Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)732 E

MAX-PLANCK-INSTITUT
ZUR ERFORSCHUNG VON
KRIMINALITÄT, SICHERHEIT UND RECHT

MPI-CSL · Günterstalstr. 73 · 79100 Freiburg i.Br. · Deutschland

Prof. Dr. Ralf Poscher
Geschäftsführender Direktor
Direktor Abteilung Öffentliches Recht

Tel.: +49 761 7081-500
public-law@csl.mpg.de

Freiburg, 18. Februar 2021

Konzept für ein periodisches Überwachungsbarometer

Prof. Dr. Ralf Poscher
unter Mitarbeit von Dr. Michael Kilchling, Dr. Katrin Kappler und Lukas Landerer

Der Antrag der BT-Drs. 19/23695 „Freiheit und Sicherheit schützen – Für eine Überwachungsgesamtrechnung statt weiterer Einschränkungen der Bürgerrechte“ greift einen Gedanken auf, der in der Literatur zur Evaluierung der staatlichen Überwachungsinstrumente in Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts entwickelt wurde. Seit Herbst 2020 wird in meiner Abteilung am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht ein Konzept erarbeitet, mit dem sich die Überwachungsgesamtrechnung operationalisieren lässt. Das Projekt wird von der Friedrich-Naumann-Stiftung gefördert. Es befindet sich noch in einem sehr frühen Stadium, doch soll seine Grundidee im Folgenden kurz erläutert werden, da es einen Weg aufzeigt, wie sich eine größere Transparenz in Bezug auf staatliche Überwachungsmaßnahmen herstellen ließe.

Der Kern des Konzepts besteht darin, Zugriffe von Sicherheitsbehörden auf Massendatenbestände in öffentlicher oder privater Hand, in denen jedermann anlasslos erfasst ist, quantitativ zu analysieren und in Statistiken synchron und diachron aufzubereiten. Die Statistiken zu einzelnen Datenbeständen, Behörden und Instrumenten können dann in verschiedenen regionalen, zeitlichen, behördlichen und weiteren Schnitten aggregiert und verglichen werden. In der höchsten Aggregationsstufe, die alle Zugriffe abbildet, lässt sich ein Überwachungsbarometer erstellen, das einen Eindruck von dem Gesamtüberwachungsstatus durch die Sicherheitsbehörden vermittelt. Dieser hochgradig aggregierte Wert stellt zwar zunächst eine Vereinfachung dar, lässt sich aber durch die ihm zugrunde liegenden Daten zu den einzelnen Massendatenbeständen und Zugriffsarten in großer Komplexität und Detailschärfe ausfalten. Ein solches tief gestaffeltes Überwachungsbarometer würde zum einen einen Eindruck von der Überwachungsgesamtentwicklung verschaffen, zum anderen kann es auch quantitative Hinweise auf Fehlentwicklungen bei der Überwachung durch Sicherheitsbehörden

liefern, die dann qualitativ weiter untersucht werden könnten. Diese Hinweise können in ganz unterschiedliche Richtungen gehen: Einerseits kann das Überwachungsbarometer auf wachsende Bedrohungen grundrechtlicher Freiheit hinweisen. Dabei können die quantitativen Daten zu einzelnen Überwachungsinstrumenten durchaus auch Einfluss auf deren verfassungsrechtliche Bewertung haben, da ihre Eingriffsintensität durch das Bundesverfassungsgericht auch aufgrund ihrer Breitenwirkung bestimmt wird. Aus dem hochaggregierten Wert zum Gesamtüberwachungsstatus werden sich hingegen allenfalls in extremen Konstellationen verfassungsrechtliche Konsequenzen ableiten lassen. Andererseits kann das Überwachungsbarometer dazu beitragen, Fehlentwicklungen der öffentlichen Diskussion zu verhindern, indem es diese versachlicht – nicht selten bestehen in der öffentlichen Wahrnehmung unrealistische Annahmen über die Überwachungsaktivitäten der Sicherheitsbehörden. Schließlich können die quantitativen Daten und ihre Entwicklung auch Hinweise auf Defizite bei den Überwachungsinstrumenten geben, etwa dann, wenn aufgrund der technologischen Entwicklung Zugriffe an Bedeutung verlieren, die für die Sicherheitsgewährleistung als essentiell erachtet werden. Das Überwachungsbarometer bewertet die von ihm registrierten Entwicklungen nicht, sondern will einen Beitrag dazu leisten, dass sie empirisch gesättigter, transparenter und öffentlicher diskutiert werden können. Entsprechend ist es darauf angelegt, der allgemeinen Öffentlichkeit zur Verfügung gestellt zu werden. Dies schließt aber nicht aus, dass einzelne Statistiken, aus denen sich das Barometer speist, nicht in jedem Auflösungsgrad öffentlich zugänglich gemacht werden, falls dadurch die operativen Belange der Sicherheitsbehörden beeinträchtigt werden könnten – was allerdings nur selten der Fall sein dürfte, da das Überwachungsbarometer lediglich aggregierte Daten verwendet.

1. Zielsetzung

Bei der sog. Überwachungsgesamtrechnung handelt es sich um einen bislang vorwiegend theoretisch diskutierten verfassungsrechtlichen Topos, der der Erfassung bzw. Abschätzung der – kumulierten – 'Überwachungslast' in Deutschland gilt. Ursprünglich knüpft er an das Urteil des Bundesverfassungsgerichts aus dem Jahr 2010 zur Vorratsdatenspeicherung[1] an. Dort erklärte das Gericht eine Vorratsdatenspeicherung im Bereich der Telekommunikation für Zwecke sowohl der Gefahrenabwehr als auch der Strafverfolgung[2] grundsätzlich für zulässig, bewertete jedoch die konkrete Ausgestaltung der (damaligen) Regelungen im Telekommunikationsgesetz als verfassungswidrig. Das Bundesverfassungsgericht führte über diesen konkreten Einzelfall hinaus aus, dass der Gesetzgeber bei der Erwägung neuer Speicherungspflichten und -berechtigungen vor dem Hintergrund der Gesamtheit der verschiedenen bereits existierenden Datensammlungen zukünftig zu größerer Zurückhaltung gezwungen sei. Daraus hat sich, u.a. angestoßen durch Beiträge von Alexander Roßnagel, eine rechtspolitische Diskussion über die von diesem so benannte „Überwachungs-Gesamtrechnung“[3] entwickelt.[4] Mit dem etwas sperrigen Begriff wird auf die Notwendigkeit einer auch empirisch unterlegten Gesamtbetrachtung des (jeweils aktuellen) Standes staatlicher Überwachung verwiesen, die alle verfügbaren staatlichen Überwachungsmaßnahmen

[1] BVerfG, 1 BvR 256/08 u.a. v. 2.3.2010, z.B. NJW 2010, 833, 839 [Rn. 218].
[2] Die Überwachungsaktivitäten der Dienste werden in dem Beschluss nicht angesprochen.
[3] *Roßnagel*, Die „Überwachungs-Gesamtrechnung” – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238.
[4] Kritisch z.B. *Pohle*, Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung. Ein Alternativvorschlag. FIfF-Kommunikation 4/19, 37.

quasi aufaddiert.[5] Bislang gibt es allerdings noch keine Vorschläge, wie eine Überwachungsgesamtrechnung operationalisiert werden könnte.

In dem explorativen Forschungsprojekt soll der Versuch unternommen werden, den verfassungsrechtlichen Topos zu operationalisieren und Wege aufzuzeigen, wie die reale Überwachungslast,[6] der die Bürgerinnen und Bürger ausgesetzt sind, sinnvoll erfasst und quantifiziert werden kann.

Dabei teilen wir grundsätzlich die in der bisherigen Diskussion verbreitete Skepsis[7] hinsichtlich der Frage, ob eine abstrakte absolute Grenze für verfassungsrechtlich „noch" oder „gerade noch" zulässige bzw. nicht mehr zulässige Überwachungsmaßnahmen im Sinne einer fixen Taxonomie überhaupt von der Rechtswissenschaft alleine definiert werden kann. Das Projekt setzt daher auf eine relationierende Perspektive, die den synchronen und diachronen Vergleich unterschiedlicher Überwachungsniveaus ermöglichen soll. Die Möglichkeit, dass sich aus dem Vergleich Rechtfertigungslasten politischer, aber auch rechtlicher Natur ergeben, wird offengehalten. Dies gilt zum einen für die verfassungsrechtliche Perspektive – bezogen auf die abstrakte Zulässigkeit neuer, zusätzlicher Überwachungsinstrumente – zum anderen in empirisch-rechtstatsächlicher Hinsicht – etwa bezogen auf eine potenziell hohe oder zu hohe Anwendungshäufigkeit bestimmter Maßnahmen insgesamt oder auf die Unverhältnismäßigkeit einer Vielzahl einzelner Maßnahmen in einem konkreten Einzelfall[8].

Um die Dynamik der Entwicklung sowohl bei der Anwendung bestehender wie auch bei der Schaffung neuer bzw. erweiterter Überwachungstatbestände[9] erkennen und interpretieren zu können, soll die Überwachungslast nicht nur einmalig erfasst, sondern in Richtung eines regelmäßigen Monitorings im Sinne eines periodischen Überwachungsbarometers entwickelt werden. Mit einem solchen Instrument könnte dann der jeweils aktuelle Status Quo aufgezeigt und im Kontext kurz- und längerfristiger Entwicklungslinien interpretiert und die rechts- und gesellschaftspolitische Diskussion mit einer belastbaren empirischen Datengrundlage unterstützt werden. Dies wird wesentlich zur Versachlichung der politischen Debatte beitragen.

2. Probleme bisheriger Ansätze

Die Probleme bislang in der Literatur diskutierter Ansätze können stichpunktartig benannt werden:

- keine operationalisierbaren quantitativen Ansätze,
- keine klare Abgrenzung der ins Auge gefassten Datenbestände,
- Vernachlässigung privater Datensammlungen,
- übermäßige Orientierung an einem durch die Wirklichkeit zunehmend überholten Konzept der Datenvermeidung,

[5] Additiver Grundrechtseingriff.
[6] *Adensamer*, [österr.] Handbuch Überwachung (2020), spricht etwa plakativ von „Überwachungsdruck".
[7] Vgl. *Pohle,* FIfF-Kommunikation 4/19, S.4; *Bieker/Bremer/Hagendorff,* Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in *Roßnagel/Friedewald/Hansen* (Hrsg.) DuD-Fachbeiträge 2018, S. 144 ff.
[8] Bei der wissenschaftlichen Evaluation ausgewählter Überwachungsmaßnahmen nach dem BKAG (a.F.) wurden bspw. mehrere Vorgänge identifiziert, in denen jeweils mehr als 50, einmal mehr als 100 und in einem Fall sogar 426 einzelne verdeckte Ermittlungsmaßnahmen zur Anwendung kamen; vgl. *Albrecht & Poscher*, BT-Drucks. 18/13031 (23.6.2017), S. 21 (Tabelle 4).
[9] Auch die technologische Entwicklung ist dabei zu berücksichtigen; vgl. auch *Adensamer*, Aspekte einer Überwachungs-Gesamtrechnung, FIfF-Kommunikation 4/19, 25.

- Befangenheit in grundrechtlicher Konzeption, die teils dazu tendiert, den Datenschutz zum Selbstzweck werden zu lassen und damit der Akzeptanz des Datenschutzes schadet.

3. Lösungsansätze

Die in dem Konzept angelegten Lösungsansätze greifen diese Probleme auf:

- Abstellen auf quantitativ erfassbare Datennutzung durch Sicherheitsbehörden,
- primäre Orientierung an anlasslos erfassten Massendaten,
- Einbeziehung privater Datenbestände,
- Orientierung an einer Konzeption des Rechts auf informationelle Selbstbestimmung als Querschnittsgrundrechtsschutz gegen die abstrakten Gefahren staatlicher Datenverarbeitung, die für die einzelnen Datenverarbeitungssysteme auch *quantitativ* zu spezifizieren sind.[10]

4. Phasen des Konzepts

4.1. Phase 1

Die erste Phase gilt der Sichtung und Eingrenzung der für das Konzept zunächst zu berücksichtigenden Datenbestände.

Es existiert eine Vielzahl **staatlicher** – d.h. staatlich generierter und administrierter – **und privater Datensammlungen**. Eine umfassende Bestandsaufnahme der Überwachungs-„Landschaft" existiert bislang nicht. Daher werden in einem ersten Arbeitsschritt die besonders praxisrelevanten Überwachungsszenarien gesammelt und systematisiert, wobei im Rahmen der Konzeptstudie zunächst nur eine begrenzte Auswahl berücksichtigt werden kann. Die zu erarbeitende Auflistung soll als Orientierung für die in das spätere Überwachungsbarometer einzubeziehenden Sachverhalte dienen.

Die erste Auswahl wird sich schwerpunktmäßig auf **anlasslos gespeicherte Massendaten** konzentrieren. Dies ist nicht zuletzt auch im Kontext der Forderung nach einer Berücksichtigung des Gesamtüberwachungsstatus in der Rechtsprechung gerechtfertigt. Die Forderung wurde aus Anlass der Vorratsdatenspeicherung erhoben, die gerade auf die anlasslose Speicherung von jedermanns Kommunikationsdaten zielte. Vorläufig grundsätzlich nicht einbezogen werden die verschiedenen *anlassbezogenen* sicherheitsbehördlichen Datenbanken. Diese können zwar je nach ihrer konkreten Organisation und Ausgestaltung Merkmale einer (behördlichen) Vorratsdatenspeicherung aufweisen;[11] sie haben jedoch nicht den Charakter einer jedermann erfassenden Massendatensammlung, die ursprünglich Anlass zur Entwicklung des Topos der Überwachungs-gesamtrechnung gab. Da sie dennoch zum Gesamtüberwachungsstatus beitragen, sollten in einer Ausbauphase des Projekts jedenfalls solche anlassbezogenen Datenbanken Berücksichtigung finden, die von besonderer grundrechtlicher Relevanz sind. Um einen Eindruck davon zu gewinnen, welche besonderen Fragen sich hinsichtlich entsprechender Dateien stellen, wird die **Antiterror-Datei** exemplarisch bereits in die Entwicklung des Konzepts einbezogen.

[10] Dazu *Poscher*, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in *Gander et al*. (Hrsg.), Resilienz in der offenen Gesellschaft (2012), S. 167–190; *ders*., The Right to Data Protection, in Miller (ed.), Privacy and power, CUP 2017, 129–142.

[11] *Stubenrauch*, Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten (2009), 122f., ordnet die ATD als "informationelle Vorsorge" ein.

Bereits die Vorratsdatenspeicherung hat keine Daten zum Gegenstand, die von staatlichen Behörden gesammelt werden. Vielmehr bezieht sie sich auf Daten, die bei Telekommunikationsanbietern gesammelt werden sollen. Bereits eine erste Durchsicht zeigte, dass dies kein Zufall ist. Die Daten bzw. **Datenbestände privater Akteure** – die im privaten Umfeld angelegten ebenso wie die bei privatwirtschaftlichen Dienstleistern (vom Internet-Provider bis zur privaten Hausbank) hinterlegten und von diesen generierten – übersteigen die durch unmittelbare staatliche Eingriffe erhobenen Datenbestände quantitativ inzwischen deutlich.

Gerade auch wegen der zunehmenden Bedeutung der Datenbestände in privaten und privatwirtschaftlichen Händen knüpft das Konzept nicht an die Datenbestände als solche, sondern an die **staatlichen Zugriffsrechte** auf derartige Datenbestände (einschließlich entsprechender pro-aktiver Auskunfts- und Meldepflichten) an. Die zu entwickelnden Instrumente sollen also erfassen, wie häufig staatliche Stellen auf die Massendatenbestände zugreifen, in denen die Daten jedermanns verwaltet werden. Nicht berücksichtigt werden nichtstaatlich veranlasste und administrierte Überwachungssachverhalte – wie z.B. die umfangreichen Datensammlungen der Wirtschaftsauskunftei SCHUFA oder die Bewegungsprofile, die im Rahmen der permanenten Aufenthaltsüberwachung von Sportlerinnen und Sportlern zur Ermöglichung unangemeldeter Dopingkontrollen durch Sportverbände und NADA anfallen.[12]

Die Stoßrichtung der Überlegungen des Bundesverfassungsgerichts sowie der Überwachungsgesamtrechnung zielt nicht auf jede staatliche Datenverarbeitung, sondern die Überwachung der Bürger. Das Konzept fokussiert daher auf die Datenabfragen durch **Sicherheitsbehörden**, zu denen neben den Staatsanwaltschaften auch die Polizeien der Länder und des Bundes gerechnet werden, sowie die Nachrichtendienste. Die Datenverarbeitung von Fachverwaltungen wie der Steuerverwaltung, der gesetzlichen Krankenkassen oder der gesetzlichen Rentenversicherung sind nicht Gegenstand des Konzepts.

Die untersuchungsrelevanten Überwachungssachverhalte umfassen etwa folgende Datenbestände:

- Telekommunikationsdaten: Bestands-, Verkehrs-, offene und verschlüsselte Inhaltsdaten,
- Finanztransaktions-, Konto- und weitere Bankdaten,
- Mobilitätsdaten,
- Daten aus dem privaten Lebensbereich (Wohnraumüberwachung, Zugriff auf smarte Haushaltsgeräte); im Falle ihrer Einführung würde künftig wohl auch die Überwachung des privaten Kommunikationsverhaltens in sozialen Netzwerken nach dem NetzDG in diesen sachlichen Kontext fallen,
- Gesundheitsdaten,
- sonstige private Daten, die in Mobilgeräten lokal oder in Firmenservern oder Cloudspeichern abgelegt sind, oder technische Daten, die bei IT-Dienstleistungen aller Art automatisch anfallen[13] – soweit diese nicht unter den besonderen Schutz der Art. 10 oder 13 GG fallen, können sie grds. auf der Grundlage allgemeiner Zugriffsnormen oder Generalklauseln beschlagnahmt werden,
- Meldedaten im Kontext der automatisierten Passbildabfrage sowie

[12] Vgl. Art. 3 der NADA Standards für Meldepflichten.

[13] Ein Beispiel aus der Vergangenheit ist die massenhafte Auswertung der Abrechnungsdaten von ca. 22 Mio. Kreditkarten im Rahmen der "Operation Mikado" (strafrechtliche Ermittlungen gegen einen internationalen Kinderpornografie-Ring im Jahr 2006), die von den zuständigen Gerichten als unbedenkliche kriminalistische Ermittlungsmethode und nicht als Rasterfahndung eingestuft wurde; vgl. BVerfG, 2 BvR 1372/07 (Nichtannahmebeschluss d. 2. Kammer des Zweiten Senats) v. 17.2.2009.

- die Rasterfahndung, die Daten erfasst, die zunächst auf anderer gesetzlicher Grundlage erhoben und gespeichert wurden, und durch die analytische Zusammenführung eine Informationsverdichtung und damit einhergehend ggf. eine qualitative Intensivierung der Überwachungswirkung erfahren.

Dem Projekt geht es zunächst darum, den Überwachungsgesamtstatus anhand der Nutzung von Massendatenbeständen öffentlicher oder privater Akteure durch Sicherheitsbehörden transparenter zu machen. Die Beschränkungen die damit einhergehen, sind jedoch nicht dem Konzept geschuldet, sondern dem explorativen Charakter des Forschungsprojekts. Anhand quantitativ und qualitativ bedeutender Massendatensammlungen, die jedermann betreffen, sollen besonders auch die Voraussetzungen und Bedingungen geklärt werden, die es für eine aussagekräftige Ausarbeitung der Instrumente bedarf. Sollte es sich als grundsätzlich machbar und aussagekräftig erweisen, ist das Modell grundsätzlich auf alle relevanten Datensammlungen erweiterbar. So bleiben etwa Videoüberwachungen im öffentlichen Raum unberücksichtigt, da es an einer zentralen Datensammlung fehlt, bei der sich die Zugriffe grundsätzlich leichter feststellen lassen. Aber selbst dort, wo die Videoüberwachung durch Private erfolgt, wäre es möglich, polizeiliche Zugriffe auf private Überwachungsaufnahmen zu erfassen und in das Modell aufzunehmen.

4.2. Phase 2

Die zweite Phase gilt zum einen der rechtlichen Analyse und normativen Bewertung der Zugriffstatbestände. Die normative Bewertung der Zugriffsrechte ist erforderlich, um eine gewichtete Aggregation der verschiedenen Zugriffszahlen zu ermöglichen. Zum anderen gilt sie der Analyse der bestehenden einfach- und verfassungsrechtlichen Dokumentationspflichten der Behörden für ihre Datenzugriffe. Die Dokumentation der Zugriffe ist Grundvoraussetzung für das Projekt. Ohne eine Dokumentation, die die Ableitung statistischer Daten erlaubt, sind quantitative Analysen, auf denen das Konzept beruht, nicht möglich.

4.2.1. Rechtliche Analyse der Eingriffstatbestände und Dokumentationspflichten

Zunächst soll analysiert werden, unter welchen konkreten **Voraussetzungen** die staatlichen Zugriffe auf die aufgelisteten Daten möglich sind. Im Ergebnis wird eine umfassende vergleichende Übersicht vorliegen, die auch Auskunft über mögliche Unterschiede im normativen Bestand bundes- und landesrechtlichen Regelungen zu den jeweiligen Zugriffstatbeständen geben werden.

In einem zweiten Schritt erfolgt dann die **verfassungsrechtliche Analyse der abstrakten Eingriffsschwere** der verschiedenen Zugriffsmöglichkeiten. Basis wird die umfassende Auswertung aller relevanten höchstrichterlichen Entscheidungen (namentlich des Bundesverfassungsgerichts) und ihre fachliche Kommentierung sein. Ferner kann die im ersten Schritt erhobene konkrete Ausgestaltung des Zugriffs, insbesondere die rechtlichen Vorkehrungen, herangezogen werden, um die Eingriffsintensität zu bewerten und damit die Zugriffe bei der Aggregation zu gewichten.

Das Konzept ist auf die Registrierung von staatlichen Datenabfragen und -zugriffen angewiesen. Insoweit ist hervorzuheben, dass das Bundesverfassungsgericht in seinem Urteil „Bestandsdatenauskunft II“ vom Mai diesen Jahres für eingriffsintensivere Datenabfragen bereits von einer verfassungsrechtlich zwingenden Pflicht nicht nur zur Registrierung, sondern auch zu Dokumentation der Abfragen ausgeht. Eine entsprechende Eingriffsintensität hat es etwa für die Zuordnung dynamischer IP-Adressen angenommen.[14] Bereits aus verfassungsrechtlichen Gründen müssen die für das Projekt besonders relevanten eingriffsintensiveren Zugriffe von den Behörden

[14] BVerfG, 1 BvR 1873/13, 1 BvR 2618/13 v. 27.5.2020, Rn. 248 ff.

dokumentiert werden. Im Interesse einer größeren Transparenz der Sicherheitsbehörden sollten sie jedoch nicht bei dem verfassungsrechtlich geforderten Minimalstandard stehen bleiben und auch der Gesetzgeber zumindest eine technische Registrierung aller Abfragen verlangen, die dann in das Überwachungsbarometer eingespeist werden können. Nicht zuletzt verschafft dies den Behörden auch Rechtssicherheit, da die verfassungsrechtliche Kategorisierung in eingriffsintensive und weniger eingriffsintensive Maßnahmen vage und in der Rechtsprechung noch nicht ausdifferenziert ist.

4.2.2. Erste empirische Daten

Parallel zur rechtlichen Analyse soll die **Zugriffspraxis** bezogen auf die Anzahl der tatsächlichen Zugriffe untersucht werden. Hierfür ist ein Stufenkonzept vorgesehen.

Zunächst soll erfasst werden, zu welchen Eingriffsbefugnissen bereits **statistische Erhebungen** vorliegen, sei es in öffentlich zugänglicher Form (z. B. die Jahresübersichten des Bundesamtes für Justiz zur Telekommunikationsüberwachung oder die Statistiken der Finanztransaktionsuntersuchungen zur Geldwäschekontrolle), sei es zum internen Gebrauch. Auch Informationen aus parlamentarischen Materialien (Berichte der G10-Kommission oder der ParlKK sowie Antworten auf Große/Kleine Parl. Anfragen) sollen ausgewertet werden. Die mitgeteilten Zahlen betreffen allerdings zumeist Vorgänge aus der Vergangenheit und sind in der Regel auch nicht systematisch erhoben. Als Zwischenergebnis ist zu erwarten, dass jedenfalls die öffentlich zugänglichen Daten aktuell so lückenhaft sind, dass daraus ein realistisches Bild zur Überwachungspraxis allenfalls punktuell für sehr spezifische Zugriffe wie die repressive Telekommunikationsüberwachung gewonnen werden kann.

Daher sollen die Möglichkeiten für eine **eigene empirische Untersuchung** der Zugriffspraxis ausgelotet und getestet werden**.** Eine wichtige Quelle hierfür können die heutzutage elektronisch dokumentierten polizeilichen Einsatzprotokolle sein. Die Exploration kann auf der Basis einer nach verschiedenen, im Einzelnen noch zu definierenden Parametern strukturierten Analyse erfolgen. Erhoben werden könnten bspw. quantitative und qualitative, sektorbezogene, maßnahmenbezogene oder adressatenbezogene Aspekte. Dieser Projektteil hätte den Charakter einer **explorativen Studie**, die zunächst auf eine Bundesbehörde und eine oder mehrere Landes(-polizei-)behörden begrenzt werden soll.[15] Die Zugangsmöglichkeiten und der Genehmigungsbedarf werden derzeit zunächst für Baden-Württemberg ermittelt. Ziel dieses Arbeitsschrittes wird es sein, zum einen Struktur und Qualität der dort vorhandenen Daten abzuklären und zum anderen die Felder zu ermitteln, in denen es für die Behörden ohne großen Aufwand möglich sein wird, aggregierte Daten zuzuliefern.

Als ergänzende Informationsquelle sollen zusätzlich Informationen aus den internen Erhebungen wichtiger Provider beigezogen werden. Die internationalen Konzerne weisen in ihren periodischen Transparenzberichten bereits einige allgemeine Angaben zur Häufigkeit behördlicher Abfragen aus, die gegebenenfalls weiter spezifiziert werden könnten. Anfragen bei den zuständigen Abteilungen von *Microsoft*, *Apple* und *Google* nach der grundsätzlichen Kooperationsbereitschaft und den Möglichkeiten zur Einsicht in bzw. Zulieferung von Informationen über zusätzliche, für das Projekt relevante Angaben zu den einschlägigen Fällen sind aktuell in Bearbeitung. Die Auswahl der Firmen ist selektiv. Eine lückenlose Erfassung aller, auch kleinerer Anbieter dürfte nicht realistisch sein. Doch insoweit kommt die hohe Marktkonzentration bei einigen wenigen Akteuren dem Projekt entgegen, da die Daten der meisten Menschen bei diesen gesammelt werden. Die Zugriffszahlen dürften daher eine hohe Repräsentativität für den privaten Sektor haben.

[15] Aufgrund der Erfahrungen des MPI aus früheren Forschungsprojekten ist zu erwarten, dass die Kooperationsbereitschaft in den verschiedenen Bundesländern unterschiedlich ausgeprägt sein wird.

Behörden- und Providerdaten können allerdings nicht einfach aufaddiert werden. Die Daten sind bereits methodisch nicht vergleichbar. Anders als die Behördendaten spiegeln Providerdaten jeweils nur einen Ausschnitt der Gesamtheit aller Abfragen wider. Darüber hinaus kann eine behördliche Maßnahme Daten mehrerer Provider betreffen. Die tatsächliche Streuwirkung kann in ihrer Gesamtheit nur auf der Grundlage der behördlichen Einsatzdokumentationen erfasst werden. Gleichwohl haben die Providerdaten einen hohen Nutzwert. Sie reflektieren die Adressaten-perspektive der behördlichen Maßnahmen und könnten bspw. einen Einblick in den Umfang der abgefragten und übermittelten Informationen geben, etwa die betroffenen Datenarten und Datenvolumina.

Beide Perspektiven – die behördliche und die providerseitige – könnten dann idealiter in Bezug auf verschiedene Datenkategorien gegenübergestellt werden.

Die **endgültige Auswahl der Überwachungstatbestände** wird unter anderem pragmatisch gesteuert sein. Im Fokus werden die präventiven und repressiven Anwendungsalternativen stehen. Auch die Zulieferung belastbarer Informationen der Nachrichtendienste zu ihrer Überwachungspraxis soll überprüft werden. Hier bestehen natürlich spezifische operative Geheimhaltungsinteressen. Diese müssen aber den für das Projekt benötigten aggregierten Daten nicht entgegenstehen, zumal auch verschiedene Aggregationsniveaus denkbar sind. Im Hinblick auf die spezifischen (rechtlichen) Aufgaben der Dienste und der besonderen Kontrollmechanismen wären für eine vernünftige Bewertung dieser Maßnahmen allerdings eigene Kriterien[16] zu entwickeln, was erst in einem späteren Ausbaustadium des Projekts leistbar erscheint.

Für die Bewertung der Befunde sollen am Ende ein oder ggf. mehrere alternative Modelle für eine **verfassungsrechtliche informierte normative Gewichtung** der verschiedenen Überwachungs-szenarien entwickelt werden, orientiert an Variablen wie beispielsweise Anlass, betroffener Grundrechts- und Lebensbereich, Zweckbestimmung, Zugriffsart, -dauer, -breite und -tiefe u.v.a.m. Für die Ermittlung und Ausweisung der jeweiligen Überwachungslast ermöglichen die Daten verschiedene Perspektiven:

- stichtagsbezogen,
- kumuliert für ein Kalenderjahr,
- fokussiert auf eine konkrete – eventuell im Rahmen der Exploration zu identifizierende – Zeitperiode mit potenziellen Überwachungsspitzen (z.B. Sommerzeit),
- behördenspezifische,
- regionale,
- maßnahmenbezogene,
- sogar personale, wenn etwa diachrone Veränderungen mit dem Wechsel der Behördenleitung korrelieren.

Je nach Datenlagen bietet es sich an, die Datensammlung im Rahmen der Pilotstudie auf ein Referenzjahr zu beschränken, oder für einige Bereiche, Zugriffszahlen bereits diachron darzustellen, wie es dem Grundgedanken des Überwachungsbarometers entspricht, das auf einen relativen Vergleich verschiedener Überwachungsniveaus angelegt ist.

Die Ergebnisse der ersten explorativen Studie können als Prototyp bzw. **Demonstrator** dienen, auf deren Grundlage Empfehlungen für die Aufbereitung der Zugriffszahlen in anderen Bereichen

[16] Auch der explizite Bezug des Bundesverfassungsgerichts bei der Bewertung der Vorratsdatenspeicherung auf die Bereiche Gefahrenabwehr und Strafverfolgung könnte in diesem Sinne zu interpretieren sein, siehe oben Fn. 2.

formuliert werden. Am Ende sollen Empfehlungen für die Schaffung eines regelmäßigen Monitoringkonzepts und dessen endgültige konzeptionelle Ausgestaltung erarbeitet werden. Dies beinhaltet neben der Identifizierung solcher Bereiche, in denen gesetzlich normierte Berichts- bzw. Evaluationspflichten verfassungsrechtlich zu implementieren sind, auch die Erarbeitung von Standards, denen die Aufbereitung der Daten entsprechen müsste. Ein periodisches **„Überwachungsbarometer“** könnte dann die Basis für flexible, auf die jeweilige temporäre Überwachungssituation ausgerichtete (rechts-)politische Bewertungen sein. Hierfür könnten die Daten in verschiedenen Aggregationsniveaus aufbereitetet werden: von dem einfach zu erfassenden Gesamtüberwachungsniveau über die Praxis einzelner Behörden bzw. Behördenzweige bis hin zur konkreten Betrachtung der Situation in Bezug auf einzelne Massendatenbestände und Zugriffsinstrumente. Im Übrigen können die Ergebnisse auch im Rahmen künftiger verfassungsgerichtlicher Prüfverfahren von Nutzen sein.

4.3. Zukunftsperspektiven (Phase 3)

Die erstmalige Implementation eines ausgereifteren Überwachungsbarometers und seine Administration und Fortentwicklung wären eine längerfristige Aufgabe, die die Möglichkeiten einer auf zeitnahe Ergebnisse ausgerichteten explorativen Studie im Hinblick auf die erforderlichen personellen und finanziellen Ressourcen deutlich übersteigt. Im Sinne der angedachten Gesamtkonzeption wäre dies die dritte Projektphase. Sie könnte bei einer Behörde oder an einer Forschungseinrichtung angesiedelt werden.

Soweit dies für uns ersichtlich ist, wäre Deutschland mit dem Aufbau eines Überwachungsbarometers das erste Land, dem es gelingen würde, ein quantitatives Instrument für das Monitoring staatlicher Überwachung zu entwickeln. Sollte das Überwachungsbarometer dazu beitragen, die öffentliche Diskussion staatlicher Sicherheitsmaßnahmen empirisch zu unterfüttern und zu versachlichen, könnte es+ – etwa im Kreis der Mitgliedstaaten der Europäischen Union – ein Interesse geben, das Modell aufzugreifen. Damit würde dann auch ein völlig neuer internationaler Vergleich des Zustandes staatlicher Überwachung ermöglicht.