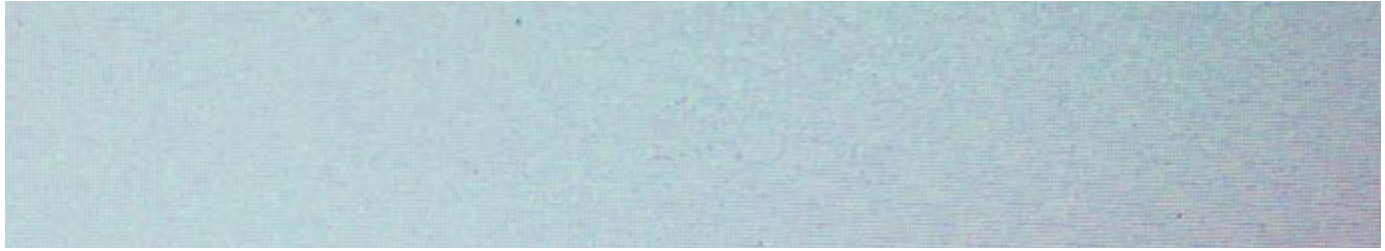
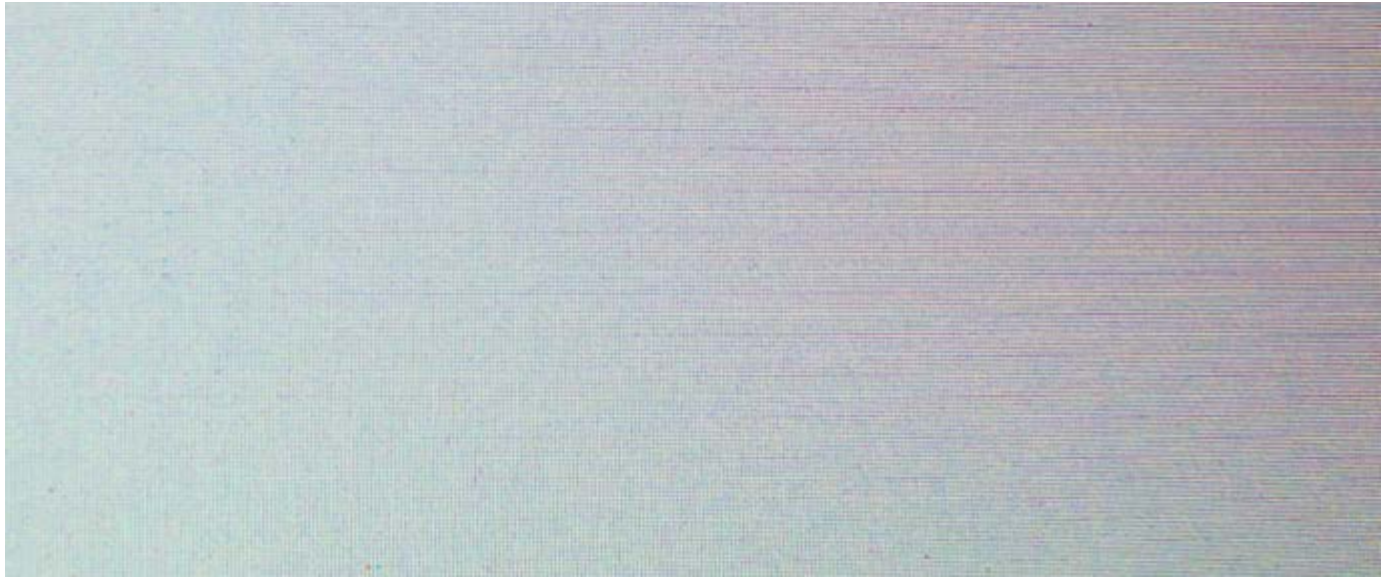


Digitale Schwellen

Privatheit und Freiheit in der digitalen Welt

Mit Beiträgen von: Ulrike Ackermann, Marion Albers, Jan Philipp Albrecht, Leonard Dobusch, Hannes Federrath, Marco Ghiglieri, Yvonne Hofstetter, Stefan Köpsell, Benjamin Lange, Johannes Lichdi, Johannes Näder, Marcel Rosenbach, Peter Schaar, Hervais Simo, Matthias Spielkamp, Holger Stark, Michael Waidner



weiterdenken
HEINRICH BÖLL STIFTUNG SACHSEN
NETZPOLITIK

DIGITALE SCHWELLEN –
PRIVATHEIT UND FREIHEIT IN DER DIGITALEN WELT

Digitale Schwellen – Privatheit und Freiheit in der digitalen Welt

Herausgegeber:
Weiterdenken - Heinrich-Böll-Stiftung Sachsen
Johannes Lichdi

Weiterdenken – Heinrich-Böll-Stiftung Sachsen, Schützengasse 18, 01067 Dresden
fon 0049 351 49 43 311 | fax 0351 49 43 411 | www.weiterdenken.de

Redaktionsschluss: April 2015
Druck: Union-Druckerei Dresden
Satz/Layout, Grafik: Antje Meichsner
Fotoserie «Annäherung an den Bildschirm»: Antje Meichsner

Bestelladresse:
Weiterdenken - Heinrich-Böll-Stiftung Sachsen | www.weiterdenken.de

NETZPOLITIK

Digitale Schwellen

Privatheit und Freiheit in der digitalen Welt

INHALT

MARION ALBERS

Zukunftsszenarien polizeilicher Überwachung

Dieser Beitrag erörtert aus rechtlicher Perspektive die Überwachung durch Sicherheitsbehörden und hier vor allem durch Polizeien. Einige Schlagworte sind in der Öffentlichkeit bekannt: zunehmende Ausweitung der Ermittlungsmethoden wie etwa der Videoüberwachung, Internet-Aufklärung oder Online-Durchsuchungen, eine zunehmende Vernetzung der Sicherheitsbehörden unter anderem durch Gemeinsame Dateien wie die Anti-Terror-Datei und nicht zuletzt der NSA-Skandal.

Im ersten Abschnitt soll ein übergreifender Rahmen geschaffen werden. Denn technische Möglichkeiten aufgrund der Digitalisierung oder des Internets liefern keine ausreichende Erklärung für die Veränderungen sicherheitsbehördlicher Ermittlungs-, Datenverarbeitungs- oder Datenaustauschformen. Die Genese und der Einsatz von Techniken sind ebenso wie die Nutzung des Internets immer auch in soziale Zusammenhänge eingebettet. Daher ist die Erläuterung der übergreifenden Sicherheitsarchitektur notwendig, die den Kontext für polizeiliche oder nachrichtendienstliche Aktivitäten liefert und die sich von den überkommenen Mustern der Gefahrenabwehr einerseits und der Strafverfolgung andererseits längst gelöst hat. Diese neue Sicherheitsarchitektur ist zugleich der Hintergrund für die im zweiten Abschnitt thematisierten Zukunftsszenarien. Der Fokus richtet sich hierbei auf neue polizeiliche Konzepte wie die prädiktive Polizeiarbeit, auf neue technikermöglichte Ermittlungsmethoden sowie die Verknüpfung so erlangter Daten, auf technikgestützte Vernetzungen der Sicherheitsbehörden und auf die globalisierte Überwachung. Mit all dem steht eine freiheits- und menschenrechtsorientierte Regulierung vor erheblichen Herausforderungen.

I. Wandel der Sicherheitsarchitektur

Die überkommene Sicherheitsarchitektur unterliegt seit den 1970er Jahren einem grundlegenden, nachhaltigen und dynamisch fortschreitenden Wandel. Die wesentlichen Stichworte lauten: Prävention wird zur Leitidee. Polizeiliche Kompetenzen werden in das Vorfeld der Gefahrenabwehr und der Strafverfolgung ausgedehnt; qualitativ neue Ermittlungsmethoden erweitern das bisherige Instrumentarium. Im föderalen System werden die Bundespolizeien mehr und mehr ausgebaut. Neben dem Bundes- und dem Zollkriminalamt entwickeln sich die Nachrichtendienste zu «Informationsschaltstellen» im Netzwerk der Sicherheitsbehörden. All dies führt dazu, dass die inhaltlichen und organisatorischen Differenzierungen, die das rechtsstaatliche Markenzeichen der überkommenen Sicherheitsarchitektur waren, jedenfalls nicht mehr in der traditionellen Form existieren und neue freiheitssichernde Muster benötigt werden.

1. Bausteine der traditionell-rechtsstaatlichen Sicherheitskonzeption

Die traditionellen rechtsstaatlichen Sicherheitskonzeptionen, hinter denen das bürgerlich-liberale Gesellschaftsmodell mit seinen Charakteristika und Grenzen steht, bauen darauf auf, dass Aufgaben und Institutionen inhaltlich und organisatorisch differenziert und zugleich eingegrenzt werden. Für die Gefahrenabwehr sind neben den Ordnungsbehörden prinzipiell die Polizeien der Länder zuständig. Die Aufgabe richtet sich auf die Abwehr von Schäden für die Integrität der Rechtsordnung und individueller Rechtsgüter. Polizeiliches Handeln setzt Gefahrensituationen voraus. Diese liegen nur vor, wenn hinreichende Tatsachen und Kausalitätserfahrungen den Schluss erlauben, dass bei ungehindertem Fortlauf Schäden entstehen. Aus Prognosesicherheits- und Effektivitätsgründen werden die Eingriffs- und Abwehrmaßnahmen zeitlich so nah wie möglich an den befürchteten Schadenseintritt herangerückt. Personen sind nach Verantwortlichkeitskriterien in Anspruch zu nehmen, also beispielsweise, weil ihr Verhalten die Gefahr verursacht. Jemand, der nicht verantwortlich ist, darf nach der traditionellen Konzeption nur unter sehr engen Voraussetzungen mit polizeilichen Maßnahmen belastet werden.

Die Strafverfolgung obliegt demgegenüber der Staatsanwaltschaft, der die Polizei als Hilfsorgan untergeordnet ist, sowie – nach Anklageerhebung – den Strafgerichten. Im Fokus stehen nicht künftige Gefahren, sondern Sanktionen für in der Vergangenheit begangene Straftaten. Die Einleitung eines Ermittlungsverfahrens setzt den Anfangsverdacht einer begangenen oder begonnenen Straftat voraus, also eine konkrete Tatsachenbasis, die den Schluss erlaubt, dass eine Straftat stattgefunden hat. Die Ermittlungsmaßnahmen sind auf eine konkrete Straftat bezogen, für die ein Anfangsverdacht bestehen muss. Verdächtige müssen eingriffsintensivere Maßnahmen dulden als bloße Zeugen.

Den Nachrichtendiensten, also den Ämtern für Verfassungsschutz, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst, sind Informationsaufgaben im Hinblick auf den Schutz der freiheitlich-demokratischen Grundordnung, die Sicherheit der Streitkräfte oder die außen- und sicherheitspolitischen Interessen der Bundesrepublik zugewiesen. Diese Behörden greifen nicht selbst in relevante Geschehen ein. Sie sind nach der überkommenen Konzeption auf die Aufgabe der Information der Bundes- oder der Landesregierungen beschränkt, die eher als übergreifend-generalisierte Wissensvermittlung ausgestaltet war. Vor diesem Hintergrund sah man weitreichende Ermittlungs-, Datenerhebungs- und Datenverarbeitungsbefugnisse der Nachrichtendienste als gerechtfertigt an: die Einschreitschwellen waren niedrig, eine Überwachung von Personen im Umfeld der für relevant erachteten Aktivitäten möglich und Instrumente der heimlichen Datenbeschaffung üblich. Deswegen wurden Nachrichtendienste vormals scharf gegen Polizei und Staatsanwaltschaft abgegrenzt.

2. Die Karriere der Prävention

Diese durch inhaltliche und institutionelle Differenzierungen, durch Einschreitschwellen wie Gefahr und Verdacht sowie durch eine begrenzte Inanspruchnahme der Bürger und Bürgerinnen gekennzeichnete Sicherheitsarchitektur hat sich inzwischen deutlich verändert. Dazu hat die Veränderung der Kriminalitätsformen beige-

tragen. Beispiele hierfür sind der Terrorismus der 1970er Jahre oder die organisierte Kriminalität mit ihren übergreifend-langfristigen, Legalität und Illegalität verflechtenden Zielen und Organisationsstrukturen. Überdies erscheinen Gefahren in der «Risikogesellschaft» nicht mehr als naturgegeben, sondern als Folge mangelnder Vorsorge. Prävention, also das «Zuvor-Kommen», wird zur Leitidee. Sie zielt darauf, absehbare oder auch nur denkbare Schäden und Gefahrenlagen bereits an deren Quellen zu verhindern. Sie setzt anders als die Gefahrenabwehr nicht mehr so spät, sondern so früh wie möglich an. Niemand hat diese Leitidee für die Polizei deutlicher formuliert als Horst Herold, der ehemalige Präsident des Bundeskriminalamts, der vor dem Hintergrund der Verwissenschaftlichung der Polizeiarbeit und der beginnenden elektronischen Datenverarbeitung die Vision eines Systems hatte, «das befähigt, Problemen zuvorzukommen, bevor sie zutage treten, erst recht, bevor sie bedrohlich werden».[1]

Prävention hat Vorteile, aber auch Nachteile. Negative Folgen resultieren daraus, dass sich die alten für Gefahrenabwehr und Strafverfolgung begründeten Einschreitschwellen auflösen.[2] Das Präventionsinstrumentarium ist wegen der zahlreichen Gefahrenquellen breit gefächert; Einschreitschwellen werden unter Umständen weit vorverlagert. Es erscheint legitimierbar, dass Bürger und Bürgerinnen auch dann Überwachungen, Inpflichtnahmen, Einflussnahmen oder Risikobeurteilungen hinnehmen müssen, wenn sie selbst dafür keinen Anlass gegeben haben.[3] Prävention birgt eine Dynamik: Sie lässt sich immer noch erweitern, immer weiter vorverlagern und immer weiter verbessern. Zumindest als Prinzip kennt sie keine immanenten sachlichen, personellen, räumlichen oder zeitlichen Grenzen.

3. Die Praxis der Polizei

Die Praxis der Polizei hat die Idee der frühzeitig ansetzenden Kriminalprävention recht schnell aufgegriffen und «operative» Konzepte forciert. Die operative Betrachtung stellt Überlegungen und Ziele in den Mittelpunkt, die über die einzelne Situation, die Abwehr einer konkreten Gefahr oder die Aufklärung eines konkreten Verdachts, hinausgehen. Gerade im Bereich der organisierten Kriminalität, so ist das operative Konzept erläutert worden, komme es nicht darauf an, einige bestimmte Taten beweiskräftig zwecks Strafverfolgung festzustellen oder einige weitere Straftaten präventiv zu verhindern. Wichtig sei vielmehr die umfassende Unterbindung der Aktivitäten einer kriminellen Organisation. Ansatzpunkt ist daher nicht eine Einzelfallaufklärung, sondern die Aufdeckung übergreifender Zusammenhänge und krimineller Strukturen. Man führt – im Sinne einer «network-detection» – Erkenntnisse nicht nur täter-, sondern auch milieu-, umfeld- und kontaktbezogen zusammen und versucht, Querverbindungen zu erkennen. Das erfordert «proaktive» Vorfeldermittlungen und heimliche Ermittlungsmethoden ebenso wie die umfassende Sammlung und mehrdimensionale Auswertung von Informationen und Daten zu organisations- oder milieubezogenen Ermittlungsergebnissen, zu übergreifenden

1 Herold (1972): 134 (Hervorh. im Orig.).

2 Ausführlich zum «Präventionsdilemma» Albers (2012).

3 Näher dazu Grimm (1991): 198 ff. Für das Recht der inneren Sicherheit Huster/ Rudolph (2008): 17 ff.

Strukturanalysen oder zu Lagebildern. Dies ähnelt den Arbeitsweisen der Nachrichtendienste, die ihrerseits aufgrund einer Vielzahl gesammelter Erkenntnisse strukturelle Analysen oder Lagebilder erarbeiten, in denen einzelne Daten oder Ereignisse als Mosaikstein erscheinen, vielfältig verwendet und immer wieder neu bewertet werden. Mit solchen Ansätzen hat sich die polizeiliche Tätigkeit von dem traditionellen Konzept der differenzierten Wahrnehmung der Aufgaben Gefahrenabwehr, Strafverfolgung oder nachrichtendienstliche Information der Regierungen entfernt, in das Vorfeld von Gefahren oder Straftatverdachtslagen ausgegriffen und Methoden eingesetzt, die zuvor allein die nachrichtendienstlichen Tätigkeiten kennzeichneten.

4. Gesetzliche Gestaltung der neuen Sicherheitsarchitektur

Nicht zuletzt vor dem Hintergrund dieser polizeilichen Praxis sind seit den 1980er Jahren alle Polizeigesetze und die Strafprozessordnung fundamental verändert worden.[4] Institutionell hat die Polizei an Bedeutung gewonnen, insbesondere gegenüber der im Strafverfolgungsbereich eigentlich leitenden Staatsanwaltschaft. Neben Gefahrenabwehr und Strafverfolgung sind die Straftatenverhütung und die Verfolgungsvorsorge als neue Aufgaben gesetzlich verankert worden. Die Straftatenverhütung deckt das relativ unbestimmte und weit reichende Vorfeld von Gefahren, die Verfolgungsvorsorge für die Straftatenverfolgung das Vorfeld des Verdachts ab. In diesem Vorfeld sind Ermittlungen unterhalb der Gefahrenschwelle, Maßnahmen ohne Vorliegen eines Straftatverdachts, die Sammlung von Daten über Personen, bei denen man erwartet, dass sie künftig Straftaten begehen werden, Analysen struktureller Zusammenhänge einer «kriminellen Szene» oder die Erarbeitung übergreifender Lagebilder möglich. Dies wird um Vorverlagerungen des materiellen Strafrechts ergänzt: Insbesondere im Bereich organisierter oder terroristischer Kriminalität stehen mittlerweile auch die Vorbereitungs-, Unterstützungs- oder Organisationshandlungen im Vorfeld der eigentlichen Rechtsgutverletzung unter Strafe.

Konsequenterweise sind in allen Polizeigesetzen und in der Strafprozessordnung im Laufe der Zeit die Ermittlungs- und Datenverarbeitungsermächtigungen deutlich erweitert worden. Die neuen Ermittlungsmethoden spiegeln häufig die neuen technischen Möglichkeiten wider. Oft funktioniert dies im Wege einer Massendatenerfassung mit entsprechend hohe Streubreite, d. h. viele unbeteiligte Personen werden miterfasst. Die Maßnahmen reichen von der Raster- und Schleierfahndung über die Videoüberwachung öffentlicher Räume und die akustische oder optische Überwachung von Wohnräumen, die automatische Kennzeichenerfassung oder die Ausschreibung zur polizeilichen Beobachtung bis hin zur Telekommunikations- und Internet-Überwachung. Gerade dieser letzte Bereich ist für Ermittlungen eine sehr ergiebige Quelle und wird zunehmend ausgebaut. Unter bestimmten Voraussetzungen zulässig sind etwa die Erhebung von Telekommunikationsverkehrs- und -nutzungsdaten, die Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten, der verdeckte Eingriff in informationstechnische Systeme (sog. Online-Durchsuchung) oder die Internet-Aufklärung etwa in sozialen Netzwerken. In seiner berühmten Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht an diese zwar hohe, an die Internet-Aufklärung jedoch denkbar niedrige

4 Ausführlich Albers (2001): 97 ff.

Anforderungen gestellt. Die insgesamt nicht überzeugende Begründung lautete unter anderem, dass man im Internet ohnehin kein Vertrauen in die Authentizität seines Kommunikationspartners haben dürfe.[5] Allgemein bekannt ist außerdem die Diskussion um die Vorratsdatenspeicherung: Provider und Diensteanbieter sollen die Verkehrsdaten länger als für ihre Zwecke erforderlich speichern, damit Sicherheitsbehörden unter bestimmten Voraussetzungen darauf zugreifen können. Die Vorratsdatenspeicherung ist auch ein Beispiel für das zunehmende Zusammenspiel von Datensammlungen Privater und staatlichen Zugriffen. Die jeweiligen gesetzlichen Ermittlungsermächtigungen sind also zahlreich. Sie haben allerdings recht differenzierte Voraussetzungen, manchmal auch deshalb, weil das Bundesverfassungsgericht entsprechende Anforderungen aufgestellt hat.

Im Rahmen des Wandels der Sicherheitsarchitektur haben sich darüber hinaus die Datenverarbeitungs- und Datenaustauschmöglichkeiten stark erweitert und verändert. Obwohl sie mindestens genauso wichtig sind wie die Ermittlungsmethoden oder die Datenerhebungsmöglichkeiten, werden sie in den öffentlichen Debatten ebenso wie bei der Regulierung vernachlässigt. Die rechtlichen Grundlagen sind hier oft unangemessen generalisierend, vage und weit gefasst. Demgegenüber kommt es entscheidend darauf an, in welche Zusammenhänge erhobene Daten gestellt werden, wie sie verändert und verknüpft werden, welche Informationen aus ihnen gewonnen werden, wie sie bewertet werden und an welche Stelle sie weiter übermittelt und dann neu verarbeitet werden. Dies wird im Zuge der Digitalisierung der Kommunikation und der Vernetzung der Sicherheitsbehörden noch deutlicher, und künftig müssen die Datenflüsse, -veränderungen und -verknüpfungen sowie die daraus resultierende Informations- und Wissenserzeugung in bestimmten Kontexten angemessene Aufmerksamkeit erhalten.

Die neue Rolle der Polizeien wird durch die Stärkung der Bundespolizeien mitbestimmt. Das Bundeskriminalamt, das zu Beginn seiner Tätigkeit als eine vorwiegend Informationen sammelnde und auswertende Serviceeinrichtung für die Länderpolizeien verstanden wurde, wird mit seinem heutigen Organisations- und Aufgabenprofil als eine multifunktionale «Intelligence-Behörde»[6] bezeichnet. Es fungiert als Zentralstelle, die Daten sammelt und auswertet, zentrale Dateien und Informationssysteme betreibt und auch darüber hinaus «kriminalistische Expertise» bündelt. Zudem ist es Schaltstelle für die internationale Zusammenarbeit. Seine Rolle wird weiter durch die Aufgaben auf dem Gebiet der Strafverfolgung in bestimmten Kriminalitätsbereichen und durch die präventiven Aufgaben bei der Bekämpfung des internationalen Terrorismus geprägt. Aus dem früheren Bundesgrenzschutz ist die Bundespolizei mit einer gewissen Aufgabenvielfalt geworden. Eine erhebliche Bedeutung hat inzwischen auch der Zoll. Vor dem Hintergrund der mit dem grenzüberschreitenden Warenverkehr vermittelten strategischen Position sind den Zollbehörden Aufgaben etwa im Bereich des illegalen Technologie- oder Waffentransfers, des Rauschgifthandels, der Geldwäsche und der Terrorismusfinanzierung zugewiesen worden. Zollfahndungsämtern und dem Zollkriminalamt stehen weitreichende Datenerhebungs- und -verarbeitungsbefugnisse zu. In der Vernetzung der Sicherheitsbehörden spielt der Zoll ebenfalls eine prominente Rolle.

5 BVerfG, Urt. vom 27.02.2008, 1 BvR 370/07: Rn. 311.

6 Abbühl (2010): 353 ff.

Nachrichtendienste treten zu diesem Bild nicht nur deshalb hinzu, weil es zwischen Nachrichtendiensten und Polizeien zunehmende Aufgabenüberschneidungen gibt, unter anderem wegen des Ausbaus der Staatsschutzdelikte. Maßgebliche Veränderungen bewirken die wachsenden Formen institutionalisierter informationeller Zusammenarbeit. Über ihre klassische Rolle der Regierungsinformation hinaus sind auch die Nachrichtendienste mittlerweile zu «Informationsschaltstellen» im Verbund der Sicherheitsbehörden geworden.

5. Die gegenwärtige Sicherheitsarchitektur als Basis von Zukunftsszenarien

Im Sicherheitsrecht haben sich die traditionell-rechtsstaatlichen Differenzierungen von Aufgaben und Institutionen ebenso relativiert wie die durch Gefahr oder Verdacht markierten Grenzen für sicherheitsbehördliche Eingriffe und die Inanspruchnahme von Personen. Gefahrenabwehr und Strafverfolgung sind um die deutlich weiter ausgreifenden Aufgaben der Straftatenverhütung und die Strafverfolgungsvorsorge ergänzt, das materielle Strafrecht ist um Vorbereitungs- und Organisationsdelikte erweitert worden. Unter bestimmten rechtlichen Voraussetzungen sind Vorfeldermittlungen ohne Gefahrenlage, die Verdachtsgewinnung im Vorfeld eines Straftatverdachts, der Einsatz zahlreicher heimlicher Ermittlungsmethoden, die Sammlung von Daten über potenzielle künftige Straftäter, die Inanspruchnahme Unbeteiligter, Analysen struktureller Zusammenhänge zwischen erfassten Personen oder die Erarbeitung übergreifender Lagebilder zulässig und Bestandteil polizeilicher Praxis. Institutionell ist die «Polizei» heute ein Netzwerk von Länder- und zunehmend ausgebauten Bundespolizeien. Mehr und mehr hat man insgesamt mit sicherheitsbehördlichen Netzwerken zu tun, in die Polizeien, andere Behörden mit Ordnungsaufgaben und vor allem auch die Nachrichtendienste eingebettet sind. Diese Sicherheitsarchitektur ist inzwischen weitgehend verfestigt. Sie bietet den Hintergrund für Zukunftsszenarien. Dabei sind die Digitalisierung ebenso wie die Internetvermitteltheit der Kommunikation entscheidende Faktoren.

II. Zukunftsszenarien

Die in diesem Abschnitt im Mittelpunkt stehenden Szenarien sind zum Teil bereits eingeleitet und werden die Zukunft der Sicherheitsbehörden prägen. Die Aufmerksamkeit gilt neuen polizeilichen Konzepten wie der «prädiktiven Polizeiarbeit», neuen technikermöglichten Ermittlungs-, Verknüpfungs- sowie Auswertungsmethoden, technikgestützten Vernetzungen der Sicherheitsbehörden und der globalisierten Überwachung.

1. Neue polizeiliche Konzepte, insbesondere: prädiktive Polizeiarbeit

Prädiktive, also die vorhersagende Polizeiarbeit umreißt als aktuelles Stichwort neue polizeiliche Konzeptionen, die Präventionsstrategien in Gestalt einer weit vorverlagerten Prognose kriminalitätsrelevanter Ereignisse weitertreiben. Das sich in den USA bereits verbreitende «predictive policing»[7] wird derzeit in Deutschland aufgegriffen und diskutiert.[8] Mehr noch als bei der im Kern handlungsorientierten Prävention der vergangenen Jahrzehnte richtet sich dabei der Blick auf Datenverarbeitungs-, Datenanalyse- und Wissensgewinnungsinstrumentarien, die mit den Entwicklungen der Techniken und Netze ermöglicht werden. Prädiktive Polizeiarbeit ist insofern ein Bündelungsbegriff, der verschiedene Ansätze wie Data Mining-Strategien, Crime Mapping, Netzwerkanalysen oder «Big Data»-Visionen aufnehmen kann. Die integrierende Vision lautet erneut: eine Straftat hat noch gar nicht begonnen und die Polizei ist schon da.

Prädiktive Polizeiarbeit ist außerordentlich voraussetzungsvoll. Die – regelmäßig von privaten Unternehmen entwickelten – Datenverarbeitungs-, Datenanalyse- und Wissensgewinnungstechniken und -programme, die sie ermöglichen sollen, stehen selbst noch am Anfang. Die ersten Einsatzfelder betreffen überschaubare Kontexte: Bestimmte Delikte, etwa Eigentumsdelikte in Form von Einbruchsdiebstählen, stehen im Vordergrund. Auswertungen sind auf begrenzte Räume bezogen, etwa auf die verschiedenen Bezirke einer Stadt. In ein leistungsfähiges Datenverarbeitungs- und -analyseprogramm werden zahlreiche Daten aus unterschiedlichen Zusammenhängen und längeren Zeitperioden eingespeist. Dazu gehören etwa die bekannten Einbruchsdiebstähle der vergangenen zwanzig Jahre, genauer Ort, genaue Zeit, Art der Begehung, Ergebnisse der jeweiligen Ermittlungen, Vorkommnisse an Gewalttätigkeiten in dem Bezirk, Drogenhandelsplätze und deren Veränderungen, Gestaltung und Veränderungen des lokalen Umfelds im Laufe der Zeit, Bevölkerungsfluktuation, statistische Einkommensverhältnisse in dem Bezirk, Erkenntnisse aus Ermittlungen in sozialen Netzwerken – eben alles, was an Daten zur Verfügung steht und was irgendwie relevant sein könnte. Automatische Programme und Algorithmen analysieren die Daten in unterschiedlicher Form. Im einfachsten Fall könnten sie eine regelmäßige zeitliche Häufung von Einbruchsdiebstählen in bestimmten Gegenden anzeigen, die die Vorhersage erlaubt, dass im Falle künftiger Einbruchsmeldungen in derselben Gegend weitere Einbrüche passieren werden, so dass hier verstärkte

7 Siehe dazu näher Perry/ McInnis/ Price/ Smith/ Hollywood (2013).

8 Siehe etwa mit differenzierter Beurteilung Gluba (2014). Siehe auch die Antwort der Bundesregierung in BT-Drucksache 17/11582.

polizeiliche Kontrollen stattfinden sollten. Ausgefeiltere Analyseprogramme sollen insbesondere zuvor unbekannte Muster und Trends herauskristallisieren und bei komplexeren Daten- und Datenverarbeitungsgrundlagen würden die Vorhersagen selbst von Algorithmen errechnet und Auswertungsergebnisse geliefert. «Intelligente» Programme wären so konzipiert, dass sie aus neu eingespeisten Daten ebenso wie aus Ergebnissen lernten und ihre eigenen Strukturen und Abläufe anpassten.

Ebenso wie Prävention kann prädiktive Polizeiarbeit mit positiven und mit negativen Folgen verbunden sein. Für sich genommen bietet es zahlreiche Vorteile, wenn kriminelle Aktivitäten tatsächlich treffsicherer prognostiziert und polizeiliche Ressourcen effektiv eingesetzt werden könnten. Aber der Einsatz der «intelligenten» Datenverarbeitungs-, -analyse- und -auswertungsprogramme erzeugt im Schatten zugleich Probleme, Defizite und potenzielle Nachteile. Der dynamisch wachsende, aus sich heraus praktisch nicht mehr begrenzte Datenbedarf – «alles kann ja irgendwann und irgendwie mal wichtig sein»[9] – ist einer der hier zu nennenden Faktoren. Der Kern der Problematik besteht jedoch darin, dass die eingesetzte Software weitaus mehr ist als eine äußerlich bleibende Technologie. Nicht nur hinter ihrer Auswahl, sondern auch hinter ihrer Ausgestaltung und den Programmierungsschritten stecken bestimmte Theorien, Modelle und Hypothesen über Kriminalität. Bei den in den USA für Eigentumsdelikte erprobten Programmen sind dies etwa die «Near Repeat Theory» oder das «Risk Terrain Modeling».[10] Je komplexer die Software wird, desto mehr verbergen sich in ihr Werte und Meinungen, Unsicherheiten und Zweifel, Entscheidungsprozesse, (Vor-)Entscheidungen und Weichenstellungen. Software ist insofern ein «eingefrorener Diskurs». Aber zugleich installiert sie «relativ unveränderliche, als selbstverständlich hingenommene Protokolle in der alltäglichen Informationspraxis von Organisationen, vereinheitlicht die Formen der Interpretation von Ereignissen, beeinflusst die Art und Weise der Entscheidungsfindung und standardisiert solche Entscheidungen über Zeit und Raum hinweg».[11]Eine einprogrammierte Lernfähigkeit kann (Fehl-)Annahmen korrigieren, aber die Problematik auch noch steigern.

Prädiktive Polizeiarbeit greift über die punktuellen einzelfallbezogenen Perspektiven und über die entsprechenden sachlichen, zeitlichen und personellen Einschreitschwellen der klassischen Sicherheitskonzeptionen hinaus. Sie lässt auch bisherige Datenschutzmechanismen als partiell veraltet erscheinen, soweit diese allein personenbezogene Daten und deren Erhebung sowie die Erhebungsmethoden für problematisch halten. Künftig muss sich mehr Aufmerksamkeit auf den Einsatz und auf die Handhabung von Datenverarbeitungsprogrammen und auf die damit verbundenen Folgen richten. Da dies den Kernbereich der Polizeiarbeit

9 Extrabreit (1981), Polizisten.

10 Der Near Repeat Theory liegt u.a. folgende Annahme zu Grunde: Sobald in einer bestimmten Gegend Delikte wie Einbruchsdiebstähle verübt werden, gibt es eine erhöhte statistische Wahrscheinlichkeit, dass kurz nach einem Ausgangsdelikt weitere ähnliche Delikte in dieser Gegend oder in der näheren Umgebung begangen werden. Das Risk Terrain Modeling legt zu Grunde, dass Kriminalität eine Funktion einer dynamischen Interaktion zwischen sozialen, physikalischen und verhaltensbezogenen Faktoren ist, die an bestimmten Orten stattfindet, und dass auf dieser Basis für bestimmte Bereiche bestimmte Risikofaktoren identifiziert und kartografiert werden können. Vgl. insgesamt Ferguson (2012): 277 ff.

11 Leyshon/ Thrift (1999): 453 (Übersetzung von Marion Albers).

betrifft, wird man neue Formen der – gegebenenfalls indirekten – Regulierung sowie neue Formen institutionalisierter und öffentlicher Kontrolle finden müssen.

2. Neue technikermöglichte Ermittlungs- und Datenverarbeitungsformen

Digitalisierung und Netzvermitteltheit der Kommunikation ermöglichen unter quantitativen und qualitativen Aspekten neue Formen der Ermittlung und der Datenverarbeitung. Anschaulich hierfür ist die Videoüberwachung: Aus einem ehemals punktuell und gezielt genutzten Instrument hat sich eine im privaten mehr noch als im öffentlichen Raum weit verbreitete und namentlich in Großbritannien nahezu flächendeckend eingesetzte Überwachungstechnik entwickelt. Die Videoüberwachung durch Bundes- oder Länderpolizeien erfolgt in Deutschland im Rahmen der grenzziehenden gesetzlichen Ermächtigungen. Allerdings können die Polizeibehörden unter wiederum rechtlich begrenzten Voraussetzungen auf Aufzeichnungen privater Personen oder Unternehmen zugreifen. Erst die Kombination polizeilicher Videoüberwachungen und polizeilicher Zugriffsmöglichkeiten auf private Videoüberwachungen ergibt daher ein vollständiges Bild von der Überwachungsreichweite. Darüber hinaus ist die Videoüberwachungshard- und -software deutlich weiterentwickelt worden. Ursprünglich beschränkte sie sich auf die Übertragung der Bilder einer unter Umständen starren Überwachungskamera auf einen Monitor im Beobachtungsraum. Heute ermöglichen Programme und Algorithmen fließende Zoomgrade und das simultane Abprüfen unterschiedlichster Aspekte, Beobachtungen nach Differenzierungskriterien wie Geschlecht oder Hautfarbe, eine Verhaltens- und Gesichtserkennung, die Herausfilterung auffälliger Verhaltensweisen oder eine Bewegungsverfolgung.[12] Rundum drehbare Mikrokameras ergänzen sich in ihrem Beobachtungsradius. Die Aufzeichnungen können verknüpft werden und so lässt sich eine bestimmte Person auf ihrem Weg durch die Stadt verfolgen. «Smarte» Auswertungsprogramme können sich anschließen und deren Ergebnisse wiederum die Überwachung modifizieren. Und nicht zuletzt können bei Vorliegen der technischen Voraussetzungen Aufzeichnungs- und Auswertungsdaten aus Videoüberwachungen ebenso vielfältig mit anderweitigen Daten zusammengeführt wie anderweitige Daten (etwa Fotos aus sozialen Netzwerken) in die Videoüberwachungsprogramme eingespeist werden können. Wie bei den Überlegungen zum prädiktiven Konzept zeigt sich, dass es zu kurz greift, allein einzelnen Ermittlungsmethoden und den punktuellen polizeilichen Datenerhebungseingriffen Aufmerksamkeit zu schenken. Datenverknüpfungen, Datenauswertungsformen, Datenkreisläufe und Datenverarbeitungsprogramme als vorweggenommene Entscheidungs- und Bewertungsverfahren sind gleichermaßen wichtig. Beschreibungen und Beurteilungen werden so schwierig, weil man immer sowohl einen bestimmten Datenverarbeitungsschritt fokussieren als auch die gesamten Verarbeitungsprozesse und -zusammenhänge im Blick haben muss.

12 Ausführlicher Held (2014): 15 ff.; Gouaillier/ Fleurant (2009): 26 ff.

3. Technisierte Vernetzung der Sicherheitsbehörden

Die informationelle Vernetzung der Sicherheitsbehörden ist ein wesentliches Kennzeichen der neuen Sicherheitsarchitektur. Moderne Infrastrukturen und Datenverarbeitungstechniken machen ihre gegenwärtige Gestalt erst möglich. Neben den vielfältigen Formen wechselseitigen Datenaustauschs sind inzwischen zahlreiche Zentraldateien und Verbunddateien institutionalisiert, die bei einer Stelle geführt werden und in die die daran beteiligten Stellen nach vielfältigen, partiell gestuften Vorgaben selbst Daten einpflegen und aus denen sie Daten abrufen.[13] Solche Dateien stärken noch einmal die Rolle der Bundespolizeien, bei denen sie regelmäßig geführt werden; Beispiele sind das polizeiliche Informationssystem INPOL beim Bundeskriminalamt oder das Zollinformationssystem INZOLL beim Zollkriminalamt. Projektbezogene gemeinsame Dateien und gemeinsame Dateien in bestimmten Sachbereichen wie die «Antiterrordatei» oder die Rechtsextremismusdatei treten hinzu. Automatisierte zentrale gemeinsame Dateien verdichten die Datenlage zu bestimmten Personen, Objekten oder Sachverhalten. Sie zeichnen sich aber immer auch durch ein eigenständiges, technisch mitgeprägtes Datenformat und durch eine spezifische, meist durchaus hohe Selektivität der Datenbasis aus, die sich auf die jeweilige Wissenserzeugung der datennutzenden Sicherheitsbehörde auswirkt. Anschaulich ist etwa das Problem, inwieweit bewertende personengebundene Hinweise, wie etwa «geisteskrank» oder «gewalttätig», in gemeinsame Dateien eingespeist werden sollen, obwohl Bewertungsgrundlagen und -kontext nicht unbedingt mitgespeichert werden können, so dass die abrufende Behörde die Bewertung möglicherweise fehlinterpretiert. Umgekehrt werden aber auch Freitextfelder kritisiert, weil sie Raum für unbegrenzte Eingaben zu Personen gewährten. Vor diesem Hintergrund werden gemeinsame Dateien teilweise auf die Funktion knapper Nachweise beschränkt, die einen anderweitigen näheren Datenaustausch zwischen den Sicherheitsbehörden anbahnen können.

Die einzelnen Datenverarbeitungsschritte, nämlich welche Behörde unter welchen Voraussetzungen welche Daten eingeben und abrufen darf, werden in gesetzlichen Grundlagen, Verordnungen und teilweise als Verschlusssache eingestuften Errichtungsanordnungen relativ detailliert geregelt. Das Kernproblem, welche Folgen gemeinsame Dateien und die Art der dort gespeicherten Datensätze für die behördliche Wissenserzeugung in den Kontexten haben, in die die Daten dann fließen, kann allerdings nicht mit isolierend-punktuellen, sondern nur mit übergreifenden, prozess- und kontextbezogenen Perspektiven erfasst werden. Solche Perspektiven sind auch wichtig für die rechtliche Beurteilung. Gemeinsame Dateien dürfen beispielsweise nicht dazu führen, dass Nachrichtendienste, die persönliche Daten nach Maßgabe relativ niedriger Einschreitschwellen und in weitem Umfang heimlich erheben dürfen, die so erlangten Daten unbeschränkt in eine gemeinsame Datei mit der Folge einspeisen, dass Polizeien darauf zugreifen können, obwohl für sie höhere Hürden bei der Datenerhebung gelten.

Die technisierte Vernetzung der Sicherheitsbehörden erfordert also komplexe rechtliche und informationstechnische Architekturen. Dies wird umso anspruchsvoller, je mehr Behörden beteiligt sind und je mehr man mit transnationalen

13 Zum Überblick etwa BT-Drucksache 17/14735: 9 ff.

Verbunddateien zu tun hat. Beispielsweise hat die Trennung zwischen Polizeien und Nachrichtendiensten in wichtigen anderen Mitgliedstaaten der Europäischen Union keine Tradition, so dass insoweit gar kein Anlass gesehen wird, den Datenaustausch differenziert zu gestalten. Die daraus resultierenden Abstimmungsprobleme werden mit der zunehmenden Europäisierung des Sicherheitsbereichs noch wachsen.

4. Globalisierte Überwachung

Edward Snowden hat enthüllt, in welch globalem und flächendeckendem Umfang Nachrichtendienste das Kommunikationsverhalten überwachen.[14] Dabei wird ausgenutzt, dass jede Person unter den heutigen Kommunikationsbedingungen weit reichende Datenspuren hinterlässt. Verschlüsselungstechniken scheinen wenig zu helfen. Das Datenschutzrecht steht auf sämtlichen Regelungsebenen – international, europäisch, national – vor neuen Fragen.

Die Überwachung durch ausländische Nachrichtendienste ist dabei auch, aber keineswegs allein mit internationalem Recht erfassbar. Auf allen Regelungsebenen ergeben sich vielmehr spezifische Anknüpfungspunkte, die allerdings weiter ausarbeitungsbedürftig sind. Diskutiert wird über Rechte aus den menschenrechtlichen Verträgen, unter anderem aus Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte oder Art. 12 der Allgemeinen Erklärung der Menschenrechte. Deren Anwendbarkeit setzt jedoch die Ausübung von Hoheitsgewalt als traditionellem Merkmal territorialer Herrschaft voraus, und das führt bei globalen Überwachungsmaßnahmen der US-amerikanischen National Security Agency NSA zu einigem Begründungsaufwand. Hinsichtlich des TEMPORA-Programms und der Überwachungsmaßnahmen des britischen Geheimdienstes kommt eine Verletzung insbesondere des Art. 8 oder auch des Art. 10 der Europäischen Menschenrechtskonvention (EMRK) in Betracht. Für deren Überprüfung ist der Europäische Gerichtshof für Menschenrechte (EGMR) zuständig und entsprechende Verfahren sind dort anhängig.[15] Hinsichtlich der Überwachungsaktivitäten der NSA bestehen im Rahmen der Europäischen Union (EU) zumindest mittelbare Kontrollmöglichkeiten. Das gilt etwa im Hinblick auf das Erfordernis, dass die Übermittlung personenbezogener Daten in die USA als Drittstaat dort ein angemessenes Datenschutzniveau voraussetzt. Aufgrund der «Safe-Harbor»-Absprache zwischen den USA und der EU hatte die Europäische Kommission zwar im Jahre 2000 festgestellt, dass aus EU-Sicht ausreichende Datenschutzstandards in den USA bestehen würden.[16] In Kenntnis der NSA-Überwachung und des sonstigen Umgangs mit persönlichen Daten lässt sich diese Sicht jedoch nicht halten. Zu diesem Problemkomplex steht eine Entscheidung des Europäischen Gerichtshofs (EuGH) an.[17]

14 Näher etwa Rosenbach/ Stark (2014).

15 Big Brother Watch and others against the United Kingdom, Aktenzeichen 58170/13; Bureau of Investigative Journalism and Alice Ross against the United Kingdom, Aktenzeichen 62322/14.

16 Entscheidung der Kommission vom 26. Juli 2000, ABl. L 215: 7.

17 Rechtssache C-362/14 (Schrems/Data Protection Commissioner). Es handelt sich um ein Vorabentscheidungsersuchen des High Court of Ireland, der danach fragt, ob die unabhängige Datenschutzbehörde zwingend an die Safe-Harbor-Einschätzung der Kommission gebunden ist oder im Lichte tatsächlicher Entwicklungen eigene Ermittlungen anstellen darf.

Dies zeigt zum Abschluss, dass die technik- und netzvermittelte Globalisierung der Kommunikation dazu führt, dass auch die sicherheitsbehördlichen Aktivitäten nicht mehr allein mit Blick auf die nationale Ebene und auf nationale Polizeien und Nachrichtendienste zu beobachten sind. Überwachungsmechanismen sind in bestimmtem Umfang ihrerseits globalisiert. Auch damit stellen sie uns vor neue Herausforderungen.

Literatur

Abbühl, Anicee (2010), *Der Aufgabenwandel des Bundeskriminalamts,* 2010, Stuttgart u. a.

Albers, Marion (2001), *Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge,* Berlin.

Albers, Marion (2012), *Das Präventionsdilemma,* in: Weichert/Schmidt (Hrsg.), Datenschutz, Berlin, 102 ff.

Extrabreit (1981), *Polizisten,* in: *Welch Ein Land ! - Was Für Männer:* (Song 4), Album (Vinyl), erschienen auf dem Label Reflektor Z (0060.431), Hamburg.

Ferguson, Andrew Guthrie (2012), *Predictive Policing and Reasonable Suspicion,* in: Emory Law Journal Vol. 62, 259 ff.

Gluba, Alexander (2014), *Predictive Policing – eine Bestandsaufnahme,* Hannover.

Gouaillier, Valérie/Fleurant, Aude-Emmanuelle (2009), *La vidéosurveillance intelligente: promesses et défis* (auch auf englisch verfügbar: *Intelligent Video Surveillance: Promises and Challenges),* Québec.

Grimm, Dieter (1991), *Verfassungsrechtliche Anmerkungen zum Thema Prävention,* in: ders., *Die Zukunft der Verfassung,* Frankfurt a. M., 197 ff.

Held, Cornelius (2014), *Intelligente Videoüberwachung,* Berlin.

Herold, Horst (1972), *Gesellschaftlicher Wandel – Chance der Polizei?,* Die Polizei Bd. 63, 133 ff.

Huster, Stefan/ Rudolph, Karsten (2008), *Vom Rechtsstaat zum Präventionsstaat,* in: dies. (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, Frankfurt a.M., 9 ff.

Leyshon, Andrew/ Thrift, Nigel (1999), *Lists come alive: electronic systems of knowledge and the rise of credit-scoring in retail banking,* Economic and Society Vol. 28, 434 ff.

Perry, Walter L./ McInnis, Brian/Price, Carter C./Smith, Susan C./Hollywood, John S. (2013), *Predictive Policing,* Santa Monica, CA u. a.

Rosenbach, Marcel/ Stark, Holger (2014), *Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung,* München.