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

Pilotprojekt zur Entwicklung eines periodischen Überwachungsbarometers für Deutschland

Durch das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Abteilung Öffentliches Recht, Freiburg i.Br.

Planungsstand Dezember 2020

Ralf Poscher und Michael Kilchling
unter Mitarbeit von Katrin Kappler und Lukas Landerer

Auftrag: Unter Anknüpfung an den verfassungsrechtlichen Topos einer „Überwachungsgesamtrechnung“ soll ein theoretisch und empirisch unterlegtes Konzept zur Entwicklung eines Instrumentariums zur Erfassung der realen Überwachungslast in Deutschland entwickelt und getestet werden. Hierfür sollen zunächst alle wesentlichen behördlichen Befugnisse zum Zugriff auf allgemeine Datenbestände zu Privatpersonen systematisch analysiert werden. Weiterhin sollen die Häufigkeit und ausgewählte qualitative Merkmale solcher Zugriffe und deren Bewertung auf der Grundlage (verfassungs-)rechtlicher und empirischer Parameter erfasst werden.

1. Zielsetzung

Bei der sog. Überwachungsgesamtrechnung (ÜGR) handelt es sich um einen bislang vorwiegend theoretisch diskutierten verfassungsrechtlichen Topos der der Erfassung bzw. Abschätzung der – kumulierten – 'Überwachungslast' in Deutschland gilt. Der Topos knüpft ursprünglich an das wegweisende Urteil des Bundesverfassungsgerichts (BVerfG) 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 BVerfG führte über diesen konkreten Einzelfall hinaus aus, dass der Gesetzgeber bei der Erwägung neuer Speicherungspflichten und -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen bereits existierenden Datensammlungen zukünftig zu größerer Zurückhaltung gezwungen sei. Daraus hat sich, u.a. angestoßen von Roßnagel, eine rechtspolitische Diskussion über die von ihm 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 quasi auf-

[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.

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

Für ein solches Vorhaben erscheint es nicht hinreichend, Zugriffsnormen und Anwendungszahlen rein quantitativ zu erfassen. Überwachungsmaßnahmen und Zugriffe auf datenförmig hinterlegte Informationen müssen darüber hinaus auch näher spezifiziert und im Hinblick auf ihre Zielsetzung und ihre Eingriffswirkung gewichtet werden. So dürfte beispielsweise ein nach abstrakter Bewertung eingriffsintensiver präventiver Echtzeit-Zugriff auf mobile Standortdaten einer in einem weitläufigen Waldgebiet vermissten Person oder ihrer Begleitung zur Abwendung einer konkreten Gefahr für Leib oder Leben anders zu bewerten sein als die repressive Abfrage von Kontodaten zur Aufklärung eines mutmaßlichen Geldwäsche- oder anderen Vermögensdelikts; beide könnten ihrerseits schwerer wiegen als etwa die massenhafte, potenziell Hunderttausende betreffende Verkehrsüberwachung mittels nummernbasierter Abschnittskontrolle. Als entscheidende Parameter müssen sowohl die verfassungsrechtliche als auch die empirische Eingriffsintensität berücksichtigt und zueinander ins Verhältnis gesetzt werden.

In dem explorativen Forschungsprojekt soll der Versuch unternommen werden, das den verfassungsrechtlichen Topos der ÜGR 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 verfolgt daher einen Ansatz, der auf eine relationierende Perspektive setzt. Das Projekt soll den synchronen und diachronen Vergleich unterschiedlicher Überwachungsniveaus ermöglichen. Im Rahmen des Projekts soll aber zumindest die Möglichkeit offengehalten werden, dass sich aus dem Vergleich Rechtfertigungslasten politischer, aber auch rechtlicher Natur ergeben. Dies gilt zum einen für die (verfassungs-)rechtliche Perspektive (bezogen auf die abstrakte Un-/Zulässigkeit neuer, zusätzlicher Überwachungsinstrumente) zum anderen in empirisch-rechtstatsächlicher (etwa bezogen auf eine potenziell hohe oder zu hohe Anwendungshäufigkeit bestimmter Maßnahmen insgesamt oder auf die Un-/Verhältnismäßigkeit einer Vielzahl einzelner Maßnahmen in einem konkreten Einzelfall[8]).

Es wird allerdings zu beachten sein, dass auch ohne explizite Änderung des rechtlichen Rahmens beispielsweise eine neu entwickelte technische Alternative eine bis dahin praktizierte eingriffs-intensive(-re) Überwachungsmethode überflüssig machen oder deren Anwendung reduzieren,[9]

---

[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] In diesem Sinne hat sich die Verkehrsdatenabfrage als (strafrechtliche) Ermittlungsmaßnahme seit den 1990er Jahren zu einem viel genutzten funktionalen Äquivalent zur 'klassischen' Telefonüberwachung entwickelt. Denn in vielen Fällen besteht von vornherein kein kriminalistischer Bedarf an dem im Vergleich deutlich schwerwiegenderen Abhören und Aufzeichnung von Gesprächsinhalten, die in früheren Jahren quasi 'mit' erhoben wurden. Vgl. *Albrecht & Kilchling*, Die Überwachung von Telekommunikations-Verkehrsdaten,

ebenso wie umgekehrt die Entwicklung und Nutzung neuer technologischer Möglichkeiten die (verfassungs-)rechtliche Bewertung einer bis dato als weitgehend unbedenklich bewerteten Maßnahme unter Umständen signifikant verändern kann.[10] Solche Entwicklungen der Überwachungspraxis müssen bei der Definition 'roter Linien' in vorausschauender Weise berücksichtigt werden.

Um die Dynamik der Entwicklung sowohl bei der Anwendung bestehender wie auch bei der Schaffung neuer bzw. erweiterter Überwachungstatbestände[11] zu erkennen und zu interpretieren, ist zu empfehlen, die Überwachungslast nicht nur einmalig zu erfassen, sondern in Richtung eines regelmäßigen Monitorings im Sinne eines periodischen Überwachungsbarometers weiterzuentwickeln. Mit einem solchen Instrument könnte dann der jeweils aktuelle Status Quo nicht nur aufgezeigt, sondern im Kontext kurz- und längerfristiger Entwicklungslinien interpretiert und die rechts- und gesellschaftspolitische Diskussion mit einer belastbaren empirischen Datengrundlage unterstützt werden. Dies kann auch wesentlich zur Versachlichung der politischen Debatte beitragen.

2. Probleme bisheriger Ansätze

- Keine klare Abgrenzung der ins Auge gefassten Datenbestände,
- Vernachlässigung privater Datensammlungen,
- Orientierung an einem durch die Wirklichkeit überholten Konzept der Datenvermeidung,
- Befangenheit in grundrechtlicher Konzeption, die dazu tendieren kann, den Datenschutz zum Selbstzweck werden zu lassen, die der Akzeptanz des Datenschutzes schadet.

3. Lösungsansatz

- Klare Abgrenzung durch Orientierung an anlasslos erfassten (Massen-)Daten,
- Einbeziehung privater Datenbestände,
- Orientierung an den spezifischen abstrakten Gefahren, die sich anhand der Abfragen und Zugriffe erfassen lassen,
- Orientierung an einer Neukonzeption des Rechts auf informationelle Selbstbestimmung im Sinne einer Querschnittsgrundrechtskonzeption, die der Vorverlagerung des Grundrechtsschutzes aller Grundrechte zur Abwehr abstrakter Gefahren der Datenspeicherung dient, aber auch eine Betrachtung verlangt, die an diesen dann auch zu benennenden Gefahren ansetzt.[12]

MPG-Jahrbuch 2008 (m.w.N.); *Albrecht et al*., Schutzlücken durch Wegfall der Vorratsdatenspeicherung? (2011).

[10] *Adensamer*, [österr.] Handbuch Überwachung (2020), 45, verweist auf das Beispiel sog. technologieneutraler Normen. Zu denken wäre etwa an die Beschlagnahme der Aufzeichnungen von privaten Kfz.-Navigations- oder smarten Haushaltsgeräten u.v.a.m. auf der Grundlage von Normen, die ursprünglich auf den physikalischen Zugriff auf einzelne papierne Unterlagen ausgerichtet waren.

[11] Auch die technologische Entwicklung ist dabei zu berücksichtigen; vgl. auch *Adensamer*, Aspekte einer Überwachungs-Gesamtrechnung, FIfF-Kommunikation 4/19, 25.

[12] 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.

4. Grundzüge des Untersuchungsdesigns und aktueller Planungsstand

4.1. Phase 1 (im Wesentlichen abgeschlossen)

Es existiert eine Vielzahl **staatlicher – d.h. staatlich generierter und/oder administrierter – und privater Datensammlungen**. Die besonders praxisrelevanten Überwachungsszenarien wurden in einem ersten Arbeitsschritt gesammelt und systematisiert (siehe die tabellarische Übersicht im Anhang[13]). Die Auflistung gibt einen Überblick über den aktuellen Status Quo in Deutschland. Eine solche umfassende Bestandsaufnahme der Überwachungs-'Landschaft' existierte bislang nicht. Allerdings kann im Rahmen der Pilotstudie zunächst nur eine begrenzte Auswahl hieraus exemplarisch berücksichtigt werden. Die Liste soll darüber hinaus als Orientierung für die in dem späteren Überwachungsbarometer einzubeziehenden Sachverhalte dienen. Die erste Auswahl wird sich schwerpunktmäßig auf die **anlasslos gespeicherten Massendaten** konzentrieren. Die Übersicht zeigt eindrücklich, dass Daten bzw. Datenbestände privater Akteure – die von Privatpersonen im eigenen privaten Umfeld angelegten ebenso wie die bei privatwirtschaftlichen Dienstleistern (vom Internet-Provider bis zur privaten Hausbank) hinterlegten und von diesen generierten – die durch unmittelbare staatliche Eingriffe (auf gesetzlicher, ggf. auch richterlicher Grundlage) ad hoc und selbst generierten Datenbestände quantitativ inzwischen deutlich übersteigen (vgl. Tabellenspalte 3[14]).

Im Hinblick auf die zunehmende Dominanz des privaten Datenmanagements ist zunächst eine sachliche Grenzziehung erforderlich. Der Fokus der Untersuchung soll auf die **wesentlichen staatlichen Zugriffsrechte** auf derartige Datenbestände (einschließlich entsprechender pro-aktiver Auskunfts- und Meldepflichten) gerichtet sein. A priori *nicht berücksichtigt* wurden in unserer Aufstellung daher zum einen *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[15] –, zum anderen *anlassbezogene* bzw. *durch eigenverantwortliches Verhalten der Betroffenen ausgelöste Registrierungen* in öffentlichen Dateien – Bundeszentralregister, die verschiedenen Fahndungsdateien (SIS, etc.), das Fahreignungsregister des KBA ('Verkehrssünder'-Datei), das Gewerbezentralregister, u.v.a.m.

Die gesammelten potenziell untersuchungsrelevanten Überwachungssachverhalte umfassen insbesondere die folgenden Kategorien:

- Telekommunikationsdaten: Bestands-, Verkehrs-, offene und verschlüsselte Inhaltsdaten (Nr. 1 bis 4),
- Computerdaten (Nr. 5),
- Finanztransaktions-, Konto- und weitere Bankdaten (Nr. 6, 7),
- Mobilitätsdaten (Nr. 8),
- Daten aus dem privaten Lebensbereich (Wohnraumüberwachung, Zugriff auf smarte Haushaltsgeräte, Nr. 9); im Falle ihrer Einführung würde künftig wohl auch die Überwachung des privaten Kommunikationsverhaltens in sozialen Netzwerken nach dem NetzDG in diesen sachlichen Kontext fallen (Nr. 10),

[13] Die noch ausstehen Einzelnachweise aller Landesgesetze werden im Laufe der Phase 2 vervollständigt werden.

[14] Lediglich in den unter Nr. 3, 4, 5, 8f und 9a/b aufgelisteten Fällen werden Daten direkt durch Behörden erhoben. In allen anderen Konstellationen erfolgt die Informationsgewinnung durch Abfrage von bzw. Zugriff auf anlasslos von/bei Dritten gespeicherte Datenbestände.

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

- Gesundheitsdaten (Nr. 11, noch näher zu prüfen[16]),
- sonstige private Daten, die in Mobilgeräten lokal oder in Firmenservern oder Cloudspeichern abgelegt sind, oder technische Daten, die bei IT-Dienstleitungen aller Art automatisch anfallen;[17] 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 (Nr. 12, ggf. noch näher zu spezifizieren),
- Meldedaten im Kontext der automatisierten Passbildabfrage (Nr. 13) sowie
- die Rasterfahndung (Nr. 14), 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.

Die Übersicht enthält schließlich eine Kategorie "einmalige bzw. sondergesetzliche Datenzugriffe. Als aktuelles Beispiel wird dort auf das ZensusvorbereitungsG 2021 hingewiesen (s.o., Nr. 15a). Bekanntlich hat die Dogmatik zum Grundecht auf informationelle Selbstbestimmung ihren Ursprung ja in dem sog. Volkszählungsurteil des BVerfG aus dem Jahr 1983.[18] Hierbei handelt es sich zwar um eine einmalige Datenerhebung. Im Hinblick auf die längerfristige Perspektive des geplanten Ü-Barometers erscheint es aus grundsätzlichen konzeptionellen Überlegungen durchaus sinnvoll, Einmalereignisse in einem späteren permanenten Barometer mit zu berücksichtigen und in einer Extra-Rubrik solche "Sonderereignisse" für das jeweilige Jahr auszuweisen. Besondere Situationen oder (einmalige) Ereignisse, die sich in einer ungewöhnlichen, ggf. auch kurzfristigen Häufigkeit bestimmter Maßnahmen niederschlagen würden, könnten auch im Kontext anderer Überwachungssachverhalte zu beobachten sein, z.B. durch politische Ereignisse (z.B. G20-Gipfel), Fußball-WM, Terrorschlag, großräumige Ermittlungsmaßnahmen oder Strukturermittlungen (z.B. im OK- oder Clanmilieu), etc. Eventuell könnten auch gewisse Zugriffe von Sicherheitsbehörden (Polizei, StA, Ordnungsbehörden, Dienste) auf Daten, die zunächst temporär und eigentlich zweckgebunden im Rahmen der aktuellen COVID-Maßnahmen erhoben werden (s.o., Nr. 11) unter diese Rubrik eingeordnet werden. Solche Ereignisse haben das Potenzial, die Überwachungslast in einer bestimmten Periode (Referenzjahr) temporär zu erhöhen.

Vorläufig nicht einbezogen wurden grundsätzlich die verschiedenen *polizeilichen Datenbanken*. Diese Datenbanken könnten zwar je nach ihrer konkreten Organisation und Ausgestaltung Merkmale einer (behördlichen) Vorratsdatenspeicherung aufweisen; sie haben jedoch nicht den Charakter einer Massendatensammlung, die ursprünglich Anlass zur Entwicklung des Topos der Überwachungsgesamtrechnung gab. Dennoch tragen auch sie zum Gesamtüberwachungsstatus bei. In der Ausbauphase des Projekts sollten daher jedenfalls diejenigen anlassbezogenen Datenbanken der Sicherheitsbehörden mit besonderer grundrechtlicher Relevanz Berücksichtigung finden. Um einen Eindruck

[16] Zu polizeilichen Zugriffen auf Gästelisten z.B. in Ba.-Wü.: www.swr.de/swraktuell/baden-wuerttemberg/heilbronn/gastro-gaesteliste-corona-polizei-100.html oder Bayern: www.br.de/nachrichten/bayern/bayerische-polizei-nutzt-gaestelisten-auch-bei-kleineren-delikten,S9RyYdj.

[17] 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.

[18] BVerfG, 1 BvR 209/83 v. 15.12.1983, BVerfGE 27, 1. Auch die Umstände der bevorstehenden Erhebungswelle sieht das Gericht durchaus nicht unkritisch. Ein Eilantrag wurde zwar vom BVerfG abgelehnt, das Gericht bezweifelte aber zumindest die Erforderlichkeit des Testlaufs; BVerfG, 1 BvQ 4/19 (Beschluss der 2. Kammer des Ersten Senats) v. 6.2.2019.

davon zu gewinnen, welche besonderen Fragen sich hinsichtlich entsprechender Dateien stellen, soll die **Antiterror-Datei**[19] exemplarisch in die Entwicklung des Projekts einbezogen werden.

Grundsätzlich ausgeklammert bleibt ferner die *Videoüberwachung*. Sie ist im Wesentlichen privat administriert und scheidet daher ebenfalls aus. Soweit Videoüberwachung im Öffentlichen Raum stattfindet, wird sie im Wesentlichen unter kommunaler Trägerschaft durchgeführt; eine realitätsnahe Erfassung im Rahmen des vorliegenden Projekts erscheint unrealistisch. Ferner ist bei der öffentlichen Videoüberwachung eine systematische Speicherung der Daten nicht vorgesehen. Die Bildaufzeichnungen werden in der Praxis regelmäßig nach max. 48 Stunden gelöscht.[20] Eine umfangreiche Datensammlung, wie sie im Rahmen dieses Projekts untersucht werden, existiert daher nicht. Die reine Erhebung der Daten dürfte überdies nur einen geringen Grundrechtseingriff darstellen. Maßgeblich ist hier noch die sog. Sphärentheorie des BVerfG[21], nach welcher nur ein (leicht zu rechtfertigender) Eingriff in die Sozialsphäre vorliegt. Einzelne Zugriffe auf temporär gespeicherte Bilddateien werden im Übrigen unter anderen Rubriken (vgl. Nr. 9b u. 12) miterfasst.

4.2. Phase 2

In der zweiten Phase soll zunächst 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 zwischen bundes- und landesrechtlichen Regelungen zu den jeweiligen Zugriffstatbeständen geben werden. Die konkrete Ausgestaltung des Zugriffs, insbesondere die rechtlichen Vorkehrungen, wird sicherlich ein Teilaspekt bei der rechtlichen Bewertung der Eingriffsintensität sein.

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 BVerfG) und ihre fachliche Kommentierung sein.

Die verfassungsrechtliche Analyse bietet noch weitere Anknüpfungspunkte: In seinem Urteil "Bestandsdatenauskunft II" hat das BVerfG etwa entschieden, dass es nicht verhältnismäßig ist, wenn Bestandsdaten ohne Dokumentation der Ermächtigungsgrundlage abgerufen werden, die anhand einer dynamischen IP-Adresse bestimmt werden. Dies folgerte es aus der hohen Eingriffsintensität der Maßnahme.[22] Aus diesem Grund sind alle eingriffsintensiven Maßnahmen, die ohne die Dokumentation von Rechtsgrundlagen erfolgen, verfassungswidrig. Eingriffsintensive Maßnahmen müssen bereits aus verfassungsrechtlichen Gründen dokumentiert werden. Insoweit müssen bei den Behörden also zukünftig Daten vorliegen. Darüber hinaus stellt das Gericht hinsichtlich einer möglichen Evaluation, dass eine Evaluation bei Eingriffen von geringer Intensität nicht erforderlich ist.[23] Dies bedeutet aber zumindest auch, dass aus der Verfassung bei eingriffsintensiven Maßnahmen eine Evaluierungspflicht folgen könnte. Für diese müssen die Daten dann auch aufbereitet werden. Zu berücksichtigen ist dabei zum einen, dass dies 'nur' die verfassungsrechtlichen Mindeststandards sind.

---

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

[20] *Wilhelm* in BeckOK Datenschutzrecht, BDSG § 4, Rn 49 mit Verweis auf DSK, Videoüberwachung nach der Datenschutz-Grundverordnung, Kurzpapier Nr. 15, 3.

[21] Allg. BVerfGE 34, 238, 245; allerdings gilt die Sphärentheorie wohl prinzipiell nicht im Bereich der Datenverarbeitung, vgl. *Desoi/Knierim*, Intimsphäre und Kernbereichsschutz, DÖV 2011, 398, 401; *Dreier* in Dreier GG, Art. 2, Rn. 93.

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

[23] BVerfG, aaO., Rn. 251.

Es spricht aber alles dafür, dass die Sicherheitsbehörden sich nicht auf der Grenze zur Verfassungswidrigkeit ihres Handelns bewegen sollten. Für die Behörden bedeutet eine Dokumentation im Hinblick auf die neue Rechtsprechung zudem auch Rechtssicherheit: Dokumentiert die Behörde die gesetzliche Grundlage einer Maßnahme nicht, weil sie von einer niedrigen Eingriffsintensität ausgeht, beurteilt das Bundesverfassungsgericht den Eingriff aber als hoch, wäre die jeweilige Maßnahme schon allein aufgrund der fehlenden Dokumentation rechtswidrig – unabhängig davon, ob die Tatbestandsvoraussetzungen der Ermächtigungsgrundlage vorliegen. Dies ist vor allem bedeutsam, weil die Abgrenzung des BVerfG in eingriffsintensive und weniger eingriffsintensive Maßnahmen vage und in der Rechtsprechung noch nicht ausdifferenziert ist.

Parallel hierzu 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 öffentlich zugänglicher Form (z.B. die Jahresübersichten des Bundesamtes für Justiz zur TKÜ oder die Statistiken der FIU 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) können nützlich sein; in einzelnen Bereichen könnten sie auch die einzige zugängliche (bzw. belastbare) Informationsquelle sein. Die mitgeteilten Zahlen betreffen allerding zumeist Vorgänge aus der Vergangenheit und sind in der Regel auch nicht systematisch erhoben. Als Zwischenergebnis wäre 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 TKÜ 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 strukturierte 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.[24] 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 bearbeiteten 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,

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

da die Daten der meisten Menschen bei diesen gesammelt werden. Die Zugriffszahlen dürften daher eine hohe Repräsentativität für den privaten Sektor haben.

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 für verschiedene Datenkategorien gegenübergestellt werden.

Die **endgültige Auswahl der Überwachungstatbestände** wird auch pragmatisch gesteuert sein. Im Fokus werden die präventiven und repressiven Anwendungsalternativen stehen. Auch die Zulieferung belastbarer Informationen der Geheimdienste zu ihrer Überwachungspraxis soll überprüft werden. Hier bestehen natürlich spezifische operative Geheimhaltungsinteressen. Diese müssen u.U. aber den für das Projekt benötigten aggregierten Datensammlungen 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, vom 'alltäglichen' Überwachungsgeschehen abweichende Kriterien[25] zu entwickeln, was erst in einem späteren Ausbaustadium des Projekts leistbar erscheint.

Für die finale Bewertung der Befunde sollen am Ende eines oder ggf. alternative Modelle für eine **verfassungsrechtliche und empirische (soziale) Gewichtung** der verschiedenen Überwachungs-szenarien entwickelt werden, orientiert an Variablen wie beispielsweise Anlass, betroffener Grundrechts-/Lebensbereich, Zweckbestimmung, Zugriffsart, -dauer, -breite und -tiefe, u.v.a.m. Auch für die Ermittlung und Ausweisung der jeweiligen Überwachungslast sind unterschiedliche Modelle denkbar:

- stichtagsbezogen,
- kumuliert für ein Kalenderjahr,
- fokussiert auf eine konkrete – eventuell im Rahmen der Exploration zu identifizierende – Zeitperiode mit potenziellen Überwachungsspitzen (z.B. Sommerzeit),
- etc.

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 dieser explorativen Studie können als Prototyp bzw. **Demonstrator** dienen, auf deren Grundlage Empfehlungen für die Aufbereitung der Zugriffszahlen in anderen Bereichen formuliert werden. Am Ende sollen Empfehlungen für die Schaffung eines regelmäßigen Monitoringkonzepts und

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

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 Reaktionen 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. Zukunftsperspektive (Phase 3)

Die erstmalige Implementation des kompletten Überwachungsbarometers und seine Administration und Weiterführung 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. Eine Übernahme des damit verbundenen Forschungsaufwandes erfordert eine auf einen längeren Zeitraum – ggf. mehrere Jahre – angelegte vertragliche Grundlage, ausreichende finanzielle Ressourcen sowie verlässlichen administrativen Support durch die im Rahmen der vorlaufenden explorativen Studie identifizierten datenführenden Stellen, ggf. auch in förmlicher Kooperation mit staatlichen Stellen.

Der Zeitrahmen des Projekts ist so gewählt, dass die Ergebnisse im politischen Raum angemessen rezipiert werden können. Einzelne Aspekte wie die Schaffung weitergehender behördliche Dokumentationspflichten,[26] die Bereitstellung von Haushaltmitteln für die Implementation eines periodischen Ü-Barometers und Kooperations- bzw. Datenübermittlungsregelungen könnten Gegenstand eines Programms für die kommende Legislaturperiode sein. Auch die FNF könnte hier, ebenso wie andere Akteure, unterstützend aktiv werden.

– Anhang: Systematischer Überblick über die potenziell relevanten Überwachungstatbestände –

[26] So könnte die Schaffung weiterer gesetzlicher Dokumentations- und Berichtspflichten nach dem Vorbild der §§ 88 BKAG oder 101b StPO hilfreich sein.