzf.dok-2619

https://doi.org/10.14765/zzf.dok-2619

Sicherheit, Demokratie und Transparenz

Elektronische Datenverbundsysteme in der Bundesrepublik und den USA in den 1970er und 1980er Jahren

Constantin Goschler,
Christopher Kirchberg und Jens Wegener[1]

Seit einigen Jahren versorgen Whistleblower und Wikileaks die Öffentlichkeit regelmäßig mit aktuellen Updates über die Praktiken des Sammelns und Auswertens von Daten durch geheime Nachrichtendienste. Solche Enthüllungen betrafen bislang allein westliche liberale Demokratien wie die USA und die Bundesrepublik, wo Transparenz eine zentrale politische Norm darstellt. Mit den Überwachungs- und Datensammelpraktiken der Geheimdienste verbindet sich in solchen Ländern eine doppelte Problemstellung: Erstens geht es um die mit dem Argument der Sicherheit legitimierte Durchleuchtung von Bürgern durch Nachrichtendienste. Demgegenüber steht zweitens die mit dem Recht auf demokratische Kontrolle begründete Forderung das Arkanum staatlicher Sicherheitsbehörden zu durchleuchten. Dem traditionellen Prinzip »Sehen und nicht gesehen werden« solcher Behörden stehen also politische und gesellschaftliche Akteure gegenüber, welche die elektronischen Datensammlungen geheimer Nachrichtendienste kritisieren und ihrerseits deren Tätigkeit öffentlich überprüfbar machen wollen. In Anlehnung an den Begriff der *counter-surveillance*[2] ließe sich also von Gegenüberwachung sprechen, die auch den Nachrichtendiensten Transparenz abverlangt.

Auf diese Weise bestehen also reziproke Transparenzansprüche, bei denen sich staatliche Sicherheitsbehörden und zivilgesellschaftliche Akteure gegenseitig zu visibilisieren[3] suchen beziehungsweise sich umgekehrt

1 Wir danken unseren Bochumer Kollegen Michael Wala, Marcus Böick und Marcel Schmeer für die intensiven Diskussionen und zahlreiche wichtige Hinweise.

2 Christian Fuchs et al.: Introduction: Internet and Surveillance, in: dies. (Hg.): Internet and Surveillance. The Challenges of Web 2.0 and Social Media, New York/London 2012, S. 1-28, hier: 13 ff.; Thomas Christian Bächle: Digitales Wissen, Daten und Überwachung zur Einführung, Hamburg 2016, S. 177.

3 Herfried Münkler unterscheidet zwischen Visibilisierung als Prozessbegriff und Transparenz als Strukturbegriff. Siehe ders.: Die Visibilität der Macht und die Strategien der Machtvisualisierung, in: Herfried Münkler/Jens Hacke (Hg.): Strategien der Visualisierung. Verbildlichung als Mittel politischer Kommunikation, Frankfurt a. M./New York, 2009, S. 213-230, hier: S. 214 f.

https://doi.org/10.14765/zzf.dok-2619

darum bemühen, solchen Ansprüchen zu entkommen. Doch besteht dabei ein strukturelles Ungleichgewicht der gegenseitigen Transparenzforderungen, das politisch legitimiert werden muss. Denn in liberalen Demokratien stützt sich Transparenz »auf die Vorstellung des ›Gesellschaftsvertrags‹, wonach ›freie Individuen‹ im Tausch für die Gewähr von Schutz und Sicherheit einen Teil ihrer Freiheit delegieren. Hier müssen die Autoritäten der Öffentlichkeit verlässliche Informationen liefern, um als vertrauenswürdig und verantwortlich angesehen zu werden.«[4] Es geht hier also um die grundsätzliche Frage von Vertrauen und Misstrauen gegenüber Sicherheitsinstitutionen in demokratisch verfassten Staaten.[5]

Ausgehend von diesen Überlegungen bietet der folgende Beitrag einen Problemaufriss eines für liberale Demokratien zentralen Konflikts, dem weitere empirisch gestützte Untersuchungen folgen sollen: Einerseits sammeln Sicherheitsbehörden unter Berufung auf das staatliche Sicherheitsversprechen technologisch unterstützt private Daten. Andererseits wird in der Öffentlichkeit der Schutz privater Informationen sowie die Überprüfbarkeit und Kontrolle staatlicher Handlungen gefordert. Im Mittelpunkt stehen dabei die auf mehreren Ebenen eng verflochtenen Entwicklungen in der Bundesrepublik und den USA in den 1970er und 1980er Jahren. Wie entwickelte sich also im Zusammenhang des Auf- und Ausbaus computergestützter Datenverbundsysteme westdeutscher und nordamerikanischer Sicherheitsdienste das genuin westliche Spannungsfeld von Sicherheit, Demokratie und Transparenz?

Eine erste für diesen Beitrag wichtige Zäsur liegt in den späten 1960er Jahren, als in den USA und der Bundesrepublik mit der Digitalisierung der analogen Datensammlungen begonnen wurde und sich dadurch der Umfang des Materials wie auch die Qualität und die Geschwindigkeit der Auswertung substanziell erweiterten. Der Übergang von Kartei- und Lochkarten zu Magnetbändern und elektronischen Computern und eine »neue Unübersichtlichkeit« der Gegner, die mit der Überlagerung herkömmlicher antikommunistischer Feindbilder durch amorphe Bürgerrechtsbewegungen und Neue Linke einherging, trafen in dieser Situation zusammen. Diese Zäsur lässt sich somit gleichermaßen technisch wie gesellschaftlich und politisch bestimmen.

4 Hans Krause Hansen/Mikkel Flyverbom: The Politics of Transparency and the Calibration of Knowledge in the Digital Age, in: Organization 22 (2014), S. 1-18, hier: S. 3 (Übersetzung durch Verf.).

5 Siehe dazu etwa Ivan Krastev: In Mistrust We Trust. Can Democracy Survive When We Don't Trust our Leaders, TED Conferences 2013; ders.: Der Transparenzwahn, in: Transit. Europäische Revue 44 (2013), S. 7-24.

https://doi.org/10.14765/zzf.dok-2619

Die Jahre 1983/84 markieren vor allem in der Bundesrepublik eine weitere Zäsur.[6] Mit dem Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 errangen die Verfechter der Idee des Datenschutzes einen wichtigen Erfolg. Und im darauffolgenden Jahr 1984, welches durch den gleichnamigen Roman George Orwells den Erwartungshorizont für die Dystopie einer panoptisch strukturierten Überwachungsgesellschaft markiert hatte, schien der Bann der zentralen Großrechenanlagen bereits durch den Siegeszug des Personal Computers gebrochen zu sein. Apple, heute eher ein Symbol der Vorliebe globaler Konzerne für Länder ohne transparente Steuerpraktiken,[7] propagierte 1984 bei der Einführung des Macintosh Computers werbewirksam den Gegensatz von totalitärem Zentralcomputer und demokratisch-individualistischem Mac.[8]

Diese vor allem medial bestimmte Zäsur wird in diesem Beitrag, der den Fokus auf die Datenbanksysteme der Sicherheitsdienste legt, zugunsten eines Einschnittes am Ende des Jahrzehnts überschritten. Denn mit dem Ende des Kalten Krieges und dem Wegfall der Sowjetunion als bisheriger Hauptgegner veränderte sich die Gegnerkonstellation nordamerikanischer und westdeutscher geheimer Nachrichtendienste so fundamental, dass zuvor durch den Ost-West-Gegensatz verdeckte Gefahren aufgewertet wurden. Zudem spricht einiges dafür, dass im darauffolgenden »neoliberalen« Jahrzehnt Computertechnologie vor allem als Teil der Privatwirtschaft angesehen wurde und die gesellschaftliche Aufmerksamkeit vorübergehend von der nachrichtendienstlichen Datensammelpraxis abgezogen wurde. Dies fällt nicht zufällig mit einer weiteren Zäsur zusammen: Denn nachdem 1989 im CERN die Grundlagen des WWW gelegt wurden, beschloss 1990 die National Science Foundation, das bis dahin lediglich für Universitäten zugängliche Internet für die kommerzielle – und damit auch privatwirtschaftliche – Nutzung zu öffnen.

6 Zur Frage der Zäsuren der Computerisierung vgl. etwa Jürgen Danyel: Zeitgeschichte der Informationsgesellschaft, in: Zeithistorische Forschungen/Studies in Contemporary History 9, 2 (2012), S. 186-211; ders./Annette Schumann: Wege in die digitale Moderne. Computerisierung als gesellschaftlicher Wandel, in: Frank Bösch (Hg.): Geteilte Geschichte. Ost- und Westdeutschland 1970-2000, Göttingen 2015, S. 283-320.

7 Siehe etwa Bastian Brinkmann/Lena Kampf: Neue Heimat, in: Süddeutsche Zeitung vom 7.11.2017.

8 Vgl. David Gugerli/Hannes Mangold: Betriebssysteme und Computerfahndung. Zur Genese einer digitalen Überwachungskultur, in: Geschichte und Gesellschaft 42 (2016), S. 144-174; Hannes Mangold: Fahndung nach dem Raster. Informationsverarbeitung bei der bundesdeutschen Kriminalpolizei, 1965-1984, Zürich 2017, S. 217.

https://doi.org/10.14765/zzf.dok-2619

Die zeithistorische Erforschung der Datenverarbeitung der Sicherheitsbehörden und Nachrichtendienste hat erst vor kurzem begonnen, den von Überwachungsphantasien aller Art geprägten zeitgenössischen Protestdiskurs zu überschreiten. Der Blick richtet sich dabei einerseits auf Menschen und Organisationen und greift dazu insbesondere auf politikwissenschaftliche und organisationssoziologische Ansätze zurück.[9] Dafür steht etwa die Arbeit Rüdiger Bergiens, der die Computerisierung als Faktor des Organisationswandels von Bundeskriminalamt und Ministerium für Staatssicherheit ins Zentrum seiner Untersuchung stellt.[10] Die neuere, stark kulturwissenschaftlich interessierte Technik- und Wissensgeschichte analysiert diesen Gegenstand andererseits bevorzugt mit einem poststrukturalistisch orientierten Subjektbegriff und integriert insbesondere unter Bezug auf Bruno Latours Akteurs-Netzwerk-Theorie auch Computer in ihr aus dem Zusammenhang von Menschen und Dingen geprägtes Akteurskonzept.[11] Aus einer solchen Perspektive untersucht Hannes Mangold die Informationsverarbeitung bei der bundesdeutschen Kriminalpolizei zwischen 1965 und 1984 im Spannungsfeld von Wissen und Sicherheit.[12] Demgegenüber analysiert Larry Frohman in der Perspektive einer politischen Kulturgeschichte die zivilgesellschaftlichen Reaktionen auf den Ausbau von Datenverbundsystemen in der Bundesrepublik.[13] Damit überträgt er den Blick der amerikanischen Historiografie, die den Einsatz von Datenbanken lange als Nebenaspekt der Geschichte der US-Bürgerrechtsbewegung und der Watergate-Affäre behandelte, auf die Bundesrepublik. Vor allem durch die Rezeption der stark soziologisch geprägten Intelligence und Surveillance Studies steigt jedoch auch in der anglo-amerikanischen Historiografie das Interesse an der technischen Dimension geheimdienstlicher Arbeit.[14] Der besondere

9 In diese Richtung weisen auch die Überlegungen zur Surveillance History von Sven Reichardt: Einführung. Überwachungsgeschichte(n). Facetten eines Forschungsfeldes, in: Geschichte und Gesellschaft 42 (2016), S. 5-33.

10 Rüdiger Bergien: »Big Data« als Vision. Computereinführung und Organisationswandel in BKA und MfS, in: Zeithistorische Forschungen/Studies in Contemporary History 14, 2 (2017), S. 258-285.

11 Gugerli/Mangold: Betriebssysteme und Computerfahndung, S. 145 f.

12 Mangold: Fahndung nach dem Raster.

13 Larry Frohman: Datenschutz, the Defense Law, and the Debate over Precautionary Surveillance. The Reform of Police Law and the Changing Parameters of State Action in West Germany, in: German Studies Review 38, 2 (2015), S. 307-327; ders.: »Only Sheep Let Themselves Be Counted«. Privacy, Political Culture, and the 1983/87 West German Census Boycotts, in: Archiv für Sozialgeschichte 52 (2012), S. 335-378.

14 Siehe etwa Rhodri Jeffreys-Jones: We Know All About You: The Story of Surveillance in Britain and America, Oxford 2017.

https://doi.org/10.14765/zzf.dok-2619

Reiz und die spezifische Herausforderung der Erforschung der nachrichtendienstlichen Datenbanken liegen also gerade darin, politik- und technikhistorische Perspektiven zusammenzuführen.

Die folgenden Überlegungen wollen die Möglichkeiten einer solchen integrierten Perspektive ausloten und damit zugleich einen Beitrag leisten, um die zumeist stark präsentistisch geführte Diskussion um die »gegenwärtigen Überwachungsverhältnisse in eine längerfristige historische Perspektive zu rücken«.[15] Dies geschieht in drei Schritten: *Erstens* wird nach dem Verhältnis zwischen den neuen technischen Möglichkeiten und den veränderten Gefahrenwahrnehmungen im transatlantischen Kontext gefragt, die sich bei Auf- und Ausbau computergestützter Datenbanken ergaben. Dabei konzentriert sich der Beitrag vor allem auf bundesdeutsche und US-amerikanische Nachrichtendienste, nämlich das Bundesamt für Verfassungsschutz, die CIA und das FBI, die hier exemplarisch für die netzwerkartigen Handlungszusammenhänge innerhalb des westlichen Bündnisses stehen. *Zweitens* werden die gesellschaftlichen und politischen Reaktionen auf den Aufbau dieser Datenverbundsysteme der Sicherheitsbehörden untersucht. Hierbei geht es um das Verhältnis zwischen der Abwehr von auf die Bürger gerichteten staatlichen Visibilisierungsansprüchen einerseits und um umgekehrte Visibilisierungsforderungen gegenüber den staatlichen Sicherheitsbehörden andererseits. Die zentralen Akteure auf dieser Untersuchungsebene sind dabei zivilgesellschaftliche Protestgruppen und Teile der medialen Öffentlichkeit. *Drittens* und letztens geht es schließlich um die politische Aushandlung von Sicherheitskonflikten und Sichtbarkeitsregimes. Im Mittelpunkt stehen die gesetzlichen Regelungen, mit denen die einander entgegengesetzten Transparenzforderungen von Nachrichtendiensten und kritischen Teilöffentlichkeiten adressiert wurden. Auf diese Weise sollen schließlich einige vorläufige Deutungslinien zum Wandel des Spannungsverhältnisses von Sicherheit, Demokratie und Transparenz im transatlantischen Bezugsrahmen in den 1970er und 1980er Jahren entworfen werden.

Die »Krise der Erkennbarkeit des Feindes« und die Ambivalenzen der elektronischen Visibilisierung

Wie reagierten also die Sicherheitsbehörden in den USA und der Bundesrepublik auf die in beiden Ländern seit den 1960er Jahren einsetzende gesellschaftliche Liberalisierung? Wie änderte sich ihre Gefahrenwahr-

15 Siehe Reichardt: Einführung, S. 6 f.

https://doi.org/10.14765/zzf.dok-2619

nehmung in der folgenden Zeit und welche Erwartungen und Strategien der Überwachung – und damit der Sichtbarmachung – der jeweiligen Gegner diskutierten beziehungsweise realisierten sie? Und welche Rolle spielten dabei transatlantische Austauschprozesse? Die Wechselwirkungen zwischen Unsichtbarkeit und Sichtbarmachung des Gegners auf beiden Seiten des Atlantiks müssen somit aus dem Zusammenwirken von Einstellungen, Praktiken und technischen Infrastrukturen in einer veränderlichen gesellschaftlichen und innen- wie außenpolitischen Umwelt erklärt werden. Dazu gehören insbesondere die Auswirkungen des zweiten Kalten Krieges in den 1980er Jahren sowie des von den Sicherheitsdiensten nicht vorhergesehenen Endes des Kalten Krieges 1989/90.

In der Bundesrepublik und in den USA bauten das Bundesamt zusammen mit den Landesämtern für Verfassungsschutz, das US-Justizministerium, die Central Intelligence Agency (CIA) sowie auch das Federal Bureau of Investigation (FBI) seit Ende der 1960er umfangreiche elektronische Datenverbundsysteme auf, wobei diese Institutionen vielfältig kooperierten. Diese Entwicklung lässt sich als Folge einer gleichermaßen politischen und semiotischen Repräsentationskrise innerhalb der westlichen Demokratien, namentlich in den USA und der Bundesrepublik, interpretieren: In beiden Ländern stellten zumindest Teile der Gesellschaft die Legitimität der politischen und wirtschaftlichen Ordnung infrage.[16] Umgekehrt entwickelte sich »die Gesellschaft« für die Sicherheitsbehörden zu einer Quelle neuer, unsichtbarer Gefahren, die sich nicht mehr adäquat beschreiben ließen.[17] Die in den vorangegangenen Jahrzehnten gefestigte Orientierung der Nachrichtendienste auf den sowjetischen Kommunismus wurde von einer diffusen Gefahrenwahrnehmung überlagert, in deren Mittelpunkt Bürgerrechtsbewegungen, Neue Linke und im weitesten Sinne alternative Lebensformen standen. Die Sicherheitsbehörden reagierten auf diese »Krise der Erkennbarkeit des Feindes«[18] mit dem Aufbau von Datenverbundsystemen, welche diese politischen Gefährdungen nun sichtbar machen sollten. Die Kausalitätsbeziehungen zwischen Gefahrenwahrnehmung und Technik sind allerdings komplex. Wären diese Datenverbundsysteme auch ohne eine

16 Charles Maier: Malaise. The Crisis of Capitalism in the 1970s, in: Niall Ferguson u. a. (Hg.): The Shock of the Global. The 1970s in Perspective, Cambridge, MA, 2010, S. 25-48; Bruce Schulman: The Seventies. The Great Shift in American Culture, Society, and Politics, New York, NY, 2001, S. XV.

17 Constantin Goschler/Michael Wala: »Keine neue Gestapo«. Das Bundesamt für Verfassungsschutz und die NS-Vergangenheit, Reinbek bei Hamburg 2015, S. 261-264.

18 Eva Horn: Der geheime Krieg. Verrat, Spionage und moderne Fiktion, Frankfurt a. M. 2007, S. 382-386.

https://doi.org/10.14765/zzf.dok-2619

solche Transformation der Gegnerschaft aufgebaut worden? Oder hat nicht, gerade umgekehrt, der Aufbau von Datenverbundsystemen die Konstruktion pluralisierter Gegnerkonstellationen erst ermöglicht und Letztere zugleich sichtbar gemacht? Vieles spricht dafür, dass sich beide Momente in dieser Entwicklung gegenseitig dynamisierten.

Das Nachrichtendienstliche Informationssystem (NADIS) des Bundesamts und der Landesämter für Verfassungsschutz ebenso wie das im Rahmen der Operation MH/CHAOS von der CIA aufgebaute rechnergestützte Datenverbundsystem HYDRA sammelten und indizierten Daten von Individuen und Organisationen verdächtig erscheinender Individuen und Organisationen. Handelt es sich bei NADIS um eine Abkürzung, die allenfalls bei Freunden fernöstlicher Medizin einige Assoziationen auszulösen vermag, war HYDRA offenbar ein freigewählter Codename, der ein Schlaglicht auf die damit verbundenen Bedrohungsvorstellungen wirft. Diese Datenverbundsysteme schufen neue Möglichkeiten der Analyse und Fahndung, die zeitgenössisch unter den Schlagwörtern »Rasterfahndung« und »Profiling« diskutiert wurden. Dies erfolgte unabhängig davon, dass zumindest Erstere vom Verfassungsschutz gar nicht praktiziert wurde, denn die Öffentlichkeit unterschied kaum zwischen den verschiedenen Nachrichten- und Sicherheitsdiensten. Während in der Bundesrepublik die Suche nach »Extremisten«, »Terroristen« und ihren »Sympathisanten« im Mittelpunkt der Datensammlung stand, wurden in den USA vor allem Gegner des Vietnam-Krieges und Bürgerrechtsgruppen erfasst. Dies löste heftige gesellschaftliche Debatten aus, die in den USA Mitte der 1970er Jahre im Umfeld der Watergate-Affäre den Abbruch des Programms bewirkten.[19] In der Bundesrepublik bewirkten die öffentlichen Datenschutzdebatten dagegen, dass 1979 die weit fortgeschrittene Planung weiterer Ausbaustufen von NADIS ad acta gelegt und die direkte Verkoppelung von NADIS mit INPOL, dem Datenverbundsystem des Bundeskriminalamtes, aufgegeben wurde. Ansonsten wurde das Informationssystem aber weiterbetrieben und bis heute immer weiter ausgebaut. Seit 2012 wird es als modernisierte Version NADIS WN (Nachrichtendienstliches Informationssystem Wissensnetz) betrieben.[20]

Aufgrund der seit den späten 1960er Jahren aufkommenden transnationalen Vernetzung von Protestgruppen intensivierten auch die Sicherheitsbehörden in der Bundesrepublik und in den USA die bisherigen Formen der transatlantischen Kooperation. Bereits in den späten 1960er

19 Rafalko: MH/CHAOS, S. 191.

20 Siehe dazu Mögliche Bespitzelung von Journalistinnen und Journalisten durch den Verfassungsschutz auch außerhalb Niedersachsens, 21.08. 2104. in: BT-Drucksache 18/2384, http://dipbt.bundestag.de/dip21/btd/18/023/1802384.pdf

https://doi.org/10.14765/zzf.dok-2619

Jahren nutzten FBI und CIA die *legal attaches* des US-Justizministeriums, um mit ausländischen Diensten die Überwachung der Reiseaktivitäten amerikanischer Dissidenten zu koordinieren. Dieser zunächst unstrukturierte Informationsaustausch erlangte Mitte der 1970er Jahre im Zuge der Terrorismusbekämpfung größere Bedeutung. Der terroristische Angriff auf die Olympischen Sommerspiele in München 1972, der den dort unternommenen Versuch eines unsichtbaren Sicherheitskonzepts in einem Debakel enden ließ, bildete ein einschneidendes Datum, auch wenn die darauffolgende »Erfindung« des Terrorismus[21] als »Staatsfeind« auf früheren Praktiken und Wissensbeständen aufbaute.

1970 hatte ein erstes Treffen westlicher Sicherheitsdienste unter Beteiligung von FBI und Bundesamt für Verfassungsschutz intensivierte internationale Kooperation und insbesondere gegenseitigen Datenaustausch als Mittel gegen transnationale Gewaltnetzwerke identifiziert.[22] Seit Mitte der 1970er Jahre arbeiteten die Sicherheitsbehörden im Bereich der Terrorismusbekämpfung auch auf europäischer Ebene immer enger zusammen.[23] Spätestens seit den 1980er Jahren wurden EDV-gestützte Techniken der Quantifizierung und Netzwerkanalyse konstitutiv für die Konsolidierung eines Feldes der Terrorismusforschung, das Sicherheitsbehörden, Universitäten und Forschungsinstitute verband. Private Institutionen wie die RAND Corporation oder die vom ehemaligen CIA-Mitarbeiter Edward F. Mickolus initiierte ITERATE-Datenbank (»International Terrorism: Attributes of Terrorist Events«) bauten Datenrepositorien terroristischer Zwischenfälle auf, die von einem »unsichtbaren Kollegium« (Reid and Chen) internationaler Terrorismusexperten zu Auswertungs- und Publikationszwecken genutzt wurden.[24] In Zukunft gilt es aber noch genauer zu untersuchen, inwieweit das Bestreben nach Sichtbarmachung diffuser Bedrohungen zur Entstehung neuer Praktiken internationalen und globalen Gefahrenmanagements beitrug. NADIS und HYDRA lassen sich als frühe Bausteine einer auf geheimdienst-

21 Timothy Naftali: Blind Spot. The Secret History of American Counterterrorism, New York, NY, 2005; Lisa Stampnitzky: Disciplining Terror. How Experts Invented »Terrorism«, Cambridge, MA, 2013; siehe auch Martin Schulze Wessel: Terrorismusstudien. Bemerkungen zur Entwicklung eines Forschungsfelds, in: Geschichte und Gesellschaft 35 (2009), S. 357-367.

22 Matthias Dahlke: Demokratischer Staat und transnationaler Terrorismus. Drei Wege zur Unnachgiebigkeit in Westeuropa 1972-1975, München 2011, S. 6.

23 Eva Oberloskamp: Codename TREVI. Terrorismusbekämpfung und die Anfänge einer europäischen Innenpolitik in den 1970er Jahren, Berlin/Boston, MA, 2016.

24 Stampnitzky: Disciplining Terror, S. 100; Edna F. Reid/Hsinchun Chen: Mapping the Contemporary Terrorism Research Domain, in: International Journal of Human-Computer Studies 65, 1 (2007), S. 42-56.

https://doi.org/10.14765/zzf.dok-2619

lichen Datenaustausch, neuen Analysetechniken und Computermodelle gestützten internationalen Wissensinfrastruktur zur Abwehr asymmetrischer Sicherheitsrisiken fassen, wobei ein Wandel von der Reaktion auf vergangene Gefahren zur Prävention künftiger Risiken stattfand. Ungeachtet der gemeinsamen Bündniszugehörigkeit blieb die transatlantische Kooperation der Sicherheitsbehörden allerdings von asymmetrischen Machtbeziehungen zwischen den USA und der Bundesrepublik geprägt.[25] Diese wurden durch die zunehmende Dominanz amerikanischer Technologiefirmen – vor allem von IBM – noch verstärkt.[26] Dem stand allerdings die Selbstwahrnehmung deutscher Fachleute wie des BfV-Datenbankpioniers Hans-Joachim Postel gegenüber: Dieser reiste mehrfach zum Erfahrungsaustausch mit seinen dortigen Kollegen in die USA und glaubte die technische Überlegenheit der amerikanischen Seite durch deutsche Ingeniosität bei der Anwendung zu kompensieren.[27] Freilich blieb auch bei ihm ein Gefühl dafür, dass dieser Expertenaustausch zumindest politisch nicht auf Augenhöhe stattfand: Als er 1966 von einer Besuchsreise im CIA-Hauptquartier in Langley zurückkehrte und seine Erinnerungsfotos beschriftete, setzte er seine amerikanischen »Kollegen« in Anführungszeichen.[28]

Durch den Aufbau dieser elektronischen Datenverbundsysteme wuchsen die Datenbestände zunächst in beiden Ländern stetig an. Die elektronische Visibilisierung des opaken Feindes durch derartige »disclosure devices« produzierte systemisch immer neue blinde Flecken.[29] Diese legitimierten jedoch erst recht die Notwendigkeit des Datensammelns und motivierten die Mitarbeiter ihre erweiterten Be-

25 Loch Johnson/Anette Freyberg: Ambivalent Bedfellows. German-American Intelligence Relations, 1969-1971, in: International Journal of Intelligence and Counter Intelligence 10, 2 (1997), S. 165-179; Richard Aldrich: Global Intelligence, Co-Operation versus Accountability. New Facets to an Old Problem, in: Intelligence and National Security 24, 1 (2009), S. 26-56.

26 Vgl. konzeptionelle Überlegungen dazu in Dagmar Schäfer/Marcus Popplow: Einleitung. Globalisierung, Kulturvergleich und transnationaler Techniktransfer als Herausforderung für die Technikgeschichte, in: Technikgeschichte 80, 1 (2013), S. 3-12.

27 Hans-Joachim Postel: So war es … Ein Leben im 20. Jahrhundert, Meckenheim 1999, S. 99-103.

28 Ebd., S. 173. Zu Postels Rolle beim Aufbau der Datenbanken des BfV siehe Goschler/Wala: »Keine neue Gestapo«, S. 301-305.

29 Siehe Hans Krause Hansen/Mikkel Flyverbom: The Politics of Transparency and the Calibration of Knowledge in the Digital Age, in: Organization 22 (2014), S. 1-18; Leon Hempel/Susanne Krasman/Ulrich Bröckling: Sichtbarkeitsregime. Eine Einleitung, in: dies. (Hg.): Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Wiesbaden 2011, S. 7-24, hier: S. 8.

https://doi.org/10.14765/zzf.dok-2619

obachtungslogiken in immer neue Datenbankbestände zu übersetzen,[30] nicht zuletzt auch deshalb, da fallende Preise für Speichertechnologie es immer mehr möglich machten. Ungeachtet der mit dem Aufbau und Ausbau dieser elektronischen Datenbanken verbundenen Eigendynamiken darf jedoch die Handlungsautonomie solcher Suchmaschinen nicht mystifiziert werden, denn diese bewegten sich letztlich stets innerhalb menschengemachter Vorgaben[31] und natürlich auch innerhalb der Grenzen des technisch Machbaren, die auch im Nachhinein nicht unterschätzt werden dürfen.

Hinzu kommen zum einen institutionelle Dynamiken. So starteten in den USA verschiedene Sicherheitsbehörden zunächst unkoordinierte Projekte, um Informationen über Dissidenten und regierungskritische Organisationen in Datenbanken zusammenzufassen. Dabei verwischte die Einführung der Computertechnik traditionelle Grenzziehungen zwischen kommunalen, einzelstaatlichen und föderalen Kompetenzen sowie zwischen in- und auslandsnachrichtendienstlichen Tätigkeiten. Parallel zum CIA-Computersystem HYDRA baute das US-Justizministerium ab 1967 die Inter-Division Information Unit (IDIU) auf, deren größtenteils aus FBI-Berichten ermittelten Datenbestände bald 20.000 amerikanische Staatsbürger umfasste, und diese Daten wurden wiederum im Jahr 1970 an die CIA transferiert. Durch derartigen Informationsaustausch hatten sich bis zum Ende der Operation HYDRA im Jahr 1974 Daten von etwa 300.000 Amerikanern angesammelt.[32] Da HYDRA und IDIU Mitte der 1970er Jahre eingestellt wurden, verlagerten sich die Datensammelaktivitäten der US-Sicherheitsbehörden auf die ebenfalls 1967 vom FBI eingeführte allgemeine Kriminalitätsdatenbank National Crime Information Center (NCIC), die bis 1981 über sieben Millionen Einträge umfasste,[33] sowie auf spezialisierte Datenbanken zur Terrorismusabwehr und zur Bekämpfung der organisierten Kriminalität. Mit der Einführung des Terrorist Research and Analytical Center (1980) sowie des Terrorist Information System (1985), das Mitte der 1990er Jahre Da-

30 Zur Sammelwut der HYDRA-Mitarbeiter siehe Rafalko, MH/CHAOS, S. 30 f.
31 Bächle: Digitales Wissen, S. 48.
32 Vgl. Michael Howard: James Jesus Angleton, the CIA, and the Craft of Counterintelligence, Amherst, MA, 2008, S. 247; Rafalko: MH/CHAOS; analog zum FBI: William Keller: The Liberals and J. Edgar Hoover. Rise and Fall of a Domestic Intelligence State, Princeton, NJ, 1989.
33 Office of Technology Assessment: »An Assessment of Alternatives for a National Computerized Criminal History System«, Washington, D. C., 1982, S. 39.

https://doi.org/10.14765/zzf.dok-2619

ten von 200.000 Personen umfasste, waren bald praktisch wieder ähnliche Datenmengen erreicht wie in den frühen 1970er Jahren.[34]

Zum anderen beeinflussten auch politische Zielvorgaben den Umfang der Datensammelpraxis und die Art und Weise der Datennutzung. So stieg etwa die Zahl der in den Kartei- und Computersystemen der Polizeibehörden und des Verfassungsschutzes erfassten Bundesbürger viele Jahre lang kontinuierlich an, ohne dass sich der genaue Umfang ermitteln lässt. In der Medienöffentlichkeit wurden für die 1970er Jahre stetig steigende Zahlen zwischen zwei bis über drei Millionen behauptet.[35] Seit dem Dienstantritt Gerhart Baums als Bundesinnenminister 1978 wurden allerdings deutlich weniger Daten gespeichert, da er unter anderem die Regelanfrage bei Beamtenanwärtern aussetzte.[36] Zudem galt seit Anfang der 1980er Jahre die Vorschrift, wonach Datensätze zu Personen, bei denen seit fünf Jahren (beziehungsweise 15 Jahren im Bereich des politischen Extremismus) keine Datenbewegung mehr stattgefunden hatte, gelöscht werden mussten,[37] was Historiker – anders als Datenschützer – heute sehr bedauern mögen. 2008 beispielsweise waren so in NADIS rund 1,17 Millionen personenbezogene Eintragungen vorhanden, davon allerdings mehr als die Hälfte aufgrund von Sicherheitsüberprüfungen.[38] Ein angemessenes Verständnis der Dynamik dieser nordamerikanischen und westdeutschen Datenverbundsysteme bleibt somit ein aufwendiges Unterfangen: Für die Mikropolitik der Sicherheitsapparate sind neben den bürokratischen Entscheidungsprozessen und Praktiken auch die jeweiligen technischen Systemarchitekturen als regulierende Akteure[39]

34 Harvey Rishikof: The Evolving FBI. Becoming a New National Security Enterprise Asset, in: ders./Roger George (Hg.): The National Security Enterprise. Navigating the Labyrinth, Washington, D. C., 2011, S. 177-202, hier: S. 189.

35 Siehe Der Spiegel vom 26.11.1973, »10044530111 – das Schlimmste von King Kong?«; Heiner Bremer: Ein Mann namens Meier, in: Der Stern vom 04.09.1975; Jochen Bölsche: »Das Stahlnetz stülpt sich über uns«, in: Der Spiegel vom 30.4.1979.

36 Gabriele Metzler: »Innere Sicherheit« und Rechtsstaat bei liberalen Innenministern, Vortrag im Rahmen des Theodor-Heuss-Kolloquiums 2016 »Die neoliberale Herausforderung und der Wandel des Liberalismus im späten 20. Jahrhundert«, S. 8. (http://www.theodor-heuss-haus.de/fileadmin/user_upload/pics/Unser_Programm/Heuss-Forum/THK_2016/Metzler_-_Liberale_Innenminister.pdf).

37 Vgl. Hans Joachim Schwagerl: Verfassungsschutz in der Bundesrepublik Deutschland, Heidelberg 1985, S. 204; Postel: So war es …, S. 142.

38 Verfassungsschutzbericht 2007: Vorabfassung, Bundesministerium des Innern, Bundesamt für Verfassungsschutz, S. 8 (http://www.bmi.bund.de).

39 Vgl. Gugerli/Mangold: Betriebssystem und Computerfahndung, S. 150; grundlegend: Bruno Latour: Science in Action. How to Follow Scientists and Engineers through Society, Cambridge, MA, 1987.

https://doi.org/10.14765/zzf.dok-2619

relevant. Diese interagierten wiederum mit der makropolitischen Ebene der sicherheitspolitischen und datenschutzrechtlichen Vorgaben sowie transatlantischen Beziehungen, wobei die Übersetzung beider Ebenen an der Schnittstelle von Politik und Verwaltung stattfand.

Datenbanken als Produzenten unsichtbarer Gefahren und Objekt gesellschaftlicher Transparenzforderungen

Der Aufbau großer Datenverbundsysteme nordamerikanischer und westdeutscher Nachrichtendienste führte auf beiden Seiten des Atlantiks zu heftigen gesellschaftlichen und politischen Reaktionen. Die damals aufbrechenden Konflikte reichen bis in gegenwärtige Analysen und theoretische Positionen hinein, die eine erhebliche argumentative Spannweite aufweisen. Dabei werden nicht nur die Auswirkungen der Überwachungstätigkeit und der Datensammelpraxis der Geheimdienste, sondern auch die Rolle des staatlichen Geheimnisses in liberalen Demokratien sehr unterschiedlich bewertet. Das eine Ende der Debatte markiert Giorgio Agamben, der in seiner Kritik des »Sicherheitsstaates« den Ausnahmezustand als das finstere Zentrum des liberalen Rechtsstaats identifiziert.[40] Ähnlich beschreibt die Literaturwissenschaftlerin Eva Horn die arkane Welt der Geheimdienste als Teil der »Sphäre eines heimlichen, aber auf Dauer gestellten Ausnahmezustands, die *irreguläre* Seite der Macht selbst«, die letztlich auf »die Selbstwidersprüche des Politischen in der Moderne« überhaupt verwiesen.[41]

Folgt man Agamben und Horn, so verkörpern geheime Nachrichtendienste sozusagen in radikaler Form das schmutzige kleine Geheimnis der liberalen Demokratie. Dagegen verteidigte der Politikwissenschaftler Herfried Münkler angesichts der Wikileaks-Enthüllungen ausdrücklich die Notwendigkeit eines Arkanbereichs staatlichen Geheimwissens im liberalen Rechtsstaat gegenüber Ansprüchen totaler Transparenz: Der moderne Staat sei seit der Frühen Neuzeit nicht nur zum Monopolisten des politischen Geheimnisses geworden. Später habe er mit der Verwandlung des Machtstaates in den Rechtsstaat zugleich »die Sicherstellung eines verantwortlichen, rechtlich geregelten und gerichtlich überprüf-

40 Giorgio Agamben: Die Geburt des Sicherheitsstaates, in: Le Monde Diplomatique, 14.3.2014; ders.: Ausnahmezustand. Homo Sacer II, Frankfurt a. M. 2004. Vgl. auch Cornelia Rauh/Dirk Schumann: Ausnahmezustände und die Transformation des Politischen, in: dies. (Hg.): Ausnahmezustände: Entgrenzungen und Regulierungen in Europa während des Kalten Krieges, Göttingen 2015, S. 9-36.

41 Horn: Der geheime Krieg, S. 29 f.

https://doi.org/10.14765/zzf.dok-2619

baren Umgangs mit Geheimnissen, ihrer Offenlegung wie Bewahrung« verbunden. Münkler verteidigt daher das Recht des Staates auf Geheimnisse gegenüber einem totalen Transparenzanspruch, den er für politisch verantwortungslos hält.[42] In ähnlicher Weise warnt auch der bulgarische Politikwissenschaftler Ivan Krastev vor den Gefahren radikaler Transparenz für die Demokratie, welche für ihr Funktionieren auf Vertrauen angewiesen sei.[43] Dies wirft das Problem der institutionalisierten Kontrolle des staatlichen Geheimnisses und ihrer Veränderungen auf. Gegenwärtige kulturtheoretische und politikwissenschaftliche Deutungen weisen somit in radikal unterschiedliche Richtungen, die sich ähnlich bereits in den Debatten der 1970er und 1980er Jahre wiederfinden lassen.

Innerhalb des transnational geführten gesellschaftspolitischen Diskurses über die mit elektronischen Datensammlungen verbundenen Eingriffe in die Bürgerrechte wurden die Datenverbundsysteme, die ja ihrerseits ein Reflex auf die neue Unübersichtlichkeit der politischen »Gefährder« waren, nun selbst als Produzenten neuer, unsichtbarer Gefahren problematisiert. In den 1970er Jahren formierten sich sowohl in den USA als auch in der Bundesrepublik Proteste gegen den »Datenhunger« der Sicherheitsbehörden, wobei die Transparenz staatlicher Überwachungsmaßnahmen eine zentrale Forderung darstellte. Zum Katalysator politischen Handelns in den USA wurden Recherchen des Journalisten Seymour Hersh, der 1974 unter anderem eine Reihe umstrittener Geheimdienstprogramme einer breiten Öffentlichkeit bekannt machte, und wenige Jahre später skandalisierten auch in der Bundesrepublik Bürgerrechtler und Journalisten die verborgenen Datenspeicher der Sicherheitsbehörden.[44] Organisationsnamen oder Slogans wie »Citizens Commission to Investigate the FBI« oder »Uncloaking the CIA« zeugten in den USA vom Anspruch, die Visibilisierungsdynamik umzukehren und gegen den Staat selbst zu wenden.[45] In der Bundesrepublik wurde die Gründung ähnlicher Organisationen nach amerikanischem Vorbild

42 Herfried Münkler: Vom Nutzen des Geheimnisses, in: Der Spiegel, 6.12.2010.

43 Ivan Krastev: In Mistrust We Trust; ders.: Der Transparenzwahn.

44 Für die BRD Veröffentlichungen von Bürgerrechtlern wie Peter Brückner/Diethelm Damm/Jürgen Seifert: 1984 schon heute. Oder wer hat Angst vorm Verfassungsschutz? Frankfurt a. M. 1976; Dieter Narr (Hg.): Wir Bürger als Sicherheitsrisiko: Berufsverbot und Lauschangriff – Beiträge zur Verfassung unserer Republik, Reinbek bei Hamburg 1977; sowie die groß angelegte Spiegel-Serie »Das Stahlnetz stülpt sich über uns« (Jochen Bölsche, »Das Stahlnetz stülpt sich über uns«, in: Der Spiegel vom 30.4.1979, 14.5.1979, 21.5.1979, 4.6.1979, 11.6.1979).

45 Howard Frazier: Uncloaking the CIA, New York, NY 1975; vgl. auch Rhodri Jeffreys-Jones: The FBI. A History, New Haven, CT, 2007.

https://doi.org/10.14765/zzf.dok-2619

zwar gleichfalls schon in den späten 1970er Jahren gefordert,[46] doch kam es dazu schließlich erst im Kontext der Proteste gegen die Volkszählung[47] in den frühen 1980er Jahren.

Sowohl für die USA als auch für die Bundesrepublik lässt sich somit ein regelrechtes »Sicherheitsparadoxon«[48] beschreiben: Das mit dem Aufbau der Datenverbundsysteme verbundene staatliche Sicherheitsversprechen produzierte neue gesellschaftliche Unsicherheiten und provozierte Forderungen nach Transparenz der Datensammelpraxis der Sicherheitsbehörden. Die Sicherheitsbehörden wünschten die Gesellschaft zu durchleuchten, um Bedrohungen der politischen Ordnung zu erkennen. Dagegen wurde aus der Zivilgesellschaft heraus gefordert, solche Überwachungs- und Datensammelaktivitäten offenzulegen. Daraus entwickelte sich eine Eigendynamik wachsenden gegenseitigen Misstrauens[49] und es entstanden in beide Richtungen Gefahrenwahrnehmungen. Auf diese Weise entwickelten sich auch Radikalisierungsspiralen des gesellschaftlichen Misstrauens gegenüber den Datenverbundsystemen,[50] wobei allerdings sowohl für die Bundesrepublik wie für die USA stets die Frage nach der gesellschaftlichen Reichweite solcher Kritik mitbedacht werden muss. Die nun entstehenden staatskritischen Überwachungs- und Datenschutzdiskurse, welche die »digitalen Freiheitsrisiken«[51] thematisierten, verbanden sich mit parallel aufkommenden Bedrohungsperzeptionen anderer unsichtbarer Gefahren – insbesondere die von Kernkraftwerken ausgehende Radioaktivität und andere Umweltschäden beziehungsweise Gesundheitsrisiken. In der Bundesrepublik steht dafür vor allem die Abhöraffäre um den einstigen Atommanager und nachmaligen Atomkritiker Klaus Traube in den späten 1970er Jahren.[52] In den Vereinigten Staaten wurde der Nuklearunfall von Three Mile Island im Jahr 1979 zum Referenzpunkt einer Anti-Atomkraftbewegung, die neben

46 Freimut Duve: Gründet Verfassungsschutzvereine, in: Narr (Hg.): Wir Bürger als Sicherheitsrisiko, S. 325 f.

47 Frohman: »Only Sheep Let Themselves Be Counted«, S. 348.

48 Franz-Xaver Kaufmann: Sicherheit als soziologisches und sozialpolitisches Problem, Stuttgart 1973; ders.: Sicherheit: Das Leitbild beherrschbarer Komplexität, in: Stephan Lessenich (Hg.): Wohlfahrtsstaatliche Grundbegriffe. Historische und aktuelle Diskurse, Frankfurt a. M./New York 2003, S. 73-104.

49 Byung-Chul Han, Transparenzgesellschaft, Berlin 2012.

50 Siehe Niklas Luhmann: Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität, Konstanz u. Stuttgart 2009, S. 94.

51 Ulrich Beck: Die Metamorphose der Welt, Berlin 2017.

52 Diese bereits in den 1970er Jahren einsetzende Bedrohungswahrnehmung unsichtbarer Gefahren kann dabei als Keim dessen angesehen werden, was Beck 1986 zeitdiagnostisch pointiert als Risikogesellschaft klassifizierte. Siehe Ulrich Beck: Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt a. M. 1986.

https://doi.org/10.14765/zzf.dok-2619

energiepolitischen Zielen auch Kritik an den Sicherheitsstrategien des Kalten Kriegs formulierte.[53] Zugleich kulminierte durch diesen Vorfall in der Nähe von Harrisburg grenzüberschreitend eine neue Kultur des Misstrauens gegenüber Expertenwissen.[54] Dies eröffnet eine Perspektive auf die Dynamiken der gesellschaftlichen Risikowahrnehmung sowie die gesellschaftlichen Protestbewegungen der späten 1970er und frühen 1980er Jahren.

Auch hier gilt es, die transatlantischen Verflechtungen im Blick zu behalten. Bei einer Anhörung im US-Senat zum Thema »Federal Data Banks« trat 1971 unter anderem der deutsche Umweltaktivist Wolfgang Burhenne auf – dieser war Geschäftsführer der die deutsche Umweltpolitik stark beeinflussenden Interparlamentarischen Arbeitsgemeinschaft sowie einer der Mitinitiatoren des WWF (World Wide Fund for Nature). Seine Stellungnahme vor den US-Senatoren verdichtete im totalitarismustheoretischen Sound der Zeit die Anfang der 1970er Jahre aufkommende Sorge vor einer »dossier dictatorship«: »We are increasingly speaking about the naked man – if all files, all data are collected; I really think we are living in a world where we may see others ›without clothes‹. […] I say, and I can especially say, dossiers are already existing. Modern technology gives us only better possibilities, enabling better services.« Zudem schilderte Burhenne vor dem US-Senat auch das internationale Netzwerk, welches sich über die entsprechenden Entwicklungen in England, Kanada, Schweden, Israel und der Bundesrepublik austauschte und sich in einigen dieser Länder lobbyistisch an gesetzlichen Initiativen zu deren Eindämmung beteiligte.[55] Dieses Einzelbeispiel verweist auf die Notwendigkeit, den engen Nexus der Wahrnehmung von Datenbank- und Umweltgefahren als auch die transnationale Koordination gesellschaftlicher Transparenzforderungen genauer zu erforschen, als dies bislang erfolgt ist. Dabei wird sich vermutlich bestätigen, dass der transatlantischen Zusammenarbeit der Sicherheitsbehörden beim

53 Siehe dazu Eckart Conze/Martin Klimke/Jeremy Varon (Hg.): Nuclear Threats, Nuclear Fear and the Cold War of the 1980s, New York 2016; Angela Santese: Ronald Reagan, the Nuclear Weapons Freeze Campaign and the Nuclear Scare of the 1980s, in: The International History Review 39 (2017), S. 496-520.

54 Frank Bösch: Taming Nuclear Power. The Accident Near Harrisburg and the Change in West German and International Nuclear Policy in the 1970s and Early 1980s, in: German History 35,1 (2017), S. 71-95, hier: S. 78; Christoph Wehner: Die Versicherung der Atomgefahr. Risikopolitik und Expertise in der Bundesrepublik Deutschland und den USA 1945-1986, Göttingen 2017, S. 340-343.

55 Federal Data Banks: Computers and the Bill of Rights. Hearings Before the Subcommittee on Constitutional Rights of the Committee of the Judiciary. United States Senate, 92nd Congress, 1st session, Washington, D.C., 1971, S. 332 f.

https://doi.org/10.14765/zzf.dok-2619

Auf- und Ausbau der Datenbanken eine ebenso intensive transnationale Kooperation jener gesellschaftlichen Kräfte entgegenstand, die sich dem Ziel der Gegentransparenzierung verschrieben hatten. Inwieweit sich dabei die auf beiden Seiten involvierten Expertenkreise berührten und überschnitten, wird sich zeigen müssen.

Sichtbarkeitsregimes und Misstrauensmanagement

Wie wurde nun der Konflikt zwischen den Geheimhaltungsansprüchen von Nachrichtendiensten und den Erwartungen an die Transparenz und Überprüfbarkeit staatlichen Handelns in liberalen, westlichen Demokratien[56] politisch ausgetragen? Inwieweit wurden Nachrichtendienste in den USA und der Bundesrepublik selbst nicht nur Subjekte, sondern auch Objekte von Sichtbarkeitsregimes, d. h. also von »sozialen und technischen Arrangements, die Ordnung stiften oder stabilisieren, Gefährdungen abwehren und Abweichungen korrigieren sollen und selbst eine Ordnung des Beobachtens und Beobachtetwerdens, des Zeigens und Verbergens etablieren«[57]? Durch welche rechtlichen Praktiken wurde die »Informatisierung«[58] der Bürger reguliert?[59] Welche Rolle spielte dabei die »Erfindung« der Datei als juristisches Objekt, das sich substanziell durch die Möglichkeit ihrer Auswertung durch »automatisierte Verfahren« von ihrem analogen Vorgänger, der Akte, unterschied?[60] Und wie wirkte dies wiederum auf die Praktiken des Datensammelns und -auswertens der geheimen Nachrichtendienste zurück? Auch hier gibt

56 Christopher Hood: Transparency in Historical Perspective, in: Proceedings of the British Academy 135 (2006), S. 3-23; Manfred Schneider: Transparenztraum. Literatur, Politik, Medien und das Unmögliche, Berlin 2013; Byung-Chul Han: Transparenzgesellschaft, Berlin 2012; Anita Möllering/Claus Leggewie: Debatte Transparenz. Zeitschrift für Medien- und Kulturforschung 4, 1 (2013), S. 59-70.

57 Siehe zu diesem Begriff Hempel/Krasman/Bröckling, Sichtbarkeitsregimes, S. 8.

58 Gemeint ist damit jener »soziale Prozess des bewussten, systematischen Umgangs mit Informationen […], welcher darauf zielt, Informationen vom konkreten Subjekt unabhängig nutzen zu können«, wozu Informationen aus ihrer geistigen, ideellen Form in eine materielle Form überführt werden müssen. Siehe Andreas Boes: Informatisierung, in: Berichterstattung zur sozioökonomischen Entwicklung in Deutschland. Arbeit und Lebensweisen. Erster Bericht, Wiesbaden 2005, S. 211-244.

59 Bruno Latour: Social Theory and the Study of Computerized Work Sites, in: Wanda J. Orlikowski/Geoff Walsham/Matthew Jones (Hg.): Information Technology and Changes in Organizational Work, London 1996, S. 295-306.

60 Siehe das Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. Januar 1977, §2 (3) 3.

https://doi.org/10.14765/zzf.dok-2619

es im Moment mehr Fragen als Antworten. Im Folgenden sollen aber einige erste Überlegungen dazu angestellt werden, in welcher Weise die gesellschaftlichen und politischen Transparenzforderungen gegenüber geheimen Nachrichtendiensten im Verlauf der 1970er und 1980er Jahre in eine Form des Misstrauensmanagements[61] überführt wurden.

Expertenkommissionen und Parlamente in den USA und der Bundesrepublik mussten einerseits dem Sicherheitsimperativ der staatlichen Behörden und deren Strategien der Sichtbarmachung von »Feinden« der westlich-demokratischen Ordnung Rechnung tragen. Andererseits mussten sie aber auch gesellschaftliche Forderungen berücksichtigen, die darauf zielten, die durch die neue Technik hervorgebrachten Bedrohungen sichtbar zu machen beziehungsweise einzuschränken. In den USA wurden ab 1975 im Rahmen parlamentarischer und exekutiver Kommissionen neue sicherheitspolitische Transparenznormen verhandelt.[62] Die folgenden Gesetzesinitiativen stärkten einerseits die Kontrolle über die Geheimdienste. Andererseits wurde nicht nur der bereits 1967 verabschiedete Freedom of Information Act (FOIA) in den folgenden Jahrzehnten mehrfach reformiert, sondern auch durch weitere Gesetze der Anspruch der Bürger auf Kontrolle staatlichen Handelns erweitert.[63] Indem der Freedom of Information Act immer wieder ausgeweitet wurde, entwickelten sich in den Vereinigten Staaten verstetigte Praktiken der Visibilisierung nachrichtendienstlichen Handelns: »To FOIA« (durchaus als Verb benutzt) steht dabei für die Praxis den nationalen Sicherheitsinstitutionen zumindest Teile ihrer Geheimnisse abzuringen. Seit 1985 sammelt das von privaten Stiftungen finanzierte, an der George Washington University eingerichtete National Security Archive auf diesem Wege freigegebene Dokumente US-amerikanischer Nachrichtendienste. Dies sollte man nicht vorschnell als stetig voranschreitende Zähmung der staatlichen Sicherheitsbehörden interpretieren, denn immer wieder gab es auch Gegentendenzen. So versah 1982 die Reagan-Administration den Freedom of Information Act mit zahlreichen Ausnahmen für »national security information«.[64] Die doppelte Zielrichtung des Schutzes vor

61 Für den Politologen Ivan Krastev bedeutet Transparenz nicht die Wiederherstellung von Vertrauen in Institutionen, sondern das Management von Misstrauen: siehe Krastev, In Mistrust We Trust.

62 Tity de Vries: The 1967 Central Intelligence Agency Scandal. Catalyst in a Transforming Relationship between State and People, in: Journal of American History 98, 4 (2012), S. 1075-1092.

63 Jason Ross Arnold: Secrecy in the Sunshine Era. The Promise and Failure of US Open Government Laws, Lawrence, KS, 2014.

64 Executive Order 12356 »National Security Information« vom 2.4.1982 (https://www.archives.gov/federal-register/codification/executive-order/12356.html).

https://doi.org/10.14765/zzf.dok-2619

Visibilisierung – Verteidigung der Geheimnisse der Sicherheitsbehörden und der Bürger – nahm zugleich eine paradoxe Wendung: In den USA entwickelte sich ausgerechnet die Berufung auf den Schutz der Privatsphäre ihrer Beamten neben Gründen nationaler Sicherheit zu einem Hauptargument für abgelehnte FOIA-Anträge und half so gesellschaftliche Transparenzforderungen abzuwehren.

Auch in der Bundesrepublik erweiterte 1978 das »Kontrollgremiumgesetz« die parlamentarische Kontrolle der Geheimdienste. Zuvor hatte lediglich ein von Adenauer in den 1950er Jahren ins Leben gerufenes Parlamentarisches Vertrauensmännergremium existiert, dem der Bundeskanzler selbst vorstand und dessen Mitglieder vollständig vom Vertrauen und den Informationen der Bundesregierung abhängig waren.[65] Das Personenvertrauen des Regierungschefs gegenüber den Abgeordneten wurde nun zumindest ansatzweise durch die parlamentarische Kontrolle der Regierung und des dem Bundesinnenministerium unterstellten Verfassungsschutzes ersetzt. Der Datenschutzaspekt war bereits mit einem 1973 vorgelegten Gesetzentwurf gleichfalls Teil einer gesellschaftlichen Diskussion geworden, an der Öffentlichkeit, Parlamentarier und Experten beteiligt waren. Die Debatte um diese Frage zog sich bis 1977 hin, als schließlich das Bundesdatenschutzgesetz verabschiedet wurde, und endete zumindest vorläufig damit, dass ein Bundesbeauftragter für Datenschutz eingesetzt wurde. Seine Ombudsfunktion ermöglichte es nach dem FOIA-Vorbild Bürgerinnen und Bürgern zu erfragen, welche Daten die Sicherheitsbehörden über sie speicherten, ohne dass dabei nach amerikanischem Muster ein prinzipielles Recht auf Zugang zu staatlichen Informationen anerkannt wurde.[66] Die scheinbare nordamerikanische und westdeutsche Synchronizität dieser Reformprozesse resultierte nicht zuletzt aus einem regen transatlantischen Austausch auf Expertenebene.[67] Neben Akademikernetzwerken spielte hier insbesondere die Organisation for Economic Co-operation and Development (OECD) eine wich-

65 Goschler u. Wala: »Keine neue Gestapo«, S. 268; siehe auch Thomas Walde: ND-Report. Die Rolle der geheimen Nachrichtendienste im Regierungssystem der Bundesrepublik Deutschland, München 1971, S. 248-253; Hansjörg Geiger: Wie viel Kontrolle ist möglich und nötig? Rechtliche Grundlagen und politische Praxis in Deutschland, in: Wolbert K. Smidt u. a. (Hg.): Geheimhaltung und Transparenz. Demokratische Kontrolle der Geheimdienste im internationalen Vergleich, Berlin 2007, S. 33-45, hier: S. 38.

66 https://www.bfdi.bund.de/DE/INFOFREIHEIT/Artikel/OmbudsfunktionBfDI.html?cms_templateQueryString=ombudsfunktion&cms_sortOrder=score+desc.

67 Ulrich Dammann/Otto Mallmann/Spirios Simitis: Die Gesetzgebung zum Datenschutz. Eine internationale Dokumentation, Frankfurt a. M. 1977.

https://doi.org/10.14765/zzf.dok-2619

tige Rolle, etwa indem sie 1980 die *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[68] veröffentlichte.

Als mit dem Mauerfall im Herbst 1989 bald auch der Kalte Krieg endete, war die Auseinandersetzung um die Grenzen der gegenseitigen Transparenzierung von Geheimdiensten und Gesellschaft in den USA und der Bundesrepublik weitgehend abgeebbt. Der Daten-Leviathan hatte zumindest vorübergehend seinen Schrecken verloren. Der prekäre Gesellschaftsvertrag, der auf dem Tausch zwischen der staatlichen Visibilisierung der Bürger und der Nachvollziehbarkeit staatlichen Handelns beruhte, schien also wieder bekräftigt worden zu sein. Vielleicht trug gerade diese gesellschaftliche Zuversicht zu der nahezu euphorischen Willkommenskultur bei, die beim Aufbau des Internets in den 1990er Jahren herrschte und die erst nach der Jahrtausendwende von wachsender Besorgnis vor einer neuen Art der »flüchtigen Überwachung« (Zygmunt Bauman) abgelöst wurde. Während die linksliberalen neuen sozialen Bewegungen allmählich abebbten, nahm auch die kritische und polarisierte Auseinandersetzung mit dem Staat ab, zumal diese in Gestalt ihres parlamentarischen Arms DIE GRÜNEN nun selbst verschiedentlich in Regierungsverantwortung einrückten. Dies gipfelte 1998 in einer rot-grünen Regierungskoalition auf Bundesebene.[69] Genau genommen war allerdings bereits seit Mitte der 1980er Jahre die technische, automatisierte und international kollaborierende nachrichtendienstliche Überwachung weiter ausgebaut worden, wofür das von fünf westlichen Staaten unter Führung der USA weltweit operierende westliche Kommunikationsüberwachungsprogramm ECHELON das eindrucksvollste Beispiel darstellt.[70] Doch lange Zeit nahm die Öffentlichkeit davon kaum Notiz.

Nicht zuletzt die intensive Auseinandersetzung mit den nach dem Zusammenbruch der DDR sichtbar gewordenen umfangreichen Datensammlungen des Ministeriums für Staatssicherheit trug schließlich dazu bei, dass die Transparenzforderungen gegenüber westlichen Datenverbundsystemen zunächst nicht wiederbelebt wurden. Gegenüber den nun enthüllten Praktiken des MfS verblassten ihre westlichen Pendants gewissermaßen. Aus dem nun möglichen umfassenden Einblick

68 http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

69 Vgl. dazu Edgar Wolfrum: Rot-Grün an der Macht, Deutschland 1998-2005, München 2013.

70 Kevin J. Lawner: Post-Sept. 11th International Surveillance Activity – A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe, in: Pace International Law Review, 14,2 (2002), S. 436-480; Patrick Radden Chatter Keefe: Dispatches from the Secret World of Global Eavesdropping, New York, NY, 2005.

https://doi.org/10.14765/zzf.dok-2619

in ein real existierendes gigantisches Überwachungssystem wurde zudem eine scheinbar paradoxe Schlussfolgerung gezogen: Gerade die schiere Menge der gesammelten Daten erschien nun eher als Bedingung der Unfähigkeit der staatlichen Sicherheitsbehörden, die entscheidenden politischen Bedrohungen sehen zu können. Hierfür lieferte der unvorhergesehene Untergang der DDR anscheinend den ultimativen Beweis: Die Stasi schien sprichwörtlich in ihren Daten ertrunken zu sein, die sich zumindest in der allgemeinen Wahrnehmung vor allem in Gestalt kilometerlanger Akten und Karteikästen materialisierten. Dies verband sich oftmals mit dem vor allem im Westen gerne belächelten Bild der technologischen Rückschrittlichkeit der DDR.

Die öffentlichen Stasi-Debatten konzentrierten sich daher weniger auf die bürokratische Effizienz der Überwachung, sondern auf die sozial und psychologisch zerrüttenden Folgen der umfassenden gegenseitigen Bespitzelung der DDR-Bürgerinnen und -Bürger. Im Mittelpunkt stand die soziale Figur des »IM« und nicht die (weitgehend analoge) Technologie der Datenbanken, diskutiert wurden weniger technische, sondern politische und moralische Fragen. Und während darum gestritten wurde, ob die millionenfachen Überwachung der DDR-Bürger archiviert und zugänglich gemacht werden sollte,[71] ließen nordamerikanische geheime Nachrichtendienste den Bundesverfassungsschutz gewissermaßen gnädig an den auf Karteien und Mikrofilmen gespeicherten Listen geheimer Stasi-Informanten im Westen teilhaben.[72] Die Auseinandersetzung um die Stasi-Unterlagen überlagerte somit nicht nur die zwei Jahrzehnte lang in den USA und der Bundesrepublik geführte Auseinandersetzung um die Rolle elektronischer Datenbanken westlicher geheimer Nachrichtendienste, sondern verlieh ihr auch eine andere Richtung: Statt um die Gefahren von Datenbanken in der Demokratie ging es nun um die Rolle des Individuums in der Diktatur. Zur Chiffre der Stasi-Überwachung wurde nicht der Computer, sondern der IM, mit dem sich weniger das Gefahrenpotenzial der Technik, sondern die menschlichen Abgründe des Verrats nahestehender Personen verbanden. Das »Ende der Geschichte« (Francis Fukuyama) beschloss so vorerst eine gut zwanzig Jahre andauernde gesellschaftliche Debatte um Sicherheit, Transparenz und Demo-

71 Silke Schumann: Vernichten oder Offenlegen? Zur Entstehung des Stasi-Unterlagen-Gesetzes. Eine Dokumentation der öffentlichen Debatte 1990/91 (Dokumente – Reihe A). Berlin 1995 (http://www.nbn-resolving.org/urn:nbn:de:0292-97839421303631).

72 Helmut Müller-Enbergs: »Rosenholz« Eine Quellenkritik (BF informiert 28/2007), http://www.nbn-resolving.org/urn:nbn:de:0292-97839421306911.

https://doi.org/10.14765/zzf.dok-2619

kratie, bevor sie einige Jahre später in verwandelter Form wiedereröffnet wurde.

Fazit

Als Reaktion auf die Krise der Erkennbarkeit der politischen Gegner, die gleichermaßen mit den Folgen gesellschaftlicher Liberalisierung wie der zunehmend grenzüberschreitenden Natur der Bedrohungen zu tun hatte, wurden in den frühen 1970er Jahren sowohl in den USA als auch in der Bundesrepublik Datenverbundsysteme eingeführt, die als neuartige Sichtbarmachungsinstrumente dienen sollten. Beim Aufbau elektronischer Datenverbundsysteme wie HYDRA und NADIS tauschten sich deutsche und amerikanische Experten aus und fügten der auf gemeinsamen politischen Zielen beruhenden transatlantischen Sicherheitsgemeinschaft eine technische und epistemologische Dimension hinzu. Die darauf reagierende zivilgesellschaftliche Debatte in beiden Ländern, die gleichfalls stark transatlantisch ausgerichtet war, kritisierte die drohende Visibilisierung von Bürgern und Bürgerinnen und forderte zugleich mehr Transparenz der Nachrichtendienste. Als Ergebnis dieser Auseinandersetzung wurden elektronische Datenverbundsysteme in den USA wie in der Bundesrepublik im jeweiligen nationalen Rahmen reguliert. Einerseits wurden die Nachrichtendienste damit in den USA transparenter als in der Bundesrepublik, namentlich im Bereich der Aktenfreigabe; andererseits besaß dort aber auch der Schutz der Daten der Bürgerinnen und Bürger einen geringeren Stellenwert.

Seit Mitte der 1980er Jahre verlor der Konflikt um die gegenseitige Transparenz von Gesellschaft und Nachrichtendiensten vorübergehend an Bedeutung; ein fragiles Gleichgewicht stellte sich ein. Jenseits der öffentlichen Aufmerksamkeit verstärkten aber Nachrichtendienste insbesondere auf transatlantischer und europäischer Ebene in dieser Zeit den Datenaustausch etwa bei ihrem Kampf gegen ebenfalls zunehmend global auftretende Drogenkriminalität und Terrorismus und schufen damit neue globale Wissensnetzwerke. Hier muss in Zukunft noch genauer untersucht werden, inwieweit damit die aus den gesellschaftlichen und politischen Auseinandersetzungen hervorgegangenen Visibilisierungswerkzeuge, die eine größere Transparenz der Datensammelpraxis der geheimen Nachrichtendienste in den USA und der Bundesrepublik herstellen sollten, schon wieder stumpf geworden waren, da die Orte des Wissens immer weniger greifbar wurden. Dabei wäre auch die These zu überprüfen, wonach die Orte, an denen geheime Wissensbestände

https://doi.org/10.14765/zzf.dok-2619

produziert wurden, sich potenzierten »und gleichsam in den Netzwerken der Sicherheit staatlicher und nicht-staatlicher Akteure verschwunden« seien.[73]

Wie verhalten sich diese teilweise noch vorläufigen Befunde und Beobachtungen zu der geradezu kanonischen Erzählung der Surveillance Studies, wonach sich im Untersuchungszeitraum die panoptische in eine post-panoptische, flüssige Überwachung verwandelt habe, womit zugleich eine Verschiebung von der Disziplinargesellschaft (Michel Foucault) zur Kontrollgesellschaft (Gilles Deleuze) behauptet wird?[74] Diese Kategorien sind zweifellos heuristisch wertvoll, da sich damit Veränderungen der elektronischen Datenverbundsysteme im Hinblick auf das Spannungsverhältnis zwischen den Orten des Wissens und den Praktiken der gegenseitigen Transparenzforderungen beschreiben lassen. Doch sind sie zugleich von politischen Auseinandersetzungen geprägt, bei denen es vor allem darum geht, Veränderungen der Formen von Herrschaft in westlichen Gesellschaften auf den Begriff zu bringen. Damit setzen sie sich vor allem mit der liberalen Demokratie auseinander und ersetzen dabei die alte Dystopie des zentralperspektivischen »Big Brother« gerne durch die neue Schreckensvision selbstüberwachender »neoliberaler« Subjekte. Empirisch wird genauer zu zeigen sein, inwieweit neue Formen der Visibilisierung von Gesellschaft wiederum umgekehrte Forderungen nach größerer Transparenz von Nachrichtendiensten hervorriefen, denen eben jene wandelbaren dystopischen Beschreibungen als Argument dienten. Zudem verharren solche Deutungen entgegen aller Vernetzungssemantik tendenziell in einer auf den (National-)Staat konzentrierten Perspektive. Demgegenüber hat das Problem – die Auseinandersetzung um die Bedeutung der Datensammlung und -verarbeitung und nicht zuletzt auch deren politische Nutzung – längst globale Ausmaße angenommen und ist keineswegs auf westlich-liberale Systeme begrenzt. Für die künftige Erforschung dieser Fragen gilt es somit nicht zuletzt diesen theoretischen blinden Fleck zu überwinden, um nicht ungewollt analytisch im Kontext eines Konflikts zu argumentieren, der selbst vielleicht schon historisch geworden ist.

73 Hempel/Krasman/Bröckling, Sichtbarkeitsregime. Eine Einleitung, S. 14.

74 Siehe als klassischen Referenztext Gilles Deleuze: Postskriptum über die Kontrollgesellschaften, in: ders.: Unterhandlungen 1972-1990, Frankfurt a. M. 1993, S. 254-262. Vgl. dazu Bächle, Digitales Wissen, v. a. S. 158-171; Reichart, Einführung, S. 5 f.; sowie die Beiträge von Greg Elmer, Willian Bogard u. Ayse Ceyhan in: Kirstie Ball, Kevin D. Haggerty u. David Lyon (Hg.): Routledge Handbook of Surveillance Studies, London u. a. 2014, S. 13-37.