FRIEDRICH NAUMANN
STIFTUNG Für die Freiheit.

ÜBERWACHUNGS-BAROMETER FÜR DEUTSCHLAND

EIN MODELLKONZEPT

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

Prof. Dr. Ralf Poscher, Dr. Dr. h.c. Michael Kilchling
und Lukas Landerer, LL.M.

ANALYSE

Impressum

Herausgeberin
Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheit

Autoren
Prof. Dr. Ralf Poscher, Dr. Dr. h.c. Michael Kilchling und Lukas Landerer, LL.M.
unter Mitarbeit von Esther Bauer und Joy Schilling
Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht,
Abteilung öffentliches Recht, Freiburg i.Br.

Redaktion
Teresa Widlok, Referentin für Bürgerrechte und Rechtsstaatlichkeit
Liberales Institut der Friedrich-Naumann-Stiftung für die Freiheit

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand
Januar 2022

ISBN
978-3-948950-12-5

Inhalt

Executive Summary

Die neue Bundesregierung hat sich in ihrem Koalitionsvertrag vorgenommen die bestehenden Sicherheitsgesetze und ihre Auswirkungen auf Freiheit und Demokratie zu evaluieren. Zu diesem Zweck soll eine Überwachungs-Gesamtrechnung erstellt werden. Schon im Jahr 2010 fällte das Bundesverfassungsgericht (BVerfG) ein wegweisendes Urteil zur anlasslosen Vorratsdatenspeicherung. In der Rechtswissenschaft entwickelte sich aufgrund der Hinweise in dem Urteil an den Gesetzgeber, wie mit neuen Speicherpflichten und Befugnisse zum behördlichen Zugriff auf personenbezogene Daten umzugehen sei, eine Diskussion rund um den Begriff der sogenannten „Überwachungs-Gesamtrechnung" (Roßnagel). Die Diskussion blieb bisher vor allem theoretisch und orientierte sich an den vom BVerfG in seiner Rechtsprechung aufgestellten rechtlichen Parametern.

Das Freiburger Max-Planck-Institut (MPI) zur Erforschung von Kriminalität, Sicherheit und Recht hat im Auftrag der Friedrich-Naumann-Stiftung für die Freiheit ein theoretisch und empirisch unterlegtes Konzept entwickelt, mit dem sich eine Überwachungs-Gesamtrechnung operationalisieren lässt. Das vom MPI entwickelte Modell eines Überwachungsbarometers soll die reale Überwachungslast der Bürgerinnen und Bürger in Deutschland, und damit ihre Freiheitsbelastung, erfassen. Die Quantifizierung der Überwachungslast geschieht auf Grundlage einer Kombination der aktuell existierenden rechtlichen Zugriffsmöglichkeiten (verfassungsrechtliche Perspektive) mit der realen Zugriffspraxis (empirische Perspektive).

Belastbare Informationen zu der Gesamtheit tatsächlich durchgeführter Überwachungsmaßnahmen sowie zu deren Eingriffsintensität waren und sind bislang nicht oder nur lückenhaft verfügbar. Auch das Modell eines Überwachungsbarometers für Deutschland beschränkt sich zunächst auf eine Auswahl besonders eingriffsrelevanter Überwachungssachverhalte, zu denen ausreichend auswertbare Zahlen vorliegen. Ziel ist es, reale Schwerpunkte der Überwachung auf der Grundlage der aktuellen Sicherheitsgesetzgebung und der Nutzung der damit verbundenen Eingriffsbefugnisse aufzuzeigen. Das Überwachungsbarometer schafft einen soliden evidenzbasierten Unterbau für die rechtspolitische Debatte zu Überwachungsbefugnissen und für die Bewertung der Situation durch die Rechtsprechung.

Die Erstellung des Überwachungsbarometers erfolgt in sechs Schritten:

1. Identifizierung der einzubeziehenden Datensammlungen (Überwachungsszenarien);

2. rechtliche Analyse, welche Sicherheitsbehörden auf Basis welcher rechtlichen Grundlagen und unter welchen Bedingungen Zugriff auf die Datensammlungen nehmen können;

3. Ermittlung spezifischer Zugriffszahlen für jeden der ausgewählten Zugriffssachverhalte; hierfür sind verschiedene Zugangswege denkbar; auch Provider-Daten könnten wichtige Informationen liefern;

4. Gewichtung der Zugriffe nach verfassungsrechtlichen – vom BVerfG kontinuierlich (weiter-)entwickelten – Kriterien; für jeden Zugriffspfad wird somit ein spezifischer Intensitätswert errechnet;

5. Errechnung der spezifischen Indexwerte für die einzelnen Überwachungsszenarien; hierfür wurde eine Formel entwickelt, die die Anzahl der Zugriffe (quantitative Komponente) ebenso wie ihren jeweiligen Intensitätswert (qualitative Komponente) berücksichtigt; Vorbild für die Formel war unter anderem der Index der Pressefreiheit, der von der Organisation „Reporter ohne Grenzen" herausgegeben wird;

6. Überwachungsindizes können für einzelne Zugriffspfade, ganze Überwachungsszenarien, die Überwachungslandschaft im Allgemeinen oder nach regionalen Schwerpunkten errechnet und aggregiert werden. Die Darstellung in Form von Einzelindizes verdeutlicht nicht nur die – kumulierte – Überwachungsgesamtlast, sondern auch ihre Zusammensetzung.

Der Mehrwert des vorgelegten Modellkonzepts beschränkt sich aber nicht nur auf das Endprodukt der Überwachungsindizes und des Überwachungsbarometers. In jedem der sechs Arbeitsschritte werden zusätzliche Ergebnisse generiert, die jeweils einen eigenen wissenschaftlichen und rechtspolitischen Aussagewert haben und das Spektrum der Informationen über das Überwachungsgeschehen in Deutschland damit bereichern. Einige Beispiele:

I. **Bestandsaufnahme der aktuellen Überwachungslandschaft:** Es werden 14 übergeordnete Kategorien von Datenarten identifiziert, auf die von unterschiedlichen Behörden in einer Vielzahl von spezifischen Sachverhalten zugegriffen werden kann. Die so zusammengefügten Überwachungsszenarien reichen von der klassischen Telekommunikationsüberwachung, über die Abfrage von Account-Daten bei Telemediendiensten bis hin zur anlasslosen Vorratsdatenspeicherung von Kundendaten bei Banken zur Geldwäschekontrolle oder von Flugpassagierdaten zur Terrorismusbekämpfung.

II. **Kartographie der Überwachungslandschaft:** Für die jeweiligen Zugriffsmöglichkeiten auf Datenbestände lassen sich Übersichtskarten erstellen, die die spezifischen Zugriffspfade der Behörden im Detail aufzeigen. Dadurch entsteht eine plastische Darstellung der verschiedenen Überwachungsszenarien.

III. **Häufigkeitszahlen:** Mit den verfügbaren Rohdaten ist ein Depot an Daten entstanden, das in der vorgelegten Breite und Qualität bislang noch nicht vorhanden war und für Teilbereiche bereits den zeitlichen Vergleich ermöglicht. Nicht für alle potenziell relevanten Überwachungsszenarien sind aktuell ausreichend belastbare Daten verfügbar, sodass zunächst nur Teilbereiche berechnet werden können. Für ein breiteres Gesamtbild müssen noch weitere Zahlen gesammelt werden.

IV. **Eingriffsintensität:** Für die Intensitätsberechnung der einzelnen Zugriffe wurde ein Kategoriensystem entwickelt, das eine Gewichtung der verschiedenen Überwachungsmaßnahmen ermöglicht. Es berücksichtigt 16 verfassungsrechtlich relevante Kriterien (Variablen), die in die Berechnung der Eingriffsintensität einfließen und die damit verbundene Überwachungslast nach einem einheitlichen Maßstab quantifizieren. Die Kriterien umfassen z.B. die Heimlichkeit einer Maßnahme, ob ein Richtervorbehalt vorgesehen ist, die Dauer einer Maßnahme und deren Anlass.

V. **Umfassende Datenauswertung:** Die Überwachungsindizes werden ergänzt durch weitere statistische Auswertungen der verfügbaren aggregierten Daten. Hierfür werden verschiedene Darstellungsarten vorgestellt, die das Überwachungsgeschehen erkennbar und die aus der Überwachungslast resultierenden Risiken für die Bürgerinnen und Bürger greifbar machen. Exemplarische Beispiele sind die tabellarische Darstellung ausgewählter Maßnahmen im Jahresvergleich, die Darstellung der kontinuierlichen Zu- und Abnahmeraten über einen längeren Zeitraum oder in Form der durchschnittlichen Anzahl von Zugriffen pro Tag bzw. als Inzidenzwert bezogen auf 100.000 Einwohner.

Durch die Verwendung aggregierter Daten ist das Überwachungsbarometer datenschutzrechtlich unbedenklich, unterliegt aber auch gewissen Limitationen. Zum einen können keine Aussagen zur Überwachungslast im Einzelfall oder bezogen auf bestimmte Personengruppen getroffen werden. Zum anderen ist ein Vergleich von Tatbestände der Massenüberwachung mit extremen Einzelfällen wie im Fall der sog. Quellen-TKÜ oder der Online-Durchsuchung methodisch anspruchsvoll.

Die Realisierung und kontinuierliche Erweiterung des Überwachungsbarometers wird auf politische Unterstützung angewiesen sein, auf der gesetzgeberischen Ebene sowie bei einzelnen datenführenden Behörden. Das Gutachten schließt deshalb mit rechtspolitischen Forderungen für verbesserte Transparenzregelungen und einen leichteren Zugang der Forschung zu den relevanten Daten.

1. Zielsetzung

Das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht hat im Auftrag der Friedrich-Naumann-Stiftung für die Freiheit ein theoretisch und empirisch unterlegtes Konzept zur Entwicklung eines Instrumentariums ausgearbeitet und getestet, das unter Anknüpfung an die verfassungsrechtliche Diskussion über die Notwendigkeit einer „Überwachungs-Gesamtrechnung" die reale Überwachungslast der Bürgerinnen und Bürger in Deutschland erfasst. Hierfür sollten zunächst alle wesentlichen behördlichen Befugnisse zum Zugriff auf allgemeine Datenbestände von bzw. über Privatpersonen systematisch analysiert werden. Darüber hinaus sollten die Häufigkeit und ausgewählte qualitative Merkmale solcher Zugriffe und deren Bewertung auf der Grundlage (verfassungs-)rechtlicher und empirischer Parameter erfasst und in einen allgemeinen Überwachungsindex überführt werden. Nach Abschluss der ersten explorativen Phase soll das Modell des Überwachungsbarometers, das hier vorgestellt wird, implementiert und zu einem periodischen Instrument weiterentwickelt werden, das die Entwicklung der Überwachungssituation kontinuierlich erfasst und bewertet und die Ergebnisse der interessierten Öffentlichkeit in einem regelmäßigen Turnus zur Verfügung stellt.

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 aus dem Jahr 2010 zur anlasslosen Vorratsdatenspeicherung[1] an. Dort erklärte das Gericht eine anlasslose Vorratsdatenspeicherung im Bereich der Telekommunikation für Zwecke sowohl der Gefahrenabwehr als auch der Strafverfolgung[2] zwar grundsätzlich für zulässig, bewertete jedoch die konkrete Ausgestaltung der (damaligen) Regelungen im Telekommunikationsgesetz als verfassungswidrig. Das Gericht 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 aufaddiert.[5] Die Überwachungsgesamtrechnung ist bislang nur in rudimentären Ansätzen operationalisiert worden. Die Vorschläge der Literatur halten sich noch im Vagen und begnügen sich weitestgehend mit Vorschlägen dazu, wie man die Gesamtheit der Rechtsgrundlagen abstrakt bewerten könnte.

Die bisherigen Ansätze weisen einige analytische Schwächen auf, die bei der Konzeption des Überwachungsbarometers vermieden werden sollten. Dies betrifft zunächst den mitunter einseitig auf die abstrakte Normebene und Frage zur verfassungsrechtlichen „Grenzziehung" gerichteten Fokus.[6] Der Umfang der in die Überwachungsgesamtrechnung einzubeziehenden Sachverhalte bleibt mitunter recht unbestimmt.[7] Empirisch unterlegte Konzepte fehlen bislang. Daher mangelt es auch an einer Auseinandersetzung mit Fragen zu dem Verhältnis von abstrakter Überwachungslast auf der normativen Ebene und der tatsächlichen Belastung aufgrund der quantitativen Anwendung der Rechtsgrundlagen. Ferner fällt auf, dass es häufig an einer klaren Bestimmung aller potenziell relevanten Überwachungstatbestände und der damit adressierten Datenbestände fehlt. So war die öffentliche Diskussion in der Vergangenheit auf einige ausgewählte Überwachungsszenarien, insbesondere die anlasslose Vorratsdatenspeicherung im Zusammenhang mit Telekommunikation, fokussiert, während andere Bereiche wie die vergleichbar eingriffsintensive Vorratsdatenspeicherung von Finanzdaten[8] bislang eher wenig Aufmerksamkeit genießen. Das Barometer nimmt im Gegensatz hierzu systematisch alle Arten von anlasslos erfassten (Massen-)Daten gleichermaßen in den Blick. Dabei sind private Daten bzw. Datensammlungen explizit mit einzubeziehen.[9]

1 BVerfG, 1 BvR 256/08 u.a. v. 2.3.2010, BVerfGE 150, 260 = 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 Übersicht bei *Pohle*, Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung. Ein Alternativvorschlag. FIfF-Kommunikation 4/19, 37.
5 Additiver Grundrechtseingriff. Ausführlicher *Winkler*, JA 2014, S. 881.
6 Hierzu *Bieker/Bremert/Hagendorff* in Roßnagel/Friedewald/Hansen (Hrsg.), Die Überwachungs-Gesamtrechnung, 2018, S. 139 (146 f.); Bieker/Bremert FIfF-Kommunikation 2019(4), 34.
7 So *Braun/Albrecht* VR 2017, 151.
8 Ausführlich zu den kontinuierlich erweiterten Geldwäschekontrollregimen *Vogel/Maillart*, National and International Anti-Money Laundering Law (2020). Ein gerade begonnenes Promotionsprojekt am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht analysiert die Vorratsdatenspeicherung von Finanzdaten aus verfassungsrechtlicher Perspektive.
9 Siehe auch *Poscher*, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in Gander et al. (Hrsg.), Resilienz in der offenen Gesellschaft (2012), 167–190; ders., The Right to Data Protection, in Miller (ed.), Privacy and Power, CUP 2017, 129–142; ders., Artificial Intelligence and the Right to Data Protection, Max Planck Institute for the Study of Crime, Security and Law Working Paper No. 2021/03.

2. (Verfassungs-)rechtlicher Hintergrund

Das vorliegende Konzept für ein Überwachungsbarometer knüpft an die bisherigen Überlegungen an und entwickelt sie konsequent weiter in ein theoretisch und empirisch unterlegtes Modell, das den verfassungsrechtlichen Topos der Überwachungsgesamtrechnung operationalisiert und ein methodisches Konzept zur Erfassung und Quantifizierung der **realen Überwachungslast** präsentiert, der die Bürgerinnen und Bürger ausgesetzt sind. Zur Erfassung eines realistischen Abbildes der Überwachungssituation und ihrer verfassungsrechtlichen Einordnung wäre es freilich nicht hinreichend, Zugriffsnormen und Anwendungszahlen rein quantitativ zu erfassen. Überwachungsmaßnahmen und Zugriffe auf datenförmig hinterlegte Informationen müssen jeweils 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.

Der Ansatz einer sachlichen Gewichtung der Intensität von Grundrechtseingriffen ergibt sich bereits aus der Rechtsprechung des Bundesverfassungsgerichts. Das Gericht hat eine differenzierte Kasuistik entwickelt und qualifiziert Eingriffe beispielsweise als nur „gering“[10] oder „geringfügig“[11] am einen sowie „tiefgreifend“[12] oder „besonders stark“[13] etc. am anderen Ende einer fiktiven Skala.[14] Maßnahmen, die sich eher im mittleren Bereich dieser Skala einreihen, wurden von dem Gericht etwa als „von erheblichem Gewicht“ oder „empfindlich“[15] bezeichnet.[16] Diese dem Grunde nach qualitative Bewertungstechnik adressiert die Perspektive der betroffenen Grundrechtsträger und lässt damit zugleich einen gewissen *quasi-empirischen Einschlag* erkennen. Die Bewertung hat unmittelbare Auswirkungen auf die verfassungsrechtlichen Anforderungen an die entsprechenden gesetzlichen Regelungen, indiziert aber *eo ipso* nicht deren verfassungsrechtliche Bedenklichkeit oder Unbedenklichkeit. Diesem Ansatz folgend ist auch das Überwachungsbarometer als Instrument zur objektiven Darstellung der Überwachungssituation zu verstehen. Es geht darum, die Überwachungslast messbar zu machen und die verschiedenen Überwachungsszenarien in Relation zueinander zu setzen.

Beispiele zur Qualifizierung von Eingriffen (BVerfG)

gering/ geringfügig	→	von erheblichem Gewicht/empfindlich	→	tiefgreifend/ besonders stark

Ziel ist es aufzuzeigen, wo reale Schwerpunkte der Überwachung liegen und wie diese sich insgesamt entwickelt. Steigt etwa die Überwachung bundesweit an und gibt es Unterschiede zwischen einzelnen Behördenzweigen oder Bundesländern? Ist die Überwachungslast in Bundesland A, in dem häufiger Telekommunikations-Verkehrsdaten oder Bestandsdaten im Zusammenhang mit der Nutzung von Telemedien abgefragt werden, eventuell höher als in Bundesland B, in dem häufiger die Quellen-TKÜ zum Einsatz kommt? Es sind solche und ähnliche Fragen, die mit dem Überwachungsbarometer beantwortet werden sollen. Es stellt ein empirisch unterlegtes Gerüst für die Beantwortung der sich anschließenden verfassungsrechtlichen Folgefragen zur Verfügung.

Hierfür ist eine **empirisch fundierte Operationalisierung** erforderlich, die die tatsächliche Überwachungslast, der die Bürgerinnen und Bürger aufgrund der verschiedenen Überwachungstatbestände in der täglichen behördlichen Routine bei Datenabfragen und -zugriffen ausgesetzt sind, ins Zentrum stellt. Denn neben der Beurteilung, ob ein bestehendes Gesetz oder eine neu geplante Erweiterung einer bestehenden Überwachungsmöglichkeit auf der abstrakten Rechtmäßigkeitsebene zulässig ist, müsste insbesondere auch ihr möglicher zusätzlicher Beitrag zu der Überwachungsgesamtrechnung ermittelt werden. Dabei teilen wir grundsätzlich die in der bisherigen Diskussion verbreitete Skepsis[17] 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. Es soll den synchronen und diachronen Vergleich unterschiedlicher Überwachungsniveaus ermöglichen. Zudem soll 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 Hinsicht – etwa bezogen auf eine potenziell hohe oder zu hohe Anwendungshäufigkeit bestimmter Maßnahmen insgesamt oder auf die Un-/Verhältnismäßigkeit einer Vielzahl einzelner Maßnahmen in

10 Nach BVerfGE 120, 378 (403) etwa die automatisierte Kfz-Kennzeichenkontrolle, sofern sie auf einen Abgleich mit den Kennzeichen gestohlener Fahrzeuge beschränkt bleibt.
11 Strategische Briefkontrolle, BVerfGE 67, 157 (179); siehe auch VGH Mannheim, NVwZ-RR 2011, 231 (233) – Personenfeststellung.
12 Elektronische Aufenthaltsüberwachung (Fußfessel), BVerfG, 2 BvR 916/11, 2 BvR 636/12 v. 01.12.2020.
13 Kunstfreiheit – Fall „Esra“, BVerfG, 1 BvR 1783/05 v. 13.6.2007, NJW 2008, 39.
14 Hierzu *Bäcker* in Herdegen/Masing/Poscher/Gärditz, Handbuch Verfassungsrecht (2021), § 28 Rn. 89 ff., der in der Rechtsprechung des BVerfG vier Intensitätsstufen erkennen will.
15 Siehe Sondervotum von RiBVerfG Huber zu BVerfGE 142, 234 (267).
16 BVerfGE 150, 244 (283) – autom. Kennzeichenkotrolle; BVerfG, NVwZ 2007, 688 (691) – Videoüberwachung auf öffentlichen Plätzen.
17 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, 144 ff.

einem konkreten Einzelfall.[18] Eine übermäßige Überwachung wäre mit der Verfassungsidentität der Bundesrepublik unvereinbar.[19]

Insbesondere der behördliche Zugriff auf anlasslos gespeicherte Massendaten könnte den verfassungsrechtlichen ‚Spielraum' – unterhalb einer denkbaren Überwachungs-‚Obergrenze' – bereits weitgehend ausschöpfen. Als ein konkretes Beispiel einer ‚überschießenden' Überwachungslast wurde in der Literatur die Einführung der anlasslosen Vorratsdatenspeicherung von Fluggastdaten[20] diskutiert, von der im Jahr 2019 potenziell fast 250 Millionen Passagiere[21] an deutschen Verkehrsflughäfen betroffen waren.[22]

Zugleich ist zu berücksichtigen, 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 kann. In diesem Sinne hat sich die Verkehrsdatenabfrage als (strafrechtliche) Ermittlungsmaßnahme seit den 1990er Jahren zu einem viel genutzten funktionalen Äquivalent zur ‚klassischen' Telefonüberwachung entwickelt.[23] Das hängt zu einem Teil mit der Veränderung des Kommunikationsverhaltens und der Verlagerung des Telefonverkehrs in – vollverschlüsselte (end-to-end) – internetbasierte Kanäle oder Messenger-Dienste (z.B. WhatsApp) zusammen; diese Entwicklung betrifft die präventiven Einsatzformen selbstredend in gleicher Weise. Das Fallaufkommen hat sich aber auch deshalb verändert, weil in vielen Fällen von vornherein kein kriminalistischer Bedarf an dem im Vergleich zu der Abfrage der Metadaten bei den Providern deutlich schwerwiegenderen und auch personalintensiveren Abhören und Aufzeichnen von Gesprächsinhalten gesehen wird; in früherer Zeit wurden die Verkehrsdaten im Zuge der Überwachung der Telefongespräche quasi ‚mit' erhoben.[24] Umgekehrt kann die Entwicklung und Nutzung neuer technologischer Möglichkeiten die (verfassungs-)rechtliche Bewertung einer bis dato als weitgehend unbedenklich bewerteten Maßnahme unter Umständen signifikant verändern. 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.[25] Solche Entwicklungen werden bei dem längerfristigen Monitoring der Überwachungspraxis erkennbar und müssen dann entsprechend in die (rechts-)politische Bewertung der Ergebnisse einfließen.

Daher bliebe etwa die Überwachung der Flugpassagiere mit ihrem Höchstwert aus 2019 eine prägende Komponente der Überwachungsgesamtlast in jenem Jahr, auch wenn anhängige Klagen gegen die zugrundeliegende sog. PNR-Richtlinie der EU[26] am Ende beim Europäischen Gerichtshof erfolgreich sein würden. Ein gerichtlich verfügtes Ende der aktuellen Praxis würde die aktuelle Überwachungslast nicht unwesentlich reduzieren.

Um die Dynamik der Entwicklung sowohl bei der Anwendung bestehender wie auch bei der Schaffung neuer bzw. erweiterter Überwachungstatbestände[27] zu erkennen und zu interpretieren, ist vorgesehen, 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.

Das Barometer ist zunächst auf Überwachungsmaßnahmen nationaler Behörden innerhalb Deutschlands beschränkt. Nicht berücksichtigt werden daher u.a.: Überwachungsmaßnahmen deutscher Behörden im oder ins[28] Ausland, die Übermittlung von Daten im Rahmen der internationalen Rechts- oder Amtshilfe ins Ausland sowie verdeckte Aktivitäten ausländischer Nachrichtendienste im Inland; hierzu fehlt aktuell schlicht die systematische statistische Erfassung.[29] Soweit Überwachungsmaßnahmen im Rahmen der straf- und sicherheitsrechtlichen Zusammenarbeit in der EU[30] nach deutschem Recht angeordnet und durchgeführt werden,[31] sollten diese in der Gesamtheit der inländischen Fälle wohl mit erfasst sein; dies ist im Einzelfall noch zu prüfen.[32]

An der Schnittstelle der Überwachungen mit In- und/oder Auslandsbezug stehen im Übrigen weitere Phänomene der automatisierten Auswertung von Massendaten. Neben der bereits erwähnten PNR-Datenspeicherung im Kontext nationaler und internationaler Flugreisen[33] existieren noch erheblich umfangreichere Überwachungstechniken, wie namentlich

18 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).

19 Grundlegend BVerfGE 125, 260 (324) – Vorratsdatenspeicherung. Siehe auch BVerfG, 2 BvR 916/11, 2 BvR 636/12 Rn. 210 – Fußfessel.

20 § 2 FlugDaG.

21 Siehe unten Fn. 71; im Jahr 2020 dürfte diese Zahl infolge der Corona-Pandemie drastisch zurückgegangen sein.

22 Siehe zur Gewichtung dieser auf der Grundlage von § 2 FlugDaG durchgeführten Überwachung unten 3.3.2.3. *(Tabellen 04/04a).*

23 Siehe unten 4.2., *Schaubild 10.*

24 Vgl. *Albrecht/Kilchling*, Die Überwachung von Telekommunikations-Verkehrsdaten, MPG-Jahrbuch 2008 (m.w.N.); *Albrecht et al.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? (2011).

25 Zur Bedeutung technologieneutraler Normen Adensamer, [österr.] Handbuch Überwachung (2020), 45.

26 Richtlinie (EU) 2016/681 vom 27.04.2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119/132.

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

28 Z.B. die TK-Auslandskopfüberwachung; hierzu ausführl. *Kilchling*, Die Neuregelung zur Auslandskopfüberwachung gemäß § 4 TKÜV auf dem verfassungsrechtlichen Prüfstand, 2006.

29 Dasselbe gilt für Abfragen ausländischer Behörden zu inländischen Kunden und deren Daten direkt bei privaten Providern.

30 Hierzu zählen insbes. Anordnungen auf der Basis einer europäischen Ermittlungsanordnung gem. EU-Richtlinie 2014/41/EU, ABl. L 130/1, in Deutschland umgesetzt in den §§ 91a-91j IRG. Ihre Bedeutung geht über die Strafverfolgung hinaus und kann auch das Polizeirecht betreffen; vgl. *Aden* in Lisken/Denninger, Handbuch des Polizeirechts, 2018, Rn. 256 ff.

31 Ausführlich zu dem komplexen Zusammenspiel von nationalen und europarechtlichen Rechtsgrundlagen für die Datenübermittlung am Beispiel der strafprozessualen TKÜ *Sieber* in FS Albrecht, 2021, 53 ff.

32 Soweit die Datenweitergabe normativ zulässig ist, fließt dies als potenzielles Schwereindiz stets in die Bestimmung der Eingriffsintensität der jeweiligen Maßnahme mit ein (siehe dazu unten 3.4.2.).

33 Die Daten zu Flugreisenden auf Flügen innerhalb der EU werden sogar doppelt gespeichert: im Abflug- und im Zielland.

die strategische Fernmeldeüberwachung[34] bei den Telekommunikations- und E-Mail-Verkehren und der Auslands-Auslands-Aufklärung[35], deren Volumen sich in einer geschätzten Größenordnung von mehreren hundert Millionen Überwachungsvorgängen pro Tag bewegen dürfte.[36] Diese Volumina stellen eine besondere Herausforderung für das Überwachungsbarometer dar, sowohl konzeptionell[37] als auch im Hinblick auf den nur schwerlich realisierbaren Zugang zu belastbaren Daten zu den geheimdienstlichen Aktivitäten. Aus diesen Gründen wird dieser spezifische Bereich, obwohl es sich nach der Bewertung durch das Bundesverfassungsgericht rechtlich um inländische Vorgänge handelt, in den ersten Projektphasen nicht einbezogen.

Das Konzept ist im Übrigen so angelegt, dass es inhaltlich erweitert werden kann. Perspektivisch könnte insbesondere ein EU-weites Anschlussprojekt entwickelt werden.

34 Siehe zur strategischen Überwachung Inland-Ausland gem. § 5 G-10 BVerfGE 100, 313 ff.; BVerwGE 149, 359; BVerwG, GSZ 2018, 203 mit Anm. *Gärditz*; erläuternd *Schantz*, NVwZ 2015, 873; *Bäcker*, K & R 2014, 556; *Marxsen*, DÖV 2018, 218.

35 Zur strategischen Überwachung Ausland-Ausland gem. §§ 6, 7, 13 ff., 19 ff. BNDG, BVErfG, NJW 2020, S. 2235 ff.; BVerwG, GSZ 2017, S. 28 u. Nichtannahmebeschluss des BVerfG (3. Kammer) vom 26.04.2017 – 1 BvR 456/17, BeckRS 2017, 111767. Erläuternd auch *Huber*, NVwZ-Beilage 2020, S. 3 ff.; *Marxsen*, DÖV 2018, 218 (222 ff.).

36 Vgl. z.B. *Biermann*, BND speichert 220 Millionen Telefondaten – jeden Tag, Zeit online v. 30.01.2015.

37 Eine Ausrichtung der Kalibrierung an solchen Maßstäben würde die überwiegende Mehrzahl der Überwachungssachverhalte a priori als marginal erscheinen lassen.

3. Methodisches Konzept

Die Entwicklung des hier vorgestellten Überwachungsbarometers basiert auf einem sechsstufigen Konzept:

→ Im ersten Schritt müssen die in dem Barometer zu berücksichtigenden Datensammlungen identifiziert werden (→ 3.1.).

→ Im zweiten wird analysiert, welche Sicherheitsbehörden auf Basis welcher rechtlicher Grundlagen Zugriff auf diese Daten haben und unter welchen Bedingungen der Zugriff möglich ist (→ 3.2.).

→ Im Anschluss an die Ermittlung der rechtlichen Zugriffspfade geht es im dritten Schritt darum, für jeden der ausgewählten Zugriffssachverhalte entsprechend spezifische Zugriffszahlen zu bekommen (→ 3.3.).

→ In einem vierten Schritt sind die Zugriffe dann nach verfassungsrechtlichen Kriterien zu gewichten (→ 3.4.).

→ So bewertet, lässt sich dann für die einzelnen Zugriffspfade aus den quantitativen Zugriffszahlen und dem qualitativen Intensitätswert in einem fünften Schritt ein Überwachungsindexwert berechnen (→ 3.5.).

→ Die Ergebnisse zu den einzelnen Zugriffspfaden lassen sich dann in Form eines Barometers aggregieren (→ 3.6.).

3.1. Identifikation der potenziell relevanten Überwachungsszenarien

Gegenstand eines aussagekräftigen Überwachungsbarometers sollten grundsätzlich alle staatlichen Überwachungsmaßnahmen mit sicherheitsrechtlicher Relevanz sein, unabhängig von ihrer konkreten Zielsetzung. Dies umfasst repressive Maßnahmen zur Strafverfolgung ebenso wie präventiv orientierte Interventionen durch Bundes- und Landespolizeibehörden oder andere Behörden, Maßnahmen zur Erfüllung verschiedener staatlicher Aufsichts- oder sonstiger Verwaltungsaufgaben einschließlich der Zoll- und Finanzverwaltung sowie die in aller Regel verdeckten Überwachungsmaßnahmen der Nachrichtendienste. In jedem der hier nur exemplarisch genannten Bereiche kommt es regelmäßig zu der Erhebung von bzw. dem **Zugriff auf** bereits vorhandene **staatliche – d.h. staatlich generierte und/oder administrierte – und private Datensammlungen.**

Die besonders praxisrelevanten Überwachungsszenarien wurden in der ersten Projektphase gesammelt und im Hinblick auf die Art der jeweiligen Daten systematisiert (siehe die detaillierte Übersicht Tabelle 01 im Anhang). Die Auflistung gibt einen Überblick über den aktuellen Status quo der rechtlich vorgesehenen Überwachungsmaßnahmen in Deutschland. Eine solche umfassende Bestandsaufnahme der Überwachungs-‚Landschaft' hat es in Deutschland bislang nicht gegeben.[38] Allerdings konnte im Rahmen der Pilotstudie zunächst nur eine begrenzte Auswahl exemplarisch berücksichtigt werden; dabei wurde der Schwerpunkt auf **anlasslos erhobene und gespeicherte Massendaten** sowie sicherheitsbehördliche Datenerhebungen gelegt, die jede und jeden betreffen können und zu denen Zahlen vorliegen. Im weiteren Verlauf soll die Liste dann auch den inhaltlichen Rahmen für die sukzessive Erweiterung der in das periodische Überwachungsbarometer einzubeziehenden Sachverhalte vorgeben. 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 und administrierten – die durch unmittelbare staatliche Eingriffe (auf gesetzlicher, ggf. auch richterlicher Grundlage) ad hoc und selbst generierten Datenbestände quantitativ inzwischen deutlich übersteigen (vgl. Tabelle 01 – Spalte 3[39]).

38 In Ansätzen vergleichbar ist allenfalls das österreichische HEAT-Projekt (vgl. *Tschohl* et al., aaO.) mit dem daraus hervorgegangenen [österreichischen] Handbuch Überwachung (vgl. *Adensamer*, aaO.).

39 Lediglich in den unter Nr. 3, 4, 5, 9d bis 9h und 10a/b aufgelisteten Fällen werden Daten direkt durch Behörden erhoben. In allen anderen Konstellationen erfolgt die Informationsgewinnung durch Abfrage von anlasslos von/bei Dritten angelegten und gespeicherten Datenbeständen bzw. den Zugriff darauf.

Im Hinblick auf die zunehmende Dominanz des privaten Datenmanagements ist zunächst eine sachliche Grenzziehung erforderlich. Im Hinblick auf den Gegenstand des Barometers ist der Fokus auf die **wesentlichen staatlichen Zugriffsrechte** auf derartige Datenbestände – einschließlich der mitunter weitreichenden pro-aktiven Auskunfts- und Meldepflichten – gerichtet. 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[40] –, 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 Sammlung der potenziell untersuchungsrelevanten Überwachungssachverhalte umfasst die folgenden Kategorien:

- → Telekommunikationsdaten: Bestands-, Verkehrs-, offene und verschlüsselte Inhaltsdaten (Nr. 1 bis 4);
- → Computerdaten (Nr. 5);
- → Daten im Zusammenhang mit der Nutzung von Telemediendiensten (Nr. 6);
- → Finanztransaktions-, Konto- und weitere Bankdaten (Nr. 7, 8);
- → Mobilitätsdaten (Nr. 9);
- → Daten aus dem privaten Lebensbereich (Wohnraumüberwachung: Nr. 10a/b, Zugriff auf smarte Haushaltsgeräte: Nr. 10c[41]); nach Inkrafttreten des § 3a NetzDG wird künftig wohl auch die Überwachung des privaten Kommunikationsverhaltens in sozialen Netzwerken in diesen sachlichen Kontext einzuordnen sein (Nr. 10d);
- → sonstige private Daten, die in Mobilgeräten lokal, auf Firmenservern oder in Cloudspeichern abgelegt sind, oder technische Daten, die bei IT-Dienstleistungen aller Art automatisch anfallen;[42] soweit diese nicht unter den besonderen Schutz der Art. 10 oder 13 GG fallen, können sie, jedenfalls im repressiven[43] Anwendungsspektrum, grundsätzlich auf der Grundlage allgemeiner Zugriffsnormen oder Generalklauseln beschlagnahmt werden (Nr. 11); ein weiterer potenziell relevanter Sachverhalt ist der Zugriff auf Meldedaten im Kontext der automatisierten Passbildabfrage (Nr. 12) 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 Auflistung enthält schließlich die folgende weitere Kategorie:

- → einmalige, temporäre oder sondergesetzliche Datenzugriffe mit Streuwirkung oder sonst erheblicher Eingriffsintensität (Nr. 13).

Als aktuelles Beispiel wird unter dieser Kategorie auf das ZensusvorbereitungsG 2022 hingewiesen (Nr. 13a). Bekanntlich hat die Dogmatik zum Grundrecht auf informationelle Selbstbestimmung ihren Ursprung in dem sog. Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983.[44] Hierbei handelt es sich zwar um eine einmalige Datenerhebung;[45] im Hinblick auf die längerfristige Perspektive des Überwachungsbarometers erscheint es jedoch aus grundsätzlichen konzeptionellen Überlegungen heraus 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. bei politischen Großereignissen (z.B. G20-Gipfeltreffen), einer Fußball-WM, bei Terrorlagen, großräumigen Ermittlungsmaßnahmen oder Vorfeld- und Strukturermittlungen (z.B. im OK- oder Clan-Milieu) etc. Im Rückblick könnten eventuell auch gewisse Zugriffe von Sicherheits- und anderen Behörden (Polizei, Staatanwaltschaft, Ordnungsbehörden, Nachrichtendienste) auf Daten, die zunächst temporär und eigentlich zweckgebunden im Rahmen der aktuellen COVID-Zugangs- und Aufenthaltskontrollen erhoben werden (vgl. Nr. 13b), unter dieser Rubrik einsortiert werden. Ereignisse wie die hier beispielhaft genannten haben grundsätzlich das Potenzial, die Überwachungslast in einer bestimmten Periode (Referenzjahr) temporär zu erhöhen. Im Zeitvergleich können sie auch ein bedeutsamer Erklärungs- und Abwägungsfaktor für auffällige kurzfristige Veränderungen in einem oder mehreren der im Überwachungsbarometer beobachteten Sektoren sein, auch und gerade im Hinblick auf die verfassungsrechtliche und politische Diskussion zur Überwachungsgesamtrechnung.

40 Vgl. Art. 3 der NADA-Standards für Meldepflichten.

41 Im präventiven und nachrichtendienstlichen Anwendungsspektrum str.; vgl. *Löffelmann*, GSZ 2020.

42 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 (Nicht-Annahmebeschluss d. 2. Kammer des Zweiten Senats) v. 17.2.2009.

43 Auch hierzu *Löffelmann*, GSZ 2020.

44 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 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.

45 Ein Zensus ist zwar jeweils ein Einmalereignis. Zu beachten ist freilich, dass in diesem Bereich unterschiedliche gesetzliche Grundlagen zur Datenverarbeitung existieren; siehe das ergänzende Zensusgesetz 2022 (ZensG 2022 v. 26.11.2019, BGBl. I S. 1851, geänd. durch Gesetz v. 3.12.2020, BGBl. I S. 2675) und das Registerzensuserprobungsgesetz (RegZensErpG v. 9.6.2021, BGBl. I S. 1649). Auf EU-Ebene gibt es im Übrigen Bestrebungen, den bisherigen Zehnjahresturnus durch eine jährliche, ggf. separate Erhebung zu ergänzen oder zu ersetzen; hierzu ausführl. *Körner/Krause/Ramsauer*, WISTA, Sonderheft Zensus 2021 (2019), S. 76 f. sowie die Stellungnahme des Präsidenten des Statistischen Bundesamtes Thiel bei der öffentlichen Anhörung des Bundestagsausschusses für Inneres und Heimat zum RegZensErpG vom 3. Mai 2021 zu BT-Drucks. 19/27425, der für die Zukunft sogar einen jährlichen und für bestimmte Daten noch häufigeren Turnus erwartet, vgl. Ausschussdrucks. 19(4)819 A, S. 2.

Zunächst nicht einbezogen wurden in dem aktuellen explorativen Stadium 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, wie sie ursprünglich Anlass zur Entwicklung des Topos der Überwachungsgesamtrechnung gab. Dennoch tragen auch sie zum Gesamtüberwachungsstatus bei. Denn mit Aufnahme einer Person in eine oder mehrere dieser Dateien – beispielsweise in die bundesweite Datei „Gewalttäter Sport" – erhöht sich das individuelle Risiko dieser Person, zusätzlichen Kontroll- und/oder weitergehenden Folgemaßnahmen unterzogen zu werden. In einer späteren Ausbaustufe des Barometers sollten daher jedenfalls diejenigen anlassbezogenen Datenbanken der Sicherheitsbehörden mit besonderer grundrechtlicher Relevanz Berücksichtigung finden. Um einen Eindruck davon zu gewinnen, welche besonderen Fragen sich hinsichtlich entsprechender Dateien stellen, soll in einer späteren Projektphase zunächst die Antiterror-Datei[46] exemplarisch in die Entwicklung des finalen Überwachungsbarometers einbezogen werden.

Grundsätzlich ausgeklammert bleibt ferner die *Videoüberwachung*. Sie ist häufig privat administriert und scheidet daher ebenfalls aus. Soweit Videoüberwachung im öffentlichen Raum stattfindet, wird sie zumeist 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.[47] Eine umfangreiche Datensammlung wie jene, die im Rahmen dieses Projekts untersucht werden, existiert daher nicht. Die reine Erhebung der Bilder dürfte überdies, solange es nicht zu einer Weiterverarbeitung kommt, nur einen geringen Grundrechtseingriff darstellen. Maßgeblich ist hier noch die sog. Sphärentheorie des Bundesverfassungsgerichts[48], nach welcher nur ein (leicht zu rechtfertigender) Eingriff in die Sozialsphäre vorliegt. Im Übrigen werden einzelne Zugriffe staatlicher Akteure auf temporär gespeicherte Bilddateien gegebenenfalls unter anderen Rubriken (vgl. Nr. 5, 10b u. 11) miterfasst.

3.2. Analyse der jeweils einschlägigen Zugriffsvoraussetzungen

Nach der Identifizierung der potenziell relevanten Daten(-bestände) müssen die rechtlichen Zugriffspfade analysiert werden. Hierfür ist die Auswertung der relevanten Rechtsgrundlagen erforderlich, die zunächst lediglich summarisch erfasst wurden (vgl. Anhang, *Tabelle 01*). Auf diese Weise können die Zugriffe rechtlich rekonstruiert und differenziert erfasst werden; dies ist eine wesentliche Voraussetzung für ihre korrekte rechtliche Gewichtung.

Beispielhaft wird in den *Schaubildern 01* und *02* die detaillierte Zugriffsstruktur für zwei der exemplarisch bearbeiteten Überwachungssachverhalte grafisch dargestellt.

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

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

48 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.

Schaubild 01 | Übersicht über die rechtlichen Zugriffsmöglichkeiten auf Telekommunikationsdaten

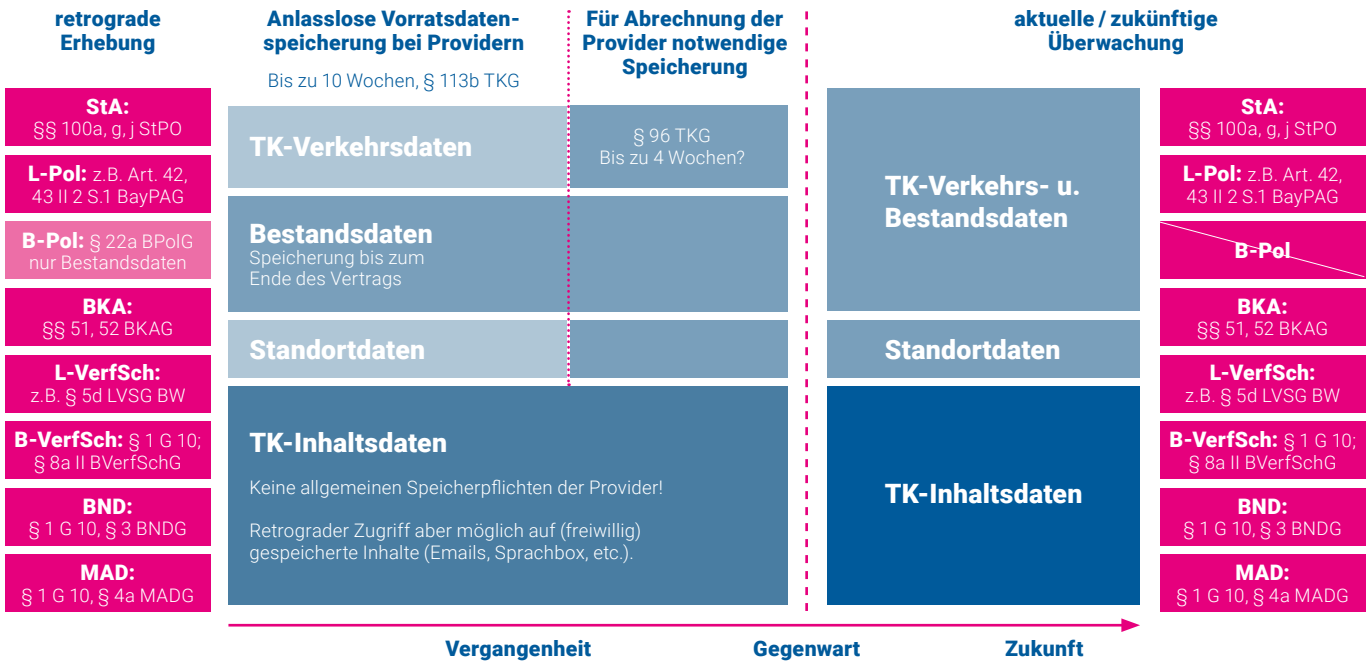
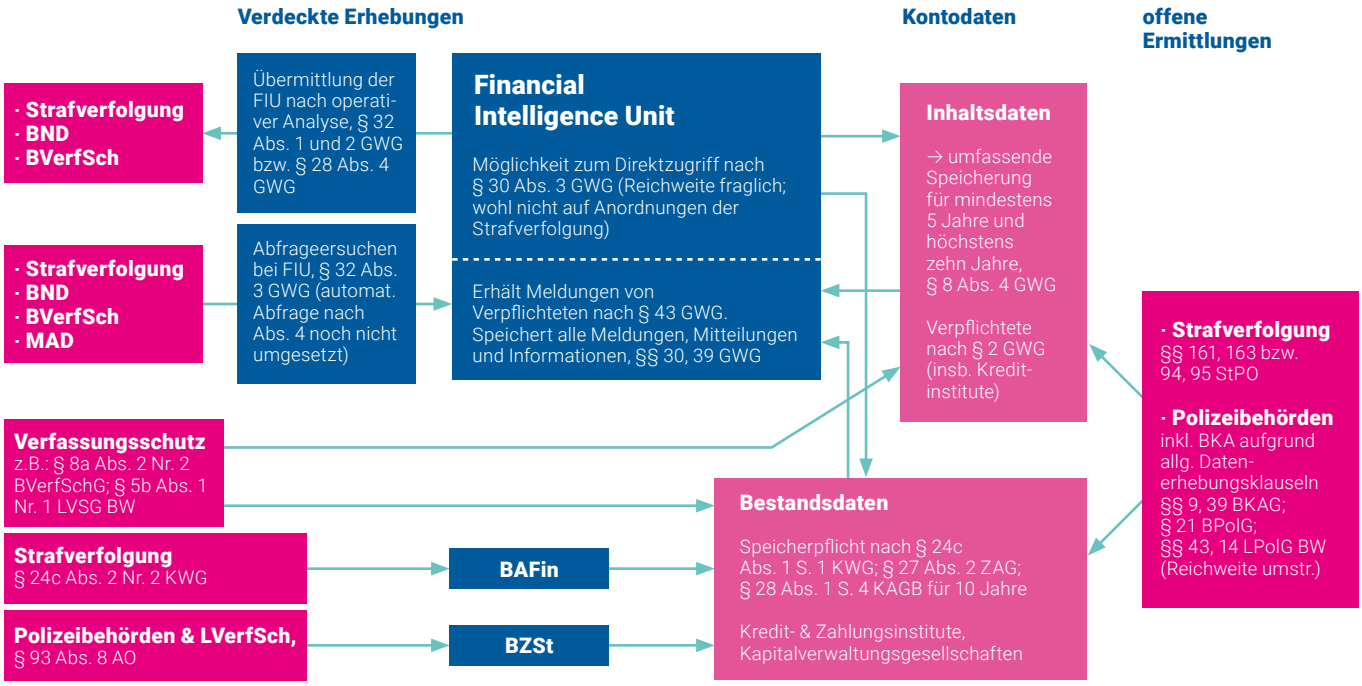


Schaubild 02 | Übersicht über die Zugriffsmöglichkeiten auf Kontodaten



Gleichsam als Nebenprodukt des Projekts entsteht so eine – regelmäßig aktualisierte – kartographische Übersicht über die sicherheitsbehördlichen Zugriffsrechte auf die untersuchten Massendatenbestände, die aufgrund ihrer oft beklagten normativen Komplexität und kompetenziellen Unübersichtlichkeit auch für Experten kaum mehr überschaubar sind.[49] In einer Ausbauphase ließen sich die Karten noch weiter systematisieren und analytisch aufbereiten. Den Bürgerinnen und Bürgern wäre es so erstmals möglich, auf einen Blick zu sehen, welche Sicherheitsbehörden unter welchen Voraussetzungen Zugriff auf etwa ihre Finanz- oder Telekommunikationsdaten haben. Wissenschaftlich ließe sich die Kartierung der Zugriffsvoraussetzungen nutzen, um ein System allgemeiner dogmatischer Strukturen des Sicherheitsrechts zu entwickeln und zu erproben.

3.3. Entwicklung des Barometers und seiner methodischen Grundlagen

Kernstück des Projekts ist, wie bereits ausgeführt, die Entwicklung eines theoretisch und empirisch unterlegten Modells zur Erfassung der realen Überwachungslast der Bürgerinnen und Bürger in Deutschland. Ein solches Modell muss, wie erwähnt, auf zwei Komponenten gestützt sein. Dabei ist die möglichst systematische Erfassung und analytische Aufbereitung der verfügbaren Daten zur Häufigkeit der relevanten Maßnahmen nur eine, wenn auch wesentliche Komponente. Prinzipiell anders als beispielsweise im Fall der sog. Gefangenenrate, dem international anerkannten Vergleichsmaßstab zur Messung der Punitivität von Gesellschaften,[50] unterscheiden sich die möglichen Überwachungssachverhalte qualitativ im Hinblick auf ihre Intensität grundlegend. Um die Überwachungslast eines Landes zu berechnen, ist es daher nicht hinreichend, ausschließlich auf die Quantität der durchgeführten Überwachungsmaßnahmen abzustellen – ebenso wenig zielführend wäre umgekehrt die isolierte Bewertung der abstrakten Gesetzeslage,[51] obgleich manche Beiträge diesen Punkt einseitig in den Vordergrund rücken.[52] Die aus den konkreten gesetzlichen Regelungen ableitbaren Belastungen fließen daher im zweiten Schritt als qualitatives Element in die Bewertung mit ein. Sie bilden den Referenzrahmen für die (verfassungs-)rechtliche Gewichtung der zuvor erhobenen statistischen Häufigkeitswerte der jeweiligen Maßnahmen. Dieses zweistufige Konzept ermöglicht die Generierung eines **evidenzbasierten Abbildes der Überwachungslast**, das die relevanten quantitativen und qualitativen Aspekte des staatlichen Überwachungsgeschehens gleichermaßen berücksichtigt.

Das vorgeschlagene Modell ist nicht statisch, sondern flexibel adaptierbar und damit anpassbar an den jeweils aktuellen rechtlichen Status Quo in einem bestimmten Refe-

49 Mit ähnlichem Tenor z.B. *Löffelmann* in der öffentlichen Anhörung des Bundestagsausschusses für Inneres und Heimat vom 18. Februar 2021 zu BT-Drs. 19/23695, der die Regelungen in der Gesamtschau als inkohärent, unübersichtlich, teilweise widersprüchlich und redundant und insgesamt impraktikabel charakterisiert; vgl. Ausschussdrucks. 19(4)732 D, S. 5.

50 Vgl. dazu *Dünkel/Geng*, Die Entwicklung von Gefangenenraten im nationalen und internationalen Vergleich – Indikator für Punitivität? Developments of prison rates in comparative perspective – indicators for punitivity? Soziale Probleme, 24 (2013), 42.

51 So auch *Starnecker*, Videoüberwachung zur Risikovorsorge, 2016, S. 369; *Moser-Knierim*, Vorratsdatenspeicherung, 2014, S. 238; im Ansatz auch schon *Roßnagel/Moser-Knierim/Schweda*, Interessenausgleich im Rahmen der Vorratsdatenspeicherung, 2013, S. 178; *Bieker/Bremert/Hagendorff* in *Roßnagel/Friedewald/ Hansen* (Hrsg.), Fortentwicklung des Datenschutzes, 2018, S. 139 (145).

52 Etwa *Roßnagel* in Beck'scher TKG Kommentar, § 113a Rn. 56 ff.; *Roßnagel* NJW 2010, S. 1238 (1240); für Österreich *Tschohl et al.*, HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze, 2016, https://epicenter.works/sites/default/files/heat_v1.2.pdf [letzter Zugriff am 10.12.2021].

renzzeitraum – Kalenderjahr, regelmäßiger Stichtag (z.B. 31. Dezember) etc. Damit ist es dazu geeignet, die häufigen normativen Veränderungen und Weiterentwicklungen, wie sie gerade im Bereich des Sicherheitsrechts zu verzeichnen sind, aufzunehmen. Denn bewertet wird nicht nur die Überwachungslast als Ganzes, sondern spezifiziert nach allen wichtigen Überwachungsszenarien (repräsentiert durch bestimmte Datenarten) sowie allen wesentlichen Ebenen (Bund und Länder) und Akteuren (Polizei, Strafverfolgung, Nachrichtendienste, Aufsichts- oder sonstige Verwaltungsbehörden). Durch die separate, sektorale Erhebung wird die Entwicklung im Bereich der Überwachung in ihrer Gesamtheit transparent. Darüber hinaus werden auch Unterschiede erkennbar. Auf dieser Basis lassen sich beispielsweise mögliche kritische Überwachungslasten in bestimmten einzelnen Sektoren identifizieren und lokalisieren. Diese können dann ein deutlicher, nicht nur abstrakt-rechtlicher, sondern empirisch fundierter Hinweis darauf sein, ob bzw. wo das Potenzial für häufigere Überwachungsmaßnahmen in einem bestimmten Bereich oder für die rechtliche Erweiterung bestehender bzw. Schaffung neuer Überwachungstatbestände oder -instrumente (weitgehend) ausgeschöpft scheint.

3.3.1. Methodische Vorbilder

Die Idee, gesellschaftliche Phänomene zu indexieren, ist nicht neu. Es existiert eine Vielzahl von wissenschaftlich betreuten Barometern, die in verschiedenen Lebensbereichen zum Einsatz kommen. In den Wirtschafts- und Finanzwissenschaften – siehe z.B. den Verbraucherpreisindex oder den sog. Gini-Index zur Erfassung der weltweiten Einkommens- und Vermögensverteilung – wie auch im (gesellschafts-)politischen Bereich – für den stellvertretend der Index der Vereinten Nationen zur menschlichen Entwicklung oder der Korruptionswahrnehmungsindex der Organisation „Transparency International" zu nennen wären – haben solche Bewertungsmodelle große Bedeutung. Ihre Zielsetzung ist es, komplexe Phänomene greifbar zu machen und ihre Entwicklung im Längs- und Querschnitt zu verfolgen.

Das neue Überwachungsbarometer hat eine methodische Verwandtschaft mit dem sog. Index der Pressefreiheit, der von der Organisation „Reporter ohne Grenzen" herausgegeben wird. Dieser Index versucht, ein konkretes Ausmaß von Freiheit unter bestimmten Gesichtspunkten in konkreten Zahlenwerten zu erfassen,[53] und weist damit auch eine gewisse inhaltliche Nähe zum Überwachungsbarometer auf. Zur Generierung des Index werden zwei Werte berechnet, die sich aus unterschiedlichen Variablen zusammensetzen, die ihrerseits unterschiedlich gewichtet werden. Der erste Wert (A) umfasst die sechs Komponenten Medienvielfalt (scorePlur), Unabhängigkeit der Medien (scoreInd), journalistisches Arbeitsumfeld und Selbstzensur (scoreEA), rechtliche Rahmenbedingungen (scoreCL), institutionelle Transparenz (scoreTra) sowie Produktionsinfrastruktur (scoreInf). Der zweite Wert (B) beinhaltet eine zusätzliche, siebte Komponente, die sich aus der Häufigkeit von Misshandlungen und Gewalt an Journalistinnen und Journalisten ergibt (scoreExa).[54] Als erfassungsrelevante Gewalttaten bzw. Misshandlungen werden politisch motivierte Morde, Inhaftierungen, Verschleppungen, Angriffe und Bedrohungen dieser Personen erfasst.[55] Die angewendeten Formeln ergeben jeweils einen Wert zwischen 0 und 100, wobei 0 das höchste Maß an Pressefreiheit darstellt. Für die Rangliste relevant ist jeweils der schlechtere der beiden errechneten Werte. Damit wird verhindert, dass Staaten, in denen es aufgrund absoluter Kontrolle der Medien mangels Notwendigkeit nicht zu Misshandlungen kommt, einen Vorteil erhalten.[56]

Die Werte der einzelnen Komponenten ergeben sich aus einem Fragebogen, der an professionelle Medienschaffende sowie Expertinnen und Experten aus den juristischen Berufen und der Soziologie in 180 verschiedenen Nationen verschickt und von „Reporter ohne Grenzen" ausgewertet wird.[57]

53 *Reporter ohne Grenzen*, Rangliste der Pressefreiheit 2020. Methodische Hinweise zur Erstellung, www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Ranglisten/Rangliste_2020/Methodik_Rangliste_der_Pressefreiheit_2020_-_RSF.pdf [letzter Zugriff am 10.12.2021].
54 Idem, S. 1.
55 *Sapienzynska/Lagos*, Int. J. of Communication 10 (2016), 549 (557).
56 Idem, S. 2.
57 *Reporter ohne Grenzen*, Rangliste der Pressefreiheit 2020: Fragebogen, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Ranglisten/Rangliste_2020/Fragebogen_Rangliste_der_Pressefreiheit_2020_-_RSF.pdf [letzter Zugriff am 10.12.2021].

Die Formel für den ersten Wert gewichtet die sechs Komponenten unterschiedlich, bevor diese addiert werden; sie lautet:[58]

Wert A (ohne Gewalt & Misshandlungen)
=
$$\frac{1}{3} * scorePlur + \frac{1}{6} * (scoreInd + scoreEA + scoreCL) + \frac{1}{12} * (scoreTra+scoreInf)$$

Bei dem zweiten Wert B wird, wie erwähnt, die weitere Variable „ScoreExa" mit einbezogen. Dieser Wert wird durch eine eigene Formel berechnet, welche verschiedene Gewaltvarianten berücksichtigt und diese wiederum einzeln gewichtet. Die Formel für diesen zweiten Wert lautet:[59]

Wert B (inkl. Gewalt & Misshandlungen)
=
$$\frac{1}{5} * scoreExa + \frac{4}{15} * scorePlur + \frac{2}{15} * (scoreInd + scoreEA + scoreCL) + \frac{1}{15} * (scoreTra + scoreInf)$$

58 *Reporter ohne Grenzen*, https://rsf.org/en/detailed-methodology [letzter Zugriff am 10.12.2021]; Sapienzynska/Lagos, Int. J. of Communication 10 (2016), 549 (557).
59 Idem.

Miteinbezogen werden hier – jeweils bezogen auf ein Jahr – die Anzahl an (politisch motivierten) Tötungen, Inhaftierungen, Verschleppungen, Vertreibungen ins Exil, Verhaftungen und physischen Attacken sowie Angriffen auf Medienhäuser bzw. deren Zensur.[60]

60 *Sapienzynska/Lagos*, Int. J. of Communication 10 (2016), 549.

Physische Attacken auf Journalistinnen und Journalisten haben auch in Deutschland, insbesondere im Rahmen von Demonstrationen, deutlich zugenommen. Dies hat dazu geführt, dass Deutschland im Rang um zwei Plätze abgesunken ist und nunmehr nur noch als „zufriedenstellend" bewertet wird.[61]

61 *Tagesschau*, 20.04.2021, www.tagesschau.de/inland/rog-pressefreiheit-deutschland-corona-101.html [letzter Zugriff am 10.12.2021].

Die Formel lautet zur Berechnung des „ScoreExa" lautet:

10 * log (90 * Mor + Coef fi * Emp + 10 * Enl + 5 * Med + 3 * Exi + Arr + Agr).[62]

62 *Sapienzynska/Lagos*, Int. J. of Communication 10 (2016), 549.

Die einzelnen Variablen stehen für die oben dargestellten Werte: *Mor* = Anzahl der (politisch motivierten) Tötungen an Journalisten; *Emp* = Anzahl der inhaftierten Journalisten; *Enl* = Anzahl der Verschleppungen; *Med* = Anzahl der Angriffe auf Medienhäuser/Zensur von Medienhäusern; Exi = Anzahl der ins Exil vertriebenen Journalisten; *Arr* = Anzahl der verhafteten Journalisten und *Ahr* = Anzahl der physischen Attacken auf Journalisten.[63]

63 Idem.

Die Anzahl der inhaftierten Journalisten *(Emp)* wird mit einem spezifischen Koeffizienten („Coef f_i") multipliziert, der die Dauer der Inhaftierung in Inhaftierungsjahren (i) darstellt.[64] Der Koeffizient ist nicht-linear konstruiert, sodass längere Haftdauern stärker ins Gewicht fallen als kürzere. Bei langen Haftzeiten von bis zu 10 Jahren oder darüber wird der Wert *Emp* sogar ähnlich stark gewichtet wie die Anzahl der ermordeten Journalisten *(Mor)*.

64 *Reporter ohne Grenzen*, https://rsf.org/en/detailed-methodology [letzter Zugriff am 10.12.2021].

Für Coef f_i gilt dabei folgende Abstufung[65]:

i	1-	2	3	4	5	6	7	8	9	10	10+
Coef f_i	10	20	35	60	80	85	87	88	89	89,5	$\lim_{\infty}$ *Coef fi* =90

65 Idem.

Der Index der Pressefreiheit verfolgt ausdrücklich nicht das Ziel, eine juristische Aussage über die Verfassungsmäßigkeit pressefreiheitsbeschränkender Maßnahmen in den bewerteten Staaten zu treffen. Vielmehr soll er – vergleichbar dem Human Development Index[66] – ausschließlich dazu dienen, den faktischen Status der Pressefreiheit unterschiedlicher Nationen zu vergleichen. Der Index bewertet den Stand lediglich mit den Noten „gut", „befriedigend", „problematisch", „schwierig" und „sehr ernst".[67] Er enthält keine Aussage zu dem (Mindest-)Maß an Pressefreiheit, welches (universell) verfassungsrechtlich (oder jedenfalls gesetzlich) gewährleistet sein sollte. Eine vergleichbare Funktion hat auch das Überwachungsbarometer. Dieses zielt in erster Linie darauf ab, die Überwachungslast nach objektiven Kriterien zu erheben, transparent zu machen und zu visualisieren. Es bekräftigt die Forderung des Bundesverfassungsgerichts nach einer transparenten Anwendungskultur der Überwachungsmaßnahmen. Insofern lässt sich das Überwachungsbarometer auch von der Zielrichtung her mit dem Index der Pressefreiheit vergleichen. Es ist ein Aufruf an die Politik, Gesellschaft, Wissenschaft und Rechtsprechung, sich mit dem aufgezeigten Maß der Überwachung auseinanderzusetzen.

66 Siehe zuletzt *United Nations Development Programme*, Human Development Report, 2020, http://hdr.undp.org/sites/default/files/hdr2020.pdf [letzter Zugriff am 10.12.2021].
67 *Reporter ohne Grenzen*, www.reporter-ohne-grenzen.de/rangliste/rangliste-2021 [letzter Zugriff am 10.12.2021].

3.3.2. Überwachungsbarometer

Für die Operationalisierung des Überwachungsbarometers sind neben den statistischen Zahlen zur Anwendungshäufigkeit als quantitativem Element insbesondere die Formeln zur Berechnung der einzelnen Freiheitsbelastungswerte und zur Relation zwischen der quantitativen und der qualitativen Dimension der Überwachungswirklichkeit bedeutsam.

3.3.2.1. Erfassung der Häufigkeit

Datenbasis für die Berechnung der Überwachungslast sind verlässliche Daten zur Häufigkeit der relevanten Maßnahmen. Diese sind möglichst systematisch zu erfassen und entsprechend der hier relevanten Fragestellung – ihrem Beitrag zu der realen Überwachungslast – analytisch aufzubereiten. Von besonderer Bedeutung für die Realisierung des Projekts ist daher der Datenzugang.

Wichtigste externe Ressource des Barometers sind amtliche **statistische Erhebungen**. Diese existieren in einigen der relevanten Bereiche, sei es in öffentlich zugänglicher Form – z.B. die Jahresübersichten des Bundesamtes für Justiz zur Telekommunikationsüberwachung oder die Statistiken der Zentralstelle für Finanztransaktionsuntersuchungen[68] zur Geldwäschekontrolle –, sei es zum internen Gebrauch. Auch in Tätigkeitsberichten verschiedener Aufsichts- oder Regulierungsbehörden können verwertbare Informationen gefunden werden. Von hohem Nutzwert können darüber hinaus auch parlamentarische Materialien (Berichte der G10-Kommission oder der Parlamentarischen Kontrollkommission sowie Antworten auf Große/Kleine Parlamentarische Anfragen) sein; in einzelnen Bereichen sind sie die einzige zugängliche (bzw. belastbare) Informationsquelle.[69] Nicht zuletzt kann schließlich der Informationsbestand des Statistischen Bundesamtes nutzbar gemacht werden. So kann beispielweise der Umfang der anlasslosen Vorratsdatenspeicherung von Fluggastdaten beim Bundeskriminalamt/Fluggastdatenzentralstelle gem. § 2 FlugDaG[70] aus der DESTATIS-Verkehrsleistungsstatistik abgeleitet werden.[71]

Alle Daten sind ausschließlich in aggregierter Form verfügbar, sodass für die spätere Bewertung der Maßnahmen a priori alle persönlichen Merkmale zu dem jeweils betroffenen Personenkreis sowie alle Informationen zu sonstigen individuellen Umständen der Überwachungsmaßnahmen fehlen. Methodologische Voraussetzung für die Feststellung solcher Informationen müsste eine einzelfallbezogene empirische Akten- bzw. Fallanalyse sein. Dies kann das Überwachungsbarometer schon aus forschungsökonomischen Gründen nicht leisten. Darüber hinaus ist es auch ein entscheidender Vorteil, dass das Überwachungsbarometer durch die Beschränkung auf aggregierte Daten datenschutzrechtlich unbedenklich ist. Dies gilt auch für statistische Daten, die – wie z.B. die auf der Basis von § 101b StPO erhobenen – vereinzelt Angaben zu einigen selektiven Erhebungsumständen beinhalten.

Aktuell am umfangreichsten sind – auch im Hinblick auf die retrospektive Bewertung der Entwicklung – die Informationen des Bundesamtes für Justiz zu repressiven TK-bezogenen Maßnahmen gemäß § 101b StPO; hier werden im kommenden Jahr auch erstmals Daten zur Anwendungshäufigkeit von Maßnahmen in Bezug auf die Nutzung von Telemedien nach dem neuen § 100k StPO verfügbar sein. Im Bereich der präventiven TK-bezogenen Maßnahmen gab es lange Zeit nahezu keine Informationen. Das ändert sich gerade. In Reaktion auf die zweite Entscheidung des Bundesverfassungsgerichts zur Bestandsdatenauskunft[72] haben nicht nur der Bundes-, sondern auch die Landesgesetzgeber zwischenzeitlich Berichtserstattungspflichten der Sicherheitsbehörden über die Anwendung ihrer Befugnisse in verschiedene Sicherheitsgesetze aufgenommen. Aktuell ist eine entsprechende Regelung auch in dem Entwurf für das BPolGModG 2021 vorgesehen.[73] Allerdings unterscheiden sich die Regelungen deutlich voneinander. Das betrifft die Art der berichtspflichtigen Maßnahmen ebenso wie den Turnus der Informationen: Mehrheitlich ist eine jährliche Veröffentlichung vorgesehen, einige Länder und der Bund visieren einen Zweijahresrhythmus an. In *Tabelle 02* sind die neuen Regelungen aufbereitet.

68 Financial Intellgence Unit (FIU); dies ist in Deutschland die Generalzolldirektion (Direktion X).

69 So ergeben sich einige Basiszahlen zu der Entwicklung der Kontoabfragen (siehe unten Tabellen/Schaubilder 10 ff.) aus BT-Drucks. 19/9177.

70 Siehe *Tabelle 01* im Anhang, Nr. 9j.

71 Dies betraf im Jahr 2019 potenziell 249.799.750 registrierte Passagiere (124.443.834 Ein- und 125.355.916 Aussteigende; Stat. Bundesamt, Verkehrsleistungsstatistik gewerblicher Luftverkehr, Tab. 2.1.1); siehe dazu auch unten *Tabelle 04*. Das übertrifft die Bevölkerungszahl um ein Vielfaches. 2020 ist diese Zahl aufgrund des durch die Corona-Pandemie bedingten Rückgangs der Flugbewegungen – jedenfalls temporär – signifikant zurückgegangen.

72 BVerfG NJW 2020, 2699 – Bestandsdatenauskunft II.

73 § 71 BPolG-E; siehe zu dem Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei ausführl. BT-Drucks. 19/26541.

Tab. 02 | Überblick zu den Transparenzregelungen in den Polizeigesetzen des Bundes und der Länder

Land	Normen	Erfasste Überwachungs-maßnahmen*	In Kraft seit	Angaben verfügbar ab/seit	Turnus
Baden-Württemberg	§ 90 PolG BW	2c, 3c, 4c, 6c, 9a, 10a, 10b	2020	2022	2 Jahre
Bayern	Art. 52 PAG	2c, 5c, 10b	2018	2019	jährlich
Berlin	§§ 24d, 25, 25a, 25b, ASOG Bln	1d, 3c, 9a, 9d	2021	2022	jährlich
Brandenburg	§§ 28a, 33a, 33b, 33c, 36a BbgPolG	1d, 2c, 3c, 9d, 10a, 10b	2006/2008		jährlich
Bremen	§ 150 BremPolG	1d, 2c, 10a, 10b	2020	*einmalige Evaluation bis 2023*	
Hamburg	§ 75 HmbgPolDVG	2c, 9d, 10a, 10b	2019	2022	jährlich
Hessen	§ 17a HSOG	10a, 10b	2018		jährlich
		2c			2 Jahre
Mecklenburg-Vorpommern	§ 48h SOG M-V	2c, 3c, 10a, 10b, 14b	2020	2021	jährlich
Niedersachsen	§ 37b NPOG	1d, 9d, 10a, 10b, 14b	2019		jährlich
Nordrhein-Westfalen	§ 34c PolG NRW	9h	2018		jährlich
	§ 68 PolG NRW	1d, 2c, 3c, 10a, 10b		teilw. 2017	2 Jahre
Rheinland-Pfalz	§ 49 POG	1d, 2c, 3c, 6c, 9a, 10a, 10b, 14b	2020	2022	jährlich
Saarland	§ 66 SPolDVG	1d, 2c, 9d, 10a,10b,	2020	2022	jährlich
Sachsen	§ 107 SächsPVDG	1d, 2c, 3c, 6a, 6c, 9a, 9d, 9h, 10a, 10b, 14b	2020	2021	jährlich
Sachsen-Anhalt	§ 31 SOG LSA	14b	2014		jährlich
Schleswig-Holstein	§§ 186b/c LVwG (i.d.F.d. LVwGPORÄndG 2021)	2c, 3c, 10a, 10b	2021	2022	jährlich
Thüringen	§ 36 Abs. 7 PAG	1d, 2c, 3c, 10a, 10b	2013		jährlich
Bund: BKA	§ 88 BKAG	1b, 2b, 3b, 4b, 5b, 6a, 9a, 9h, 10a, 10b, 14c	2018	2019	2 Jahre
Bund: BPol**	*§ 71 BPolG-E*	*(noch offen)*	-	-	*(2 Jahre)*

*) Nummerierung gem. Systematik der Überwachungsszenarien (siehe Tabelle 01 im Anhang);

**) Siehe BPolGModG-E 2021, BT-Drucks. 19/26541 (in der 19. WP nicht mehr verabschiedet).

Inhaltlich sind die neuen Berichtspflichten allerdings zumeist selektiv und lückenhaft. In einigen Ländern beschränken sie sich erkennbar auf den im Lichte der Rechtsprechung des Bundesverfassungsgerichts vermeintlich „notwendigsten" Umfang; mitunter mögen sie auch als politisches „Zugeständnis" für die Mehrheitsfindung in den Gesetzgebungsverfahren im Bereich des Sicherheitsrechts fungieren. So umfasst zum Beispiel die neu eingeführte Berichtspflicht gem. § 90 PolG BW zwar die Zugriffe auf die Telekommunikationsüberwachung (TK-Inhaltsdaten) sowie die Telekommunikations- bzw. Telemedien-Verkehrs- bzw. Nutzungsdaten, TK-Standortdaten und die Quellen-TKÜ, jedoch *nicht* die Zugriffe auf die Bestandsdaten in den beiden großen Bereichen Telekommunikations- und Telemedien-Nutzung. Gerade erst hat das Gericht noch einmal explizit auf die potenzielle Eingriffsschwere der bis in die jüngere Vergangenheit eher wenig beachteten Bestandsdatenabfragen hingewiesen.[74] Auch Informationen zu anderen wichtigen Maßnahmen mit potenzieller Überwachungsrelevanz wie beispielsweise die elektronische Aufenthaltsüberwachung, die automatisierte Kfz-Kennzeichenüberwachung und die Rasterfahndung werden ebenfalls nicht überall publik gemacht. Die Transparenzklauseln der meisten anderen Polizeigesetze einschließlich BKAG und BPolG-E sind ähnlich konstruiert. Am breitesten ist aktuell die Berichtspflicht in dem neuen sächsischen Polizeivollzugsdienstgesetz[75] angelegt, das am 1. Januar 2020 in Kraft getreten ist. Flächendeckende Daten aus allen Bundesländern werden erstmals 2022 vorliegen.

Einen neuen Weg geht, als bislang einziges Bundesland, Berlin mit dem Funkzellenabfragen-Transparenz-System (FTS). Über dieses Online-Portal können sich Bürgerinnen und Bürger über die Erfassung ihrer Mobilfunknummer im Rahmen von Funkzellenabfragen durch die Berliner Strafverfolgungsbehörden informieren lassen.[76] Das FTS ist allerdings als individuelles Auskunftssystem implementiert, in dessen Fokus selektive und personenbezogene Informationen stehen. Es wird zu prüfen sein, ob und inwieweit die Daten gegebenenfalls für das Überwachungsbarometer von Nutzen sein könnten.

Während noch vor wenigen Jahren wie erwähnt lediglich statistische Zahlen zu einer Auswahl an repressiven Maßnahmen nach der StPO verfügbar waren, werden in naher Zukunft flächendeckende Informationen zu einigen polizeirechtlichen Maßnahmen vorliegen, mit denen sich arbeiten lässt und die es ermöglichen, entsprechende Teilbarometer zu erstellen. Allerdings ignoriert die Beschränkung der Berichterstattungspflicht auf bestimmte heimliche Maßnahmen, dass auch offene Überwachungsmaßnahmen einen erheblichen Einfluss auf die Überwachungssituation ausüben. Um eine umfassende Gesamtbetrachtung vorzunehmen, müsste die Berichterstattungspflicht alle Überwachungsmaßnahmen berücksichtigen. Dazu gehören auch die Beschlagnahme und Durchsuchung, soweit im Rahmen dieser in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Hinzu kommt, dass nur auf der Grundlage einer transparenten und umfassenden Dokumentation aller relevanten Maßnahmen überhaupt erst der tatsächliche Anteil der verdeckten Maßnahmen im polizeilichen Handlungsspektrum insgesamt erkennbar wird.

Unterschiedlich sind im Übrigen dort, wo die polizeirechtlichen Berichterstattungspflichten inzwischen in Kraft getreten sind, die Unterrichtungsverfahren. Teilweise obliegt die Information der Öffentlichkeit den zuständigen Gremien der Landtage, teilweise den Landesregierungen oder Ministerien. Nicht immer sind die Zahlen über die Dokumentationssysteme der Landesparlamente oder zuständigen Ministerien auffindbar; teilweise bedarf es detektivischer Recherchearbeit, um die entsprechenden Dokumente aufzufinden.

Die genannten Informationsdefizite betreffen allerdings nicht nur die polizeirechtlichen, sondern auch die repressiven und sonstigen Überwachungssachverhalte. Als Ergänzung werden daher punktuell auch **eigene Datenrecherchen** empfehlenswert sein. Eine wichtige Quelle hierfür könnten, was zum Beispiel die polizeilichen Datenzugriffe anbetrifft, die elektronisch dokumentierten polizeilichen Einsatzprotokolle sein, wie sie in den Bundesländern heute flächendeckend implementiert sind. Allerdings haben die Landespolizeibehörden jeweils eigene IT-Anwendungen implementiert, die von unterschiedlichen Herstellern konfiguriert und betreut werden.[77] Wo keine expliziten Forschungsklauseln – z.B. §§ 476, 487 Abs. 4 StPO, § 57 PolG BW oder Art. 54 Abs. 4 BayPAG – existieren, wird man auf politische Unterstützung angewiesen sein.

Im Hinblick auf die Validierung der statistischen Daten ist im Übrigen stets auf die Vergleichbarkeit der zugrundeliegenden Erfassungskriterien zu achten. Für die statistische Erfassung existieren bislang keine verbindlichen einheitlichen Vorgaben, sodass zu überprüfen ist, ob die Erfassung durchweg maßnahmenbezogen erfolgt – etwa im Falle der Überwachung mehrerer Telefonanschlüsse oder Mobiltelefone ein und derselben Zielperson – oder ob gegebenenfalls eine personenbezogene Zählung vorliegt, auf deren Grundlage mehrere Maßnahmen gegen dieselbe Person in der Statistik lediglich mit dem Zählwert Eins erscheinen würden.[78] Die aktuelle Aufbauphase bei den landesrechtlichen Erfassungsroutinen zur Erfüllung der neuen polizeigesetzlichen Transparenzregeln könnte eine günstige Gelegenheit für eine länderübergreifende Vereinheitlichung sein (siehe hierzu auch unten *Abschnitt 6*).

74 Vgl. BVerfG, Pressemitteilung Nr. 39/2021 vom 19. Mai 2021 zu dem Nichtannahmebeschluss vom 19. April 2021 (1 BvR 1732/14).

75 Gesetz über die Aufgaben, Befugnisse, Datenverarbeitung und Organisation des Polizeivollzugsdienstes im Freistaat Sachsen (Sächsisches Polizeivollzugsdienstgesetz – SächsPVDG) vom 11. Mai 2019, SächsGVBl. S. 358.

76 Siehe https://fts.berlin.de/ [letzter Zugriff 10.12.2021]; https://netzpolitik.org/2021/transparenz-system-berlin-informiert-per-sms-ueber-funkzellenabfragen/ [letzter Zugriff 10.12.2021]; Justizsenator Behrendt spricht von „bürgerrechtlichem Neuland", www.heise.de/news/Berliner-Handybesitzer-erhalten-Informationen-zu-Funkzellenabfrage-6192058.html [letzter Zugriff 10.12.2021]; zu dem zugrundeliegenden Beschluss des Abgeordnetenhauses Drucksache 17/1975 vom 21.11.2014, Ziff. 3.

77 Ein nicht ganz vollständiger Überblick ist bei https://de.wikipedia.org/wiki/Polizei-IT-Anwendungen [letzter Zugriff 10.12.2021] zu finden.

78 Im Idealfall werden sowohl die Anzahl der Maßnahmen als auch die betroffenen Personen separat ausgewiesen; vgl. z.B. die jährlichen Berichte zu den Maßnahmen nach dem Terrorismusbekämpfungsgesetz, zuletzt BT-Drucks. 19/22388 v. 09.09.2020.

In einigen Bereichen werden belastbare statistische Zahlen – jedenfalls kurzfristig – nicht oder nur nach Überwindung erheblicher institutioneller Hürden zur Verfügung stehen. Dies gilt namentlich für die Aktivitäten der Geheimdienste. Freilich erscheint für die nähere Zukunft die weitere Ausdehnung der Berichtspflichten nicht unrealistisch, die dann auch Bereiche erschließen könnten, die für die Wissenschaft wie für die Öffentlichkeit bislang noch unzugänglich sind. Zwischenzeitlich könnten, soweit es mit den verfügbaren Ressourcen möglich ist, auf der Basis von **Schätzungen** einige der anfangs nicht vermeidbaren Datenlücken zumindest partiell überbrückt werden. Einige Informationen hierzu könnte eine Analyse der Zugriffe auf **Daten der großen TK- und IT-Anbieter** erbringen. Die internationalen Konzerne weisen in ihren periodischen Transparenzberichten bereits einige allgemeine Angaben zur Häufigkeit behördlicher Abfragen aus, die gegebenenfalls weiter spezifiziert werden könnten. Die Kooperationsbereitschaft ist allerdings unterschiedlich ausgeprägt. Nicht alle Firmen sind zur Lieferung von Informationen über zusätzliche, für das Projekt relevante Angaben zu den behördlichen Anfragen bereit. Bislang liegt die Zusage eines großen amerikanischen Unternehmens zur Spezifizierung der sehr allgemein gehaltenen Angaben in den Online-Transparenzberichten durch Zulieferung spezifizierter Daten über Abfragen deutscher Behörden vor. Zu beachten ist dabei jedoch, dass Behörden- und Providerdaten nicht einfach aufaddiert werden können. 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.

Die Providerdaten haben auch darüber hinaus einen Nutzwert für das Projekt. Sie reflektieren die Adressatenperspektive der behördlichen Maßnahmen und könnten bspw. einen Einblick in den Umfang der abgefragten und übermittelten Informationen geben, etwa die betroffenen Datenarten und Datenvolumina. Darüber hinaus könnte die Entwicklung der behördlichen Abfragepraxis bei diesem überindividuellen Adressatenkreis gegebenenfalls auch Anhaltspunkte zur Erklärung bestimmter Entwicklungen im Überwachungsgeschehen liefern. Die Recherchen und konzeptionellen Überlegungen sind insoweit noch nicht abgeschlossen.

3.4. Berechnung der Eingriffsschwere: die Intensitätsformel für die einzelnen Überwachungsmaßnahmen

Die Berechnung der Eingriffsschwere der einzelnen Überwachungsmaßnahmen erfolgt mit Hilfe eines **abstrakten Gewichtungsmodells** auf der Basis eines neu entwickelten, an verschiedenen verfassungsrechtlich relevanten Kriterien orientierten Kategoriensystems (siehe unten *Tabelle 03*). Danach wird jeder Überwachungstatbestand – zum Beispiel die repressive TKÜ nach § 100a Abs. 1 S. 1 StPO – anhand von 16 ausgewählten Kategorien bzw. Kriterien bewertet. Jeder Kategorie ist ein nominaler Wert auf einer Skala 1–10 zugeordnet; dabei korreliert der niedrigste Wert 1 stets mit einer niedrigen Grundrechtsbelastung, der Höchstwert 10 indiziert dementsprechend eine hohe Eingriffsintensität. Da sich die gesetzlichen Voraussetzungen ebenso wie die Verfahrensregeln zum Umgang mit den erhobenen Daten sowie die möglichen Folgemaßnahmen sektoral ebenso wie regional unterscheiden können, wird jede Überwachungsmaßnahme im Kontext ihrer jeweiligen konkreten Rechtsgrundlage – zum Beispiel die präventive TKÜ auf der Basis des § 25a ASOG Bln, § 54 PolG BW oder der Art. 42, 44 BayPAG usw. – als eigener Überwachungssachverhalt behandelt und isoliert/spezifisch bewertet. So ergeben sich separate Teilindizes, die jeweils einzeln betrachtet und auch miteinander verglichen werden können. In der späteren Endausbaustufe des Überwachungsbarometers können sie dann zu einem übergreifenden Bereichsindex TKÜ[79] aufaddiert werden, zusammengesetzt aus den verschiedenen Teil-Indizes repressive TKÜ, TKÜ-BKA, präventive TKÜ-Bundesland A, B, C, TKÜ-Zoll, TKÜ-Dienste etc.

3.4.1. Grundformel

Die Eingriffsschwere der verschiedenen Maßnahmen wird auf der Basis eines einheitlichen Kategoriensystems berechnet. Dieses berücksichtigt alle (grundrechtlich) relevanten Aspekte bzw. Kriterien (siehe dazu gleich unten 3.4.2.). Allerdings können die einzelnen Kategorien des Bewertungsmodells unterschiedliche Eingriffsschwere im Hinblick auf ihre Belastung für die betroffenen Grundrechtsträger haben. So bergen etwa die Merkmale des Richtervorbehaltes oder des Schutzes für Berufsgeheimnisträger eine andere Grundrechtsrelevanz als der Zeitpunkt der nachträglichen Benachrichtigung oder die interne Protokollierung. Dies wird in der Formel berücksichtigt, indem die Kriterien jeweils individuell, d.h. unterschiedlich, gewichtet werden.

In dem hierzu entwickelten Modell kann der Wert jeder einzelnen Kategorie (Basiswert) mit dem bis zu 10-fachen „Gewicht" in die Rechnung eingestellt werden (Gewichtungsfaktor). Mit diesem Gewichtungsfaktor wird der Basiswert dann multipliziert. Pro Kategorie ergeben sich also Minimalwerte zwischen 1 und 10 bzw. Maximalwerte zwischen 10 und 100. Das Endergebnis für eine Maßnahme – das wir als Intensitätsfaktor bezeichnen –, errechnet sich auf der Basis aller einbezogenen Kategorien. Hierzu wird die Summe der Basiswerte nicht etwa durch die reine Anzahl der Kategorien dividiert, sondern jeweils multipliziert mit deren Gewichtungsfaktor. Dadurch erhält eine Maßnahme, die in einer oder mehreren stark gewichteten Kategorien einen hohen Basiswert erreicht, einen höheren Endwert als eine Maßnahme, die vornehmlich in den schwach gewichteten Kategorien hohe Basiswerte erzielt. Der Endwert (Intensitätswert) ist dann stets eine (reelle) Zahl zwischen 1,0 und 10,0.

79 Siehe im Anhang *Tabelle 01* mit den relevanten Überwachungsszenarien unter Nr. 3.

Dies sei veranschaulicht an folgendem abstrakten Beispiel:

Angenommen eine Überwachungsmaßnahme (**R_x**) soll anhand von zehn Kategorien (**K_{1-10}**) bewertet werden. Der Basiswert einer jeden Kategorie K wird immer mit einem Nominalwert zwischen 1 und 10 bestimmt. Zugleich haben **K_{1-5}** den Gewichtungsfaktor 1, **K_{6-9}** den Gewichtungsfaktor 3 und **K_{10}** den Gewichtungsfaktor 5. Die Summe der Kategorien, multipliziert jeweils mit den entsprechenden Gewichtungsfaktoren, beträgt in diesem Fall: **5 + (4 * 3) + (1 * 5) = 22**.

Zu den 10 (realen) Basiswerten kommen quasi 12 fiktive Basiswerte hinzu. Am Ende wird das Ergebnis durch 22 geteilt.

Das Endergebnis liegt dann immer zwischen 1,0 und 10,0. Es repräsentiert also nicht den Durchschnittswert der 10 Basiswerte, sondern stellt ein faktorisiertes Ergebnis dar.

Nun sei angenommen, die Maßnahme **R_1** belegt in **K_{1-5}** jeweils den höchsten Basiswert 10, in **K_{6-9}** jeweils einen mittleren Wert 5 und in **K_{10}** den Bestwert 1. Würden alle zehn Kategorien gleich gewichtet, ergäbe sich fiktiv ein Durchschnittswert von 7,1.

Unter Berücksichtigung der unterschiedlichen Gewichtungsfaktoren ergibt sich stattdessen der folgende Intensitätswert **$I_{R1} = (K_1 + K_{(...)\,10}) / 22$:**

K	**K_1**					**(...)**				**K_{10}**	
Basiswert	10	10	10	10	10	5	5	5	5	1	
Gewichtungsfaktor	1	1	1	1	1	3	3	3	3	5	= 22
Zwischenergebnis	10	10	10	10	10	15	15	15	15	5	= 115
Endergebnis (Intensitätswert)	= Zwischenergebnis / 22										**= 5,27**

Diese Maßnahme hat also bezogen auf ihren Eingriffscharakter einen Intensitätswert von **5,27**.

Zum Vergleich ein zweites Beispiel, in dem eine Maßnahme **R_2** in den schwach gewichteten Kategorien mittelschwere Basiswerte hat und in den stark gewichteten Kategorien als hoch eingriffsintensiv bewertet wird. Bei Zugrundelegung des Wertes 5 für **K_{1-5}**, des Wertes 9 für **K_{6-9}** und des Wertes 10 für **K_{10}** ergäbe sich ebenfalls ein fiktiver Durchschnittswert von 7,1.

Als Intensitätswert **I_{R2}** ergibt sich hier:

K	**K_1**					**(...)**				**K_{10}**	
Basiswert	5	5	5	5	5	9	9	9	9	10	
Gewichtungsfaktor	1	1	1	1	1	3	3	3	3	5	= 22
Zwischenergebnis	5	5	5	5	5	27	27	27	27	50	= 183
Endergebnis (Intensitätswert)	= Zwischenergebnis / 22										**= 8,32**

Die Maßnahme hätte hier einen deutlich höheren Intensitätswert von **8,32** – trotz des identischen fiktiven Durchschnittswerts von 7,1. Durch die Gewichtung bekommen **R_1** und **R_2** also unterschiedliche Endwerte trotz gleicher „Durchschnittsnote".

3.4.2. Kategoriensystem zur Intensitätsberechnung

Für die Bestimmung der maßgeblichen Kategorien, die zur Bemessung der Grundrechtseingriffsintensität einer Überwachungsmaßnahme herangezogen werden sollen, kann auf eine umfangreiche Rechtsprechung zurückgegriffen werden. Der Analyse dieser Rechtsprechung hat sich u.a. *Löffelmann* gewidmet.[80] Dabei konnte er in verschiedenen Beschlüssen und Urteilen zahlreiche Kategorien bzw. Kriterien identifizieren, die die **grundrechtsorientierte Eingriffsintensität** einer Überwachungsmaßnahme determinieren. Die hier beispielhaft zitierte umfangreiche Liste[81] umfasst die folgenden Merkmale:

- → die Anzahl der unmittelbar betroffenen Grundrechtsträger,
- → die Möglichkeit der Anwendung gegenüber Berufsgeheimnisträgern,
- → der Schutz des Kernbereichs privater Lebensgestaltung,
- → die Dauer der Maßnahme,
- → ihre „Streuwirkung“,
- → ihre „Heimlichkeit“,
- → die Qualität der erlangten Daten und deren Umfang,
- → die Möglichkeit der Bildung von Verhaltens-, Kommunikations-, Bewegungs- oder Persönlichkeitsprofilen,
- → der Rang des betroffenen Grundrechts,
- → der Grad der „Beschädigung“ des betroffenen Grundrechts,
- → die gleichzeitige „Beschädigung“ mehrerer Grundrechte,
- → der Status der betroffenen Personen,
- → die Art und Weise der Datenerhebung und etwaiger sie vorbereitender Maßnahmen,
- → ob die Maßnahme durch den Staat selbst oder mithilfe privater Dritter durchgeführt wird,
- → wie viele hoheitliche Stellen zu dem Eingriff ermächtigt werden,
- → besondere Gefahren und weitere Konsequenzen für Betroffene,
- → die Möglichkeiten der weiteren Verwendung erhobener Daten,
- → die Gefährdung des Kernbereichs privater Lebensgestaltung,
- → ob Betroffene selbst einen Anlass für den Eingriff geschaffen haben,
- → ob Schutzvorkehrungen gezielt unterlaufen werden, sowie
- → die gesamtgesellschaftlichen Auswirkungen auf das Verhalten potenzieller Betroffener.

Ähnliche Kriterienkataloge finden sich in Beiträgen von *Hornung/Schnabel*[82] und *Braun/Albrecht*.[83]

Aus methodischen Gründen können nicht alle in der Literatur mit jeweils guten Gründen diskutierten Merkmale in ihrer Vielfalt im Rahmen des Überwachungsbarometers berücksichtigt werden. Datenbasis für die Berechnung der Überwachungslast ist hier der Bestand der zugänglichen statistischen Daten. Diese sind, wie erwähnt, ausschließlich in aggregierter Form verfügbar, sodass a priori alle persönlichen Merkmale zu dem jeweils betroffenen Personenkreis sowie alle Informationen zu sonstigen individuellen Umständen der Überwachungsmaßnahmen fehlen. Methodologische Voraussetzung für die Feststellung solcher Informationen müsste eine einzelfallbezogene empirische Akten- bzw. Fallanalyse sein (siehe oben 3.3.2.1.). Bewertungsgrundlage ist vorliegend daher stets die **abstrakte Eingriffsintensität**, bewertet auf der Basis der für den jeweiligen Überwachungstatbestand maßgeblichen gesetzlichen Voraussetzungen sowie etwaiger weiterer Bestimmungen zu Ziel, Dauer, Durchführung und Beendigung der Maßnahmen und möglichen Folgemaßnahmen. Die Letzteren können zugunsten (z.B. durch Löschungsregeln) oder zuungunsten der Betroffenen (z.B. im Fall einer nachfolgenden Strafverfolgung) wirken.

Unter dieser Prämisse haben wir die gesetzlichen Grundlagen aller im Rahmen des Überwachungsbarometers potenziell relevanten Überwachungstatbestände analysiert und insgesamt 16 Merkmale identifiziert, auf deren Basis die Eingriffsintensität sämtlicher Maßnahmen einheitlich bewertet werden kann. Sie sind aus *Tabelle 03* ersichtlich. Das Kategoriensystem umfasst 12 Merkmale mit konkret vorgegebenen Basiswertoptionen und 4 weitere mit jeweils offenem Bewertungsschema; im letzteren Fall werden die konkreten Bewertungen in einer gesonderten Bewertungsmatrix festgehalten. Jedes Merkmal erhält einen individuellen Basiswert zwischen 1 und 10. Für jede Kategorie wurde zudem ein individueller Gewichtungsfaktor festgelegt, der ebenfalls zwischen 1 und 10 variiert. Die konkrete Berechnung erfolgt einheitlich nach der oben erläuterten Intensitätsformel. Siehe für einige konkrete Anwendungsbeispiele unten *Tabellen 04* und *04a*. Die zugeordneten Einzelwerte sind vorläufig.

80 Insbes. *Löffelmann* GSZ 2019, 16; Löffelmann GSZ 2019, 190.
81 Vgl. *Löffelmann* GSZ 2019, 16 (19); Löffelmann GSZ 2019, 190 (191 f.).
82 *Hornung/Schnabel* DVBl 2010, 824 (826).
83 *Braun/Albrecht* VR 2017, 151 (152).

Tab. 03 | Kategoriensystem zur Berechnung der Intensität der Überwachungsmaßnahmen

	Merkmal	Basiswert	Gewichtungsfaktor
1.	**Potenziell betroffene Grundrechte (Anzahl)**		**1**
	• *[Additiv]*	je 1	
2.	**Ziel der Maßnahme**		**4**
	• Strafverfolgung	10	
	• Gefahrenabwehr	7	
	• Nachrichtendienstliche Beobachtung/Aufklärung	5	
	• Verwaltung	1	
3.	**Durchführung der Informationserhebung**		**5**
	• Eigene Erhebung	3	
	• Manuelles Auskunftsverfahren bei verpflichteten Privaten	5	
	• Automatisiertes Auskunftsverfahren bei verpflichteten Privaten	7	
	• Gesetzliche Verpflichtung zur proaktiven Zulieferung	10	
4.	**Heimlichkeit**		**5**
	• Verdeckte Maßnahme	10	
	• Maßn. für Dritte erkennbar, sanktioniertes Mitteilungsverbot	7	
	• Maßn. für Dritte erkennbar, sanktionsloses Mitteilungsverbot	5	
	• Maßn. für Dritte erkennbar, kein explizites Mitteilungsverbot	2	
	• Offene Maßnahme	1	
5.	**Richtervorbehalt**		**2**
	• Ja, immer	1	
	• Grds. ja, bei Gefahr in Verzug auch Staatsanwaltschaft	3	
	• Grds. ja, bei Gefahr in Verzug auch Polizei	7	
	• Nein	10	
6.	**Schutz für Berufsgeheimnisträger**		**3**
	• Ausnahmsloser Schutz	1	
	• Eingeschränkter Schutz	5	
	• Kein Schutz	10	
7.	**Benachrichtigungspflicht nach Durchführung**		**1**
	• Ja, unverzüglich	1	
	• Zeitlich/sachlich verzögert	5	
	• nein	10	
8.	**Zulässigkeit der Datenweitergabe**		**1**
	• Ja, uneingeschränkt	10	
	• Ja, bei Zweckänderung unter Bedingungen	7	
	• Ja, aber nur für identischen Zweck	5	
	• Nein	1	
9.	**Löschungspflicht**		**1**
	• Spezialgesetzlich: unverzüglich	1	
	• Spezialgesetzlich: zeitlich/sachlich verzögert	5	
	• Nach allgemeinem Datenschutzrecht	6	
	• *(Nein)*	*(10)*	

10.	**Protokollpflicht**		**1**
	• Ja	1	
	• Nein	10	
11.	**Zeitliche Richtung**		**1**
	• Retrograde Abfrage	10	
	• Aktuelle Abfrage (Echtzeit)	3	
	• Zukunftsgerichtete Abfrage	7	
12.	**Maximal mögliche Dauer der Maßnahme**		**3**
	• Punktuelle Abfrage	4	
	• Temporäre Überwachung bis zu 24 Stunden	5	
	• Temporäre Überwachung bis zu 2 Wochen	6	
	• Temporäre Überwachung bis zu 1 Monat	7	
	• Temporäre Überwachung über 1 Monat, aber nicht unbegrenzt	8	
	• Temporäre Überwachung über 3 Monate, aber nicht unbegrenzt	9	
	• Dauerhafte Überwachung (zeitlich unbegrenzt)	10	
13.	**Streubreite**		**10**
	• *[Bewertung nach gesonderter Bewertungsmatrix]*	1–10	
14.	**Anlass/Voraussetzungen der Datenanlegung**		**10**
	• *[Bewertung nach gesonderter Bewertungsmatrix]*	1–10	
15.	**Anlass/Voraussetzungen der Datenabfrage**		**10**
	• *[Bewertung nach gesonderter Bewertungsmatrix]*	1–10	
16.	**Privatcharakter der erhobenen/abgefragten Daten**		**10**
	• *[Bewertung nach gesonderter Bewertungsmatrix]*	1–10	

3.5. Die Indexformel

In der Zusammenschau von statistischer Häufigkeit (3.3.2.1.) und Gewichtung der Maßnahmen auf Basis der Intensitätsformel (3.4.) wird schließlich – wiederum separat für jeden Überwachungstatbestand – die effektive Überwachungslast errechnet. Der **Überwachungsindex** kann auf verschiedene Weise berechnet werden. Hierfür haben wir zwei alternative Indexformeln (Modell A und Modell B) entwickelt.

Das einfachere **Modell A** basiert auf der absoluten Zahl der Maßnahmen im jeweiligen Referenzzeitraum (**N_{Jahr}**); multipliziert mit dem zugehörigen Intensitätsfaktor (**I**) ergibt sich die Überwachungslast in dem jeweiligen Sektor. Um die Zahlen größenmäßig überschaubar zu halten, werden die Nominalwerte pro Tausend ausgewiesen und nach den allgemeinen Regeln auf- bzw. abgerundet. Das Resultat wird zusätzlich nach einem linear-progressiven Stufenmodell[84] indexiert, das insgesamt **5 Progressions- bzw. Schwerestufen** umfasst. Dabei werden alle Überwachungstatbestände mit einem Indexwert unter 100 der Gruppe 1 zugeordnet, alle über 1.000 der Gruppe 5.

84 Linear-progressives Modell: 100er – 75er – 50er-Schritte.

Überwachungsindex – Modell A:

1	2				3				4				5
<100	>100	>200	>300	>400	>500	>575	>650	>725	>800	>850	>900	>950	>1.000

Modell B ist abstrakter konstruiert. Ausgangspunkt ist hier zunächst der verfassungsrechtlich orientierte Intensitätsfaktor (**I**). Zweites Element der Formel ist ebenfalls die Anwendungshäufigkeit, allerdings nicht mit der jeweils realen Zahl, sondern in indexierter Form. Hierfür wird ein spezifischer Häufigkeitskoeffizient (**$Koeff_N$**) gebildet.

$Koeff_N$ beträgt:

Häufigkeit	<10	<50	<100	<200	<500	<1.000	<2.000	<10.000	<30.000	> 30.000
$Koeff_N$	1	2	3	4	5	6	7	8	9	10

Durch Multiplikation der beiden Werte (**I * $Koeff_N$**) ergibt sich sodann der finale Überwachungsindex; dieser bewegt sich immer zwischen den Werten 1 und 100. Da die Gewichtung hier im Vergleich zu Modell A bereits bei der Berechnung des Häufigkeitskoeffizienten stattfindet, erfolgt die Klassifizierung auf der Basis eines **linearen Stufenmodells**. Die finale Skalierung kann daher recht einfach in Dezimalschritten erfolgen; um die Vergleichbarkeit mit Modell A zu erleichtern, kann die Skalierung alternativ ebenso in 20er-Schritten erfolgen. Nachfolgend werden beide Möglichkeiten berücksichtigt.

Überwachungsindex – Modell B:

1		2		3		4		5	
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
1-10	11-20	21-30	31-40	41-50	51-60	61-70	71-80	81-90	91-100

Die unterschiedlichen Berechnungsmodelle führen zu unterschiedlichen Ergebnissen. Dies wird aus *Tabelle 04* ersichtlich, die die Überwachungsindizes an einigen konkreten Beispielen aufzeigt. Modell A bildet die Realbelastung in Form der statistischen Häufigkeit deutlicher ab als Modell B. Das hat den Vorteil, dass die erhebliche Varianz in den Anwendungszahlen für die verschiedenen Überwachungstatbestände – wenn auch in abgeschwächter Form – sichtbar bleibt. Gewisse Unschärfen stellen sich freilich bei den Maßnahmen mit niedrigen und sehr niedrigen Anwendungszahlen (< 100) ein, wie die Beispiele einzelner Anwendungen auf Landesebene (hier der bayerischen Polizei) anzeigen. Bei Modell B wird die hohe Varianz in der Häufigkeit deutlich reduziert. Dies ist eine wesentliche Folge der stärkeren Gewichtung der grundrechtlichen Eingriffsintensität. Die Anwendungszahlen selbst sind hier lediglich ein Rechenfaktor. Die Unschärfen betreffen eher den oberen Bereich (> 30.000).

Der Unterschied der Modelle wird besonders deutlich am Beispiel der anlasslosen Flugdatenspeicherung, die nach dem momentanen Stand faktisch die Überwachungsspitze repräsentiert, und ihrem Vergleich mit der strafprozessualen TKÜ.

→ Modell A (nach oben offene Index-Skala, linear-progressiv indexiert 1–5) errechnet für Erstere einen Wert von 2.080.832, für die TKÜ gemäß § 100a StPO einen Wert von 97. Die Fluggastdatenspeicherung hat danach eine 20.000-fach stärkere Überwachungslast. Indexiert liegen die beiden Überwachungstatbestände jeweils am oberen (5) und unteren Ende (1) der Progressionsskala. Dass die TKÜ nur einen Bruchteil der Bevölkerung betrifft, zeigt das Modell A schön auf. Die reale Überwachungslast der strafprozessualen TKÜ stellt sich danach eher niedrig dar. Dabei wirken sich der hohe Teiler von 1.000 und die einfache Multiplikation des Intensitätswerts rechnerisch dahingehend aus, dass die Maßnahmen in der Tendenz einen niedrigen Skalenwert haben, der ihre abstrakte Schwere unter Umständen nicht angemessen abbildet. Massensammlungen erreichen hingegen aufgrund der nicht-indexierten Einbeziehung in die Gleichung regelmäßig einen Höchstwert.

→ In Modell B (geschlossene Index-Skala, linear indexiert 1–5 bzw. 1–10) ist die Varianz zwischen den Werten deutlich geringer. Die Fluggastdatenspeicherung erreicht zwar auch hier einen sehr hohen Wert, nämlich 83,3. Ein relativer Unterschied zeigt sich aber bei der strafprozessualen TKÜ. Diese erreicht in diesem Modell einen mittleren Wert von 47,8. Indexiert entsprechen diese Werte 3 bzw. 5 auf der oben dargestellten Skala B. Weder erreicht die Flugastdatenspeicherung hier einen Maximalwert, noch wird der Unterschied in der realen Anzahl der beiden Maßnahmen so deutlich erkennbar wie nach Modell A. Die strafprozessuale TKÜ wird hier als mittelschwer dargestellt, was ihrer abstrakten Eingriffsschwere möglicherweise eher entspricht. Andererseits kann aber nicht einmal die Fluggastdatenspeicherung, welche quantitativ einen Extremwert aufweist, ungeachtet des ebenfalls recht hohen Intensitätswertes nicht das obere Ende der Skala erreichen. Dies liegt daran, dass der Intensitätswert selbst bei hoch gestreuten und intensiven Maßnahmen kaum über 90 liegen wird, da regelmäßig in den übrigen Kategorien ein Ausgleich stattfindet. Für Modell B bedeutet dies, dass weder das unterste noch das oberste Ende der Skala besonders häufig erreicht werden. Es dürfte zu mittleren Werten tendieren. Dabei bleibt freilich die Frage offen, ob der unterschiedlichen Wirkung von Massensammlungen und Individualmaßnahmen damit Genüge getan wird.

In Anbetracht der aufgezeigten Unterschiede sollen beide Modelle bis auf Weiteres parallel verwendet werden und jeweils für sich nicht den Anspruch auf Vollständigkeit und exakte Darstellung der verfassungsrechtlichen Aussagen erheben. Damit wird aber zugleich evident, dass feste Aussagen zum Verhältnis von individuellen Maßnahmen und Massensammlungen noch gar nicht existieren. Das Bundesverfassungsgericht hat sich zu beiden kritisch geäußert,[85] ohne bislang die unterschiedliche Wirkung auf die Gesamtlast der Überwachung auf die Gesellschaft ausführlich zu diskutieren.

85 Zu Individualmaßnahmen etwa in BVerfGE 141, 220 – BKAG und zur Vorratsdatenspeicherung bekanntlich in BVerfGE 125, 260 – Vorratsdatenspeicherung.

Tab. 04 | Vergleich der beiden Modelle am Beispiel ausgewählter Überwachungstatbestände

Maßnahme (R)	Anzahl der Maßnahmen in 2019 (N_{2019})	Intensitätswert (I)*	Indexwert	
			Modell A**	Modell B***
1. § 2 FlugDaG**** Übermittlung von Fluggastdaten von Flugunternehmen an das BKA (anlasslose Vorratsdaten-speicherung)	249.799.750	8,33	**2.080.832** *(5)*	**83,3** *(5)|(9)*
2. § 100a StPO TKÜ durch die Strafverfolgungs-behörden	18.225	5,31	**97** *(1)*	**47,79** *(3)|(5)*
3. Art. 42 Abs.1 BayPAG Präventive TKÜ (Polizei Bayern)	41	5,81	**0,22** *(1)*	**16,35** *(1)|(2)*
4. § 24c Abs. 3 Nr. 2 KWG Kontobestandsdatenabfrage durch die Strafverfolgungsbe-hörden	186.575	8,11	**1.513** *(5)*	**81,1** *(5)|(9)*
5. § 43 GWG Proaktive Verdachtsmeldungen von Finanzinstituten an die FIU	114.914	8,49	**976** *(4)*	**84,9** *(5)|(9)*
6. § 20a PolG NRW Präventive Erhebung von TK-Ver-kehrsdaten (Polizei NRW)	1.398	7,19	**10** *(1)*	**49,91** *(3)|(5)*
7. Art. 43 Abs.1 S. 2, Art. 42 Abs. 1, 4 BayPAG i.V.m. § 113b TKG Erhebung retrograder TK-Ver-kehrsdaten (Vorratsdaten) durch die Polizei (Bayern)	3	7,13	**0,02** *(1)*	**7,13** *(1)|(1)*
8. Art. 43 Abs. 2 S. 1 Nr. 3, Art. 42 Abs. 1 S. 1 bzw. Abs. 4 S.1 BayPAG Abfrage spezifischer Kennungen (Geräte und Kartennummern) durch die bayerische Polizei	2	4,77	**0,01** *(1)*	**4,77** *(1)|(1)*

*) Zur konkreten Berechnung der zugrundeliegenden Basiswerte siehe *Tabelle 04a*;

) (**I x N_{2019}) / 1.000;

***) **I x $Koeff_N$**;

****) Anzahl abgeleitet aus den offiziellen Passagierzahlen (siehe oben 3.2.2.1.).

Die Zusammensetzung und exakte Skalierung der einzelnen Rechengrößen ist im Übrigen vorläufig und offen für weitere Feinjustierungen.

Tabelle 04a schlüsselt die Berechnungsmethode näher auf. Hier wird am Beispiel der Telekommunikationsüberwachung gut erkennbar, dass die Intensitätsbewertung identischer Maßnahmen infolge unterschiedlicher gesetzlicher Ausgestaltung in der jeweiligen Ausprägung erkennbar variieren kann: So erreicht die repressive TKÜ auf der Grundlage von § 100a StPO (siehe Tabellenspalte 2) im Ergebnis einen niedrigeren Schwere-Score (5,31) als die präventive TKÜ unter den gesetzlichen Rahmenbedingungen des § 43 Abs. 1 BayPAG (5,81; siehe Spalte 3); in Hessen ist die Eingriffsintensität der präventiven TKÜ auf der Basis des § 15a HSOG (5,33; siehe Spalte 3a) dagegen ungeachtet einiger Unterschiede bei vier der 16 Merkmale im Ergebnis vergleichbar mit derjenigen der TKÜ zum Zwecke der Strafverfolgung. Die bayerische und die etwas grundrechtsschonendere hessische Variante der präventivpolizeilichen TKÜ unterscheiden sich ihrerseits hinsichtlich dreier Merkmale. Bei zwei Merkmalen unterscheiden sich alle drei Varianten voneinander.

Tab. 04a | Überblick über die Rechengrößen zur Berechnung ausgewählter Intensitätswerte*

Merkmal	Maßnahme (R)**								
	1	**2**	**3**	***3a****	**4**	**5**	**6**	**7**	**8**
1. Potenziell betroffene Grundrechte	2	2	2	*2*	1	1	1	1	2
2. Ziel der Maßnahme	40	40	28	*28*	40	40	28	28	28
3. Durchführung der Informationserhebung	50	15	15	*15*	35	50	25	25	25
4. Heimlichkeit	10	35	10	*35*	50	50	10	10	10
5. Richtervorbehalt	20	6	14	*14*	20	20	20	14	14
6. Schutz für Berufsgeheimnisträger	20	10	10	*10*	10	10	10	10	10
7. Benachrichtigungspflicht nach Durchführung	10	5	5	*5*	10	10	5	5	5
8. Zulässigkeit der Datenweitergabe	5	10	7	*5*	10	10	5	7	7
9. Löschungspflicht	5	5	5	*5*	5	5	5	5	5
10. Protokollpflicht	1	1	1	*1*	1	1	1	1	1
11. Zeitliche Richtung	10	7	7	*7*	10	10	10	10	3
12. Maximal mögliche Dauer der Maßnahme	12	27	27	*27*	12	12	12	12	12
13. Streubreite	100	10	10	*10*	100	100	100	100	10
14. Anlass/Voraussetzungen der Datenanlegung	0	0	0	*0*	100	100	100	100	0
15. Anlass/Voraussetzungen der Datenabfrage	100	30	90	*40*	80	60	70	70	70
16. Privatcharakter der Daten	90	100	100	*100*	60	90	80	80	70
Intensitätswert (I)	**8,33**	**5,31**	**5,81**	***5,33***	**8,11**	**8,49**	**7,19**	**7,13**	**4,77**

*) Gewichtete Basiswerte (vgl. *Tabelle 04*).

) 1: § 2 FlugDaG; 2: § 100a StPO; 3: Art. 42 Abs. 1 BayPAG; 3a: § 15a *HSOG**; 4: § 24c Abs. 3 Nr. 2 KWG; 5: § 43 GWG; 6: § 20a PolG NRW; 7: Art. 43 Abs. 1 S. 2, Art. 42 Abs. 1, 4 BayPAG i.V.m. § 113b TKG; 8: Art. 43 Abs. 2 S. 1 Nr. 3, Art. 42 Abs. 1 S. 1 bzw. Abs. 4 S. 1 BayPAG.

***) *Beispiel Nr. 3a (§ 15a HSOG) wegen fehlender Häufigkeitszahl nicht in Tabelle 04 integriert.*

3.6. Darstellung der Ergebnisse

Zur Visualisierung der Überwachungslast für die jeweiligen Maßnahme wurde ein Farbschema gewählt, das auf der leicht verständlichen (erweiterten) Ampelfarbenpalette (halbierter CMYK-Farbkreis) basiert. Das Tachometer-Format erscheint vorzugswürdig, weil sich dabei auf den ersten Blick unmittelbar die Positionierung erkennen lässt, ohne dass die betrachtende Person stets die Bedeutung des jeweiligen Farbwertes abgleichen müsste. Sowohl die Teilindizes für die einzelnen Zugriffspfade wie auch die Gesamtindizes sollen einzeln nachvollziehbar sein.

Modell A

Modell B

Tab. 05 | Überblick über die effektive Überwachungslast zum Stichtag X in ausgewählten Bereichen
[aktuell fiktive Beispielswerte, hier exemplarisch nach Modell A]

	Maßnahme	Überwachungs-Indizes	
1.	**Gesamtindex Bestandsdatenabfrage**		
	Teilindizes		
	Staatsanwaltschaften – *§ 100j StPO*	310	
	BKA – *§ 40 BKAG*	25	
	Bundespolizei – *§ 22a BPolG*	725	
	Landespolizei A – *§ X PolG A*	10	
	Landespolizei B – *§ X PolG B*	0,3	
	…		
	…		
2.	**Gesamtindex Verkehrsdatenabfrage**		
	Teilindizes		
	…		
	…		
	usw.		
	…		

Der finale Gesamtindex (hier fiktiv dargestellt für Bereich 1: Bestandsdatenabfragen) wird jeweils auf der Basis des statistischen Mittelwertes (Median) der einzelnen Teil-Indizes errechnet.

4. Ausgewählte Beispiele

Zusätzlich zu den eigentlichen Indizes sollen die periodisch aktualisierten Materialien zum Überwachungsbarometer einen ausführlicheren Bestand an Informationen bereitstellen, die – im Sinne eines Daten-Anhanges – die zugrunde liegenden Basiszahlen ausführlich dokumentieren und nach verschiedenen Parametern analysieren. Dies erscheint vor allem in denjenigen Bereichen sinnvoll, in denen das verfügbare Zahlenmaterial einen mehrjährigen Zeitraum abdeckt. Über den Zeitverlauf hinweg werden die Datengrundlagen entsprechend anwachsen und können dann jeweils fortgeschrieben werden.

Die Möglichkeiten wurden im Zuge des zunächst explorativen Projekts exemplarisch für drei Bereiche getestet, für die bereits ausreichende statistische Daten auch retrospektiv verfügbar sind:

→ Entwicklung der Telekommunikationsüberwachung und der Abfrage von Telekommunikations-Verkehrsdaten,

→ Entwicklung der Übermittlung von Finanzdaten im Rahmen der Geldwäschekontrolle,

→ Entwicklung verdeckter Abrufe von Kontobestandsdaten.

Darüber hinaus wurden stellvertretend für die Adressatenperspektive die öffentlich verfügbaren Daten zu der

→ Entwicklung bei den Auskunftsersuchen gegenüber IT-Providern[86] ausgewertet.

4.1. Entwicklung der Zugriffe im zeitlichen Verlauf

Die nachfolgenden Tabellen *10, 20, 30* und *40* zeigen zunächst die Entwicklung der Abfragen bzw. sonstigen Zugriffe auf Daten in den genannten Bereichen in der zeitlichen Abfolge in absoluten Zahlen. Diese sind in den Schaubildern *10, 20, 30* und *40* grafisch entsprechend aufbereitet.

In nahezu allen Bereichen zeigt sich eine deutliche Zunahme. Besonders ausgeprägt ist der Anstieg bei den verschiedenen Formen der Kontoabfrage und bei der strafprozessualen Verkehrsdatenabfrage. Bei der Abfrage von Kontobestandsdaten verläuft die Zunahme zuletzt fast exponentiell, mit einer Verdoppelungszeit von 3,75 Jahren bei allen Abfragen und 1,04 Jahren bei den Abfragen gem. § 93 Abs. 8 AO. Hingegen ist bei der klassischen (repressiven) Telekommunikationsüberwachung (Inhaltsüberwachung), wie bereits an anderer Stelle erläutert,[87] eine Stagnation zu beobachten. Erkennbar im Wachsen begriffen ist auch die Zahl der Datenabfragen bei den einbezogenen IT-Providern, jedenfalls bei der Gesamtbetrachtung. Allerdings variiert die Entwicklung zwischen den Unternehmen mitunter beträchtlich (vgl. ergänzend auch *Tabelle 45*), was mit Marktanteilen und der Art und Reichweite der angebotenen Dienstleistungen erklärt werden könnte.

Bezogen auf die absoluten Zahlen zeigt sich zudem, dass die Überwachungsdichte im Zusammenhang mit der anlasslosen Vorratsdatenspeicherung von Kontoführungs- und sonstigen Finanztransaktionsdaten deutlich höher ausfällt als im Bereich der Telekommunikation. Beides betrifft den Alltag aller Bürgerinnen und Bürger. Noch häufiger ist die Inzidenz bei der Bestandsdatenabfrage ihre Bankkonten betreffend.

86 Basierend auf den online publizierten Transparenzberichten / Law Enforcement Reports der Unternehmen; siehe oben 3.3.2.1.

87 Zu möglichen Erklärungen siehe oben unter 2. (Fn. 23).

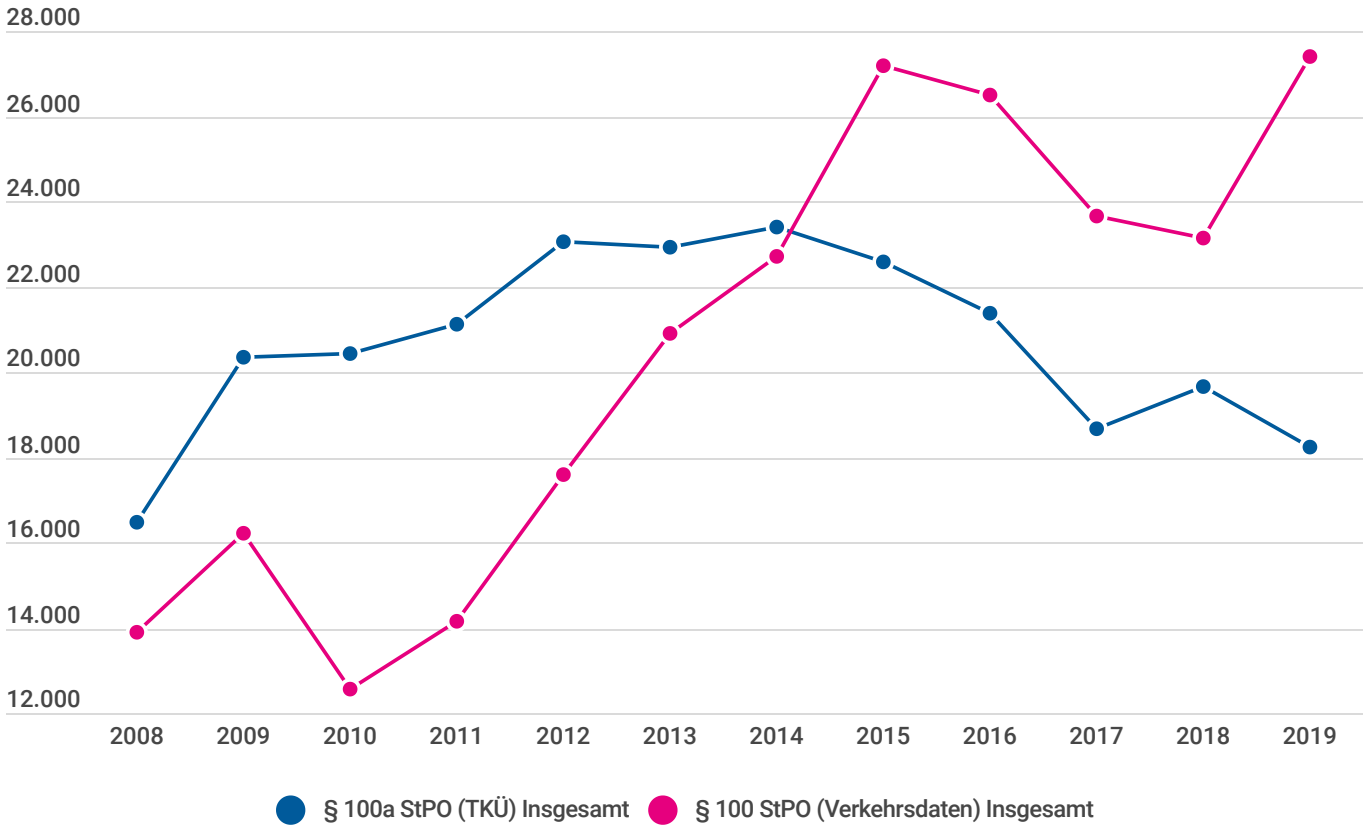
Beispiel 1: Entwicklung der Telekommunikationsüberwachung – Verkehrs- und Inhaltsdaten –
(nur Strafverfolgung, vgl. Überwachungsschema *Tabelle 01*: Nr. 2a u. 3a)

Tabelle 10 | Entwicklung der Anordnungen (absolute Zahlen)*

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
§ 100a StPO insgesamt (TKÜ)	16.463	20.358	20.438	21.118	23.061	22.917	23.382	22.590	21.355	18.651	19.474	18.225
Erstanordnungen	13.949	17.208	17.391	18.029	19.616	19.398	19.795	18.640	17.510	15.669	15.787	15.508
Verlängerungs-anordnungen	2.514	3.150	3.047	3.089	3.445	3.519	3.587	3.950	3.845	2.982	3.887	2.717
§ 100g StPO insgesamt (Verkehrsdaten)	13.904	16.226	12.576	14.153	17.599	20.923	22.701	27.164	26.504	23.640	23.143	27.405
Erstanordnungen	13.426	15.707	12.239	13.743	17.137	20.242	21.926	26.265	25.640	22.929	22.367	26.571
Verlängerungs-anordnungen	478	519	337	410	462	681	775	899	864	711	776	834

*) Datenquelle: Jahresstatistiken Bundesamt für Justiz.

Schaubild 10 | Entwicklung der Anordnungen in absoluten Zahlen



Beispiel 2: Entwicklung der proaktiven Verdachtsanzeigen der privaten Verpflichteten an die FIU im Rahmen der Geldwäschekontrolle

(vgl. Überwachungsschema Tabelle 01: Nr. 7a/b)

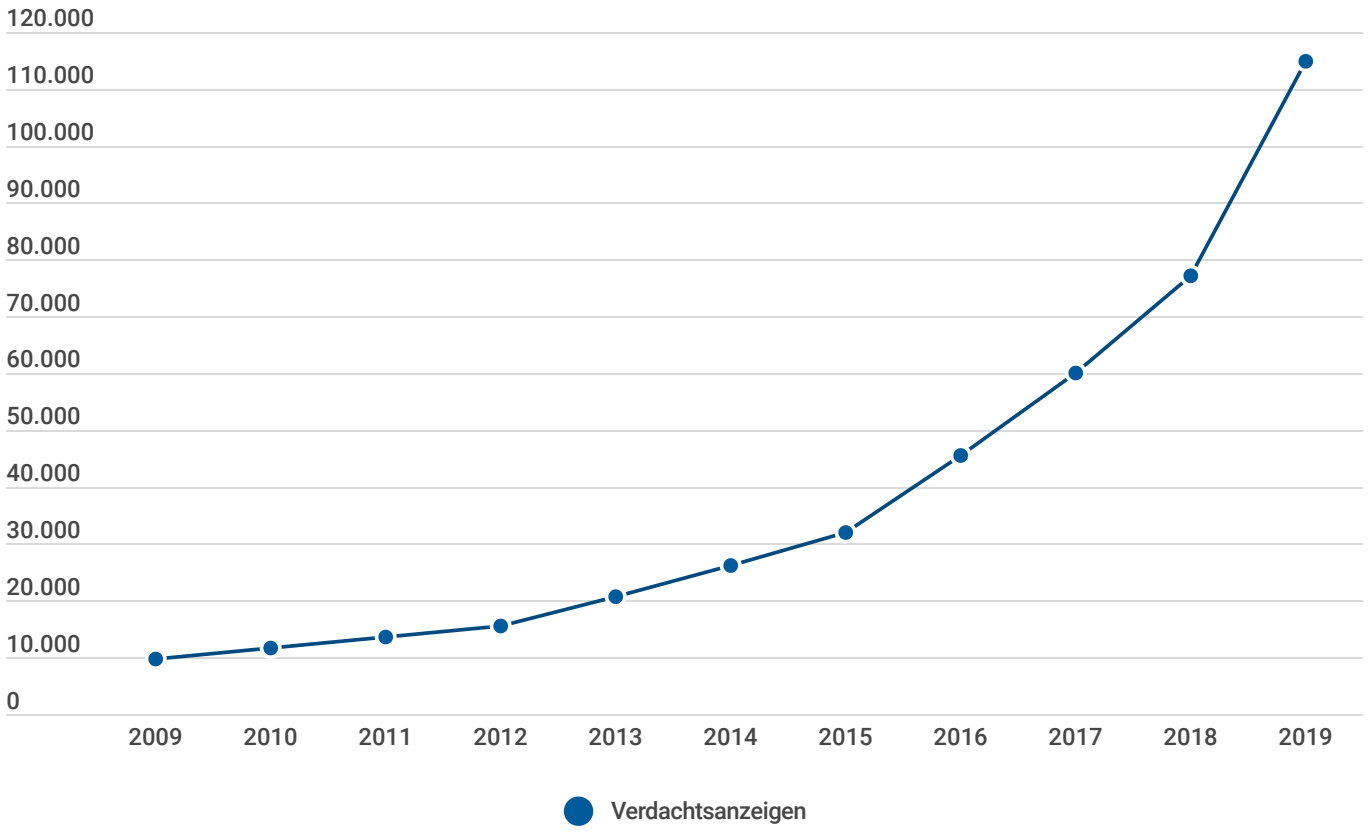
Tabelle 20 | Entwicklung der Verdachtsanzeigen nach dem GwG (absolute Zahlen)

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Verdachtsanzeigen*	9.756	11.712	13.544	15.496	20.716	25.980	32.008	45.597	59.845	77.252	114.914

Datenquelle: Generalzolldirektion, Jahresbericht 2019 der Financial Intelligence Unit.

*) Anzeigeerstattung umfasst die Übermittlung der Vorratsdaten gem. § 8 GwG (Bestands- u. Transaktionsdaten).

Schaubild 20 | Entwicklung der Verdachtsanzeigen nach dem GwG



Beispiel 3: Entwicklung der behördlichen Kontoabfragen
(ohne Nachrichtendienste, vgl. Überwachungsschema Tabelle 01: Nr. 8a)

Tabelle 30 | Entwicklung der behördlichen Kontoabfragen insgesamt und nach Zugriffstatbeständen (absolute Zahlen)*

	2005	2006	2007	2008	2009	2010	2011
Insgesamt	72.611	**106.725**	121.309	117.557	134.942	162.311	178.097
§ 93 Abs. 7 AO[1]	10.201	25.283	27.440	31.510	37.291	48.558	53.065
§ 93 Abs. 8 AO[2]	0	286	309	2.109	5.775	8.138	8.124
§ 24c KWG[3]	62.410	81.156	93.560	83.938	91.876	**105.615**	116.908

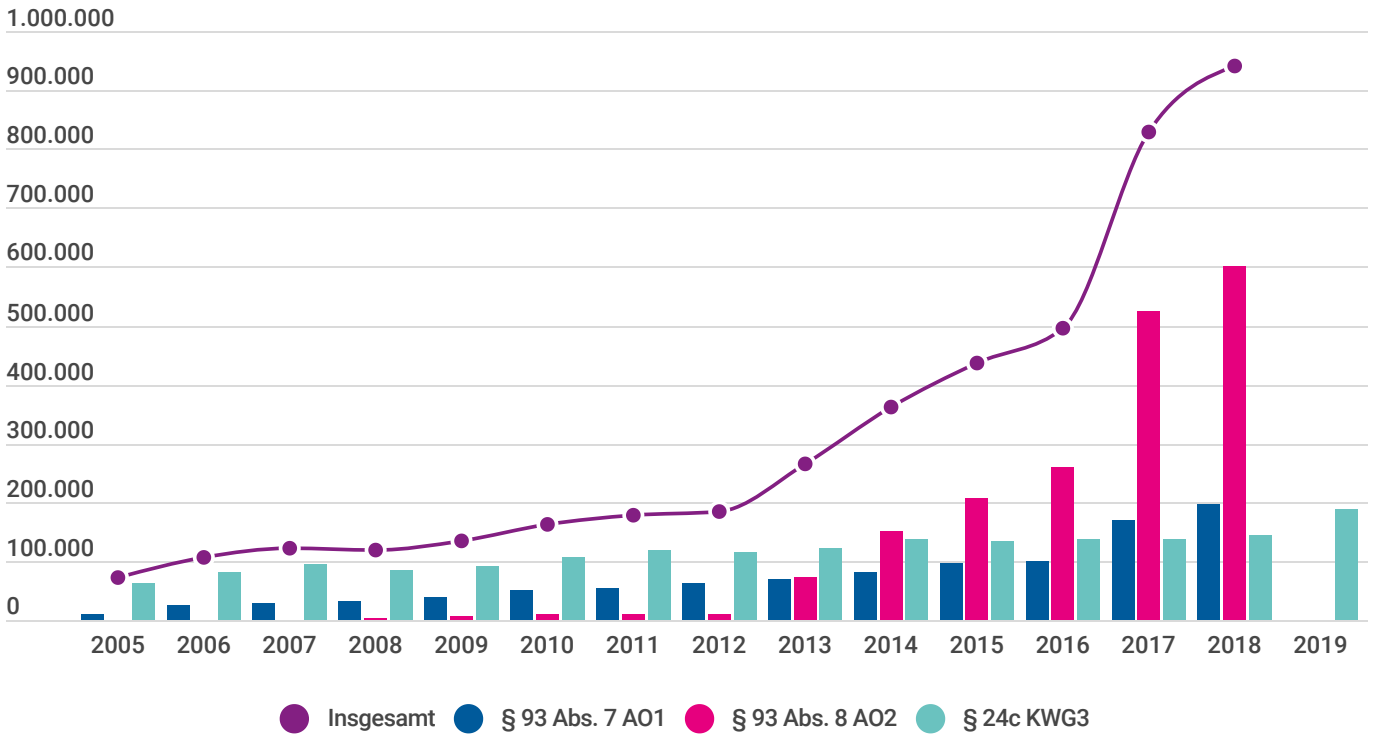
	2012	2013	2014	2015	2016	2017	2018	2019
Insgesamt	185.070	**264.304**	**360.321**	**436.105**	495.412	**829.011**	**939.488**	-
§ 93 Abs. 7 AO[1]	61.629	68.648	79.719	97.631	98.916	**167.314**	196.088	-
§ 93 Abs. 8 AO[2]	9.077	72.992	**150.823**	**204.519**	259.312	**524.852**	**600.512**	-
§ 24c KWG[3]	114.364	122.664	137.779	133.955	137.184	136.845	142.888	186.575

Datenquellen: BT-Drucksache 19/9177; BaFin Jahresberichte 2005–2019.
1) Abfrage durch Finanz- und Zollbehörden.
2) Abfrage durch Polizei-, Verwaltungs-, Sozialbehörden und Gerichtsvollzieher.
3) Abfrage durch Strafverfolgungsbehörden, Finanzbehörden (Steuerfahndung etc.), Zollbehörden, u.a.

*) Hervorhebungen zeigen jeweils Übergänge in höhere 100.000er-Stufen an.

Verdopplungszeitraum insgesamt: 3,75 Jahre; § 93 Abs. 7 AO: 3,77 J.; § 93 Abs. 8 AO: **1,04 J.**; § 24c KWG: 11,75 J.

Schaubild 30 | Entwicklung der behördlichen Kontoabfragen insgesamt und nach Zugriffstatbeständen



Beispiel 4: Entwicklung der behördlichen Abfragen bei IT-Providern

(rechtliche Zuordnung der Abfragen und Kategorisierung der abgefragten Daten im gegenwärtigen Stadium noch nicht möglich)

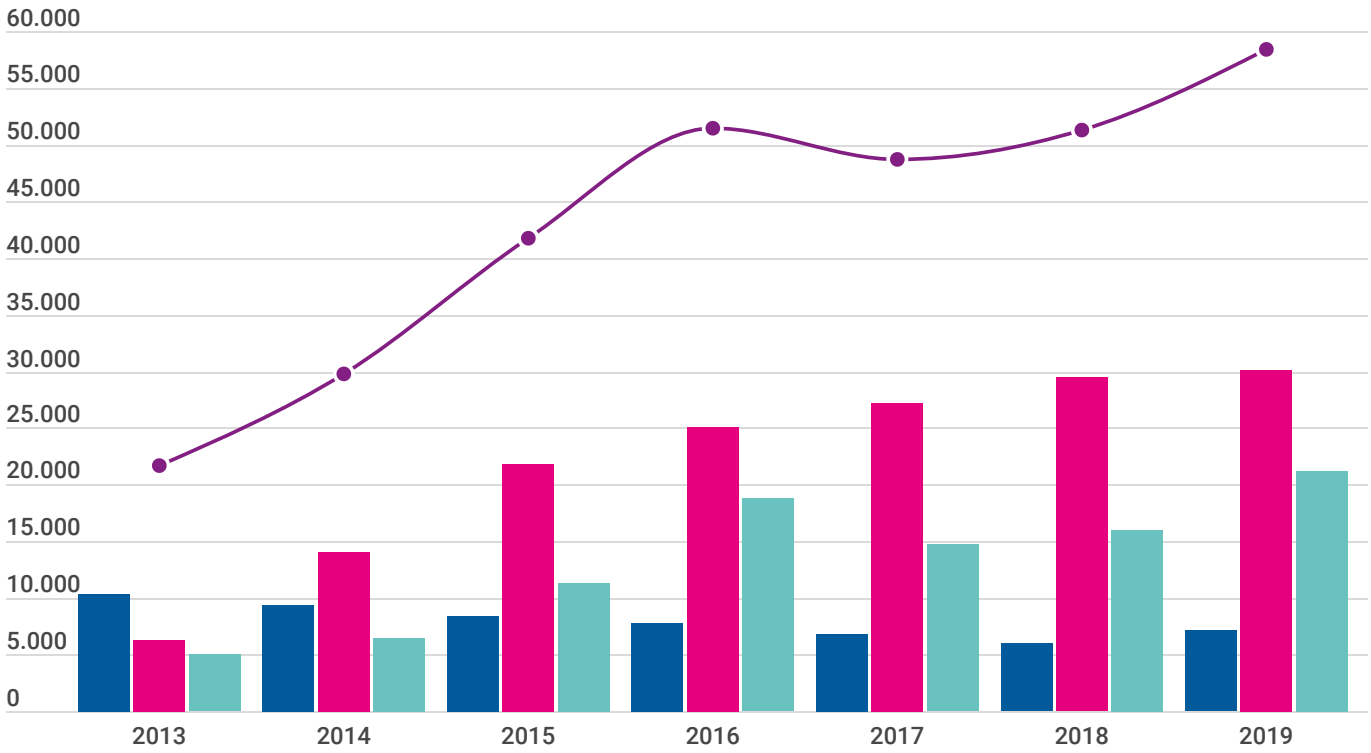
Tabelle 40 | Behördliche Auskunftsersuchen bei drei marktführenden IT-Providern* betreffend Nutzer- bzw. Inhaltsdaten

	2013	2014	2015	2016	2017	2018	2019	*2013-2019*
Microsoft	10.389	9.375	8.433	7.713	6.854	5.924	7.084	*55.772*
Apple	6.344	13.999	21.852	25.010	27.108	29.356	30.158	*153.827*
Google	4.971	6.452	11.394	18.713	14.741	15.976	21.171	*93.418*
Insgesamt	21.704	29.826	41.679	51.436	48.703	51.256	58.413	*303.017*

Datenquellen: Transparenzberichte/Law Enforcement Reports der betroffenen Unternehmen.

*) Amazon hat erstmals für das 2. Halbjahr 2020 länderspezifische Daten veröffentlicht. Danach wurden von deutschen Behörden insgesamt 11.779 Auskunftsersuchen zugestellt, davon 44 bezogen auf cloud-gespeicherte Daten (1.7. – 31.12.2020); https://d1.awsstatic.com/certifications/Information_Request_Report_December_2020.pdf.
Die verfügbaren Daten aus früheren Zeiträumen sind nicht vergleichbar; www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF.

Schaubild 40 | Behördliche Auskunftsersuchen bei drei marktführenden IT-Providern betreffend Kunden/Kundendaten



4.2. Analyse der Häufigkeitsdaten

Die Entwicklung bei den Zugriffen lässt sich auf verschiedene Art und Weise analysieren und darstellen. So lassen sich die Trends zunächst recht einfach im Hinblick auf ihre jährliche Veränderung quantifizieren. Diese kann ihrerseits auf zwei verschiedene Arten dargestellt werden.

Am häufigsten werden die Trends auf Basis der jährlichen prozentualen Zunahme bzw. Abnahme berechnet. Diese sind nachfolgend in den *Tabellen 11, 21, 31* und *41* ausgewiesen. Hier wird dann beispielsweise bei den repressiven TKÜ-Maßnahmen (Inhalts- und Verkehrsdaten) eine differenzierte Entwicklung mit Veränderungen in beide Richtungen deutlich *(Tabelle 11)*, während die Zahl der Verdachtsanzeigen *(Tabelle 21)* und der Kontoabfragen *(Tabelle 31)* von Jahr zu Jahr kontinuierlich zunimmt, bei den Letzteren mit jährlichen Zuwächsen von teilweise mehreren hundert Prozent. Die auffälligsten Einzelwerte sind alternativ farblich gekennzeichnet.

Alternativ kann auch die Gesamtentwicklung über den beobachteten Zeitraum berechnet werden. Dies ist in den *Tabellen 12, 22, 32* und *42* ausgewiesen, die jeweils die Jahreswerte im Vergleich zum Ausgangsjahr ausweisen (kumulierte Prozent). Auf dieser Basis zeigt sich beispielweise, dass die Zahl der Telekommunikationsüberwachungen 2019 nur unwesentlich über der des Jahres 2008 lag (111%), während sich die Verkehrsdatenabfragen annähernd verdoppelt haben (197 %, siehe *Tabelle 12*). Ganz andere Dimensionen sehen wir bei den Verdachtsanzeigen, die sich mehr als verzehnfacht haben (*Tabelle 22*). Dasselbe gilt für die einfachen Kontoabfragen, wobei sich die unterschiedlichen Zugriffstatbestände deutlich unterscheiden: Während sich die Abfragen auf der Basis von § 24c KWG verdoppelt haben, beträgt der Gesamtzuwachs bei den Fällen nach § 93 Abs. 8 AO mehr als 2.000 Prozent (*Tabelle 32*).

Zuletzt wurden die jährlichen Zugriffszahlen in – fiktive – tägliche Durchschnittszahlen umgerechnet. Damit werden die insgesamt recht abstrakten Größenordnungen – ganz im Sinne der Fokussierung des Überwachungsbarometers auf die reale Überwachungslast – weiter konkretisiert und auf die Perspektive der individuellen Grundrechtsträger quasi heruntergebrochen. Dies ist in den *Tabellen 13, 23, 33* und *43* konkretisiert. Demnach gab es beispielsweise im Jahr 2018 *an jedem Werktag*[88] durchschnittlich 73 TK-Überwachungsanordnungen und 110 Verkehrsdatenabfragen durch Strafverfolgungsbehörden, 309 an die FIU gerichtete Verdachtsanzeigen von Banken, 3.758 einfache Kontoabfragen und 205 Abfragen von Kundendaten durch verschiedene Behörden bei den drei betrachteten einbezogenen IT-Providern. Bereits dieser kleine Ausschnitt lässt die Überwachungslast in besonders anschaulicher Form erkennbar werden. Wenn in einem späteren Stadium Daten für deutlich mehr Überwachungsbereiche verfügbar sein werden, wird dies noch deutlich plastischer werden. Die einzelnen Tageswerte mitsamt ihrer unterschiedlichen Ausprägung können dann auch im Sinne eines fiktiven *individuellen Überwachungsrisikos* insgesamt und in den verschiedenen Kontexten verstanden werden. Alternativ kann die Betroffenheit bezogen auf 100.000 Einwohner ausgewiesen werden (*Tabellen 14, 24, 34, 44*); auch hier werden bezogen auf das Beispielsjahr 2018 die Unterschiede deutlich zwischen den Inzidenzwerten bei TKÜ-Anordnungen (28,1) und Kontoabfragen (1.353,8).

In Ergänzung zu diesen elementaren Auswertungsschritten, die einheitlich über alle Zugriffsdaten gelegt werden, können und sollen, abhängig von den verfügbaren Rohdaten, noch weitere punktuelle Detailanalysen vorgenommen werden. Dies betrifft in den hier ausgewählten exemplarischen Bereichen beispielsweise die Art der Daten oder auch die Verteilung einzelner Maßnahmen im Behörden- und Ländervergleich. So lässt sich etwa anhand der statistischen Daten zur Abfrage retrograder Daten erkennen, dass die Zahl entsprechender Abfragen im Anschluss an das Urteil des Bundesverfassungsgerichts aus dem Jahr 2010 nur kurzzeitig zurückging. Bereits 2012 lag die Zahl bereits wieder über derjenigen von 2009 *(Tabelle 10a)* und nur in jedem vierten Fall waren die Daten zuletzt (2019) nicht mehr verfügbar *(Tabelle 10b)*. Für weitere aufschlussreiche Beispiele siehe *Schaubilder 11a/b, 31* und *32*.

88 Berechnet auf der Basis von durchschnittlich 250 Behördenarbeitstagen.

Beispiel 1: Entwicklung der Telekommunikationsüberwachung – Verkehrs- und Inhaltsdaten –
(nur Strafverfolgung, vgl. Überwachungsschema Tabelle 01: Nr. 2a u. 3a)

Tabelle 10a | Art der abgefragten Verkehrsdaten*

		2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Retrograde Daten[1]	N	13.240	15.341	11.156	12.711	16.172	18.987	20.070	23.981	23.285	21.240	20.509	23.959
	%	95,2	94,5	88,7	89,8	91,9	90,7	88,4	88,3	87,9	89,8	88,6	87,4
Künftig anfallende Daten[2]	N	664	885	1.420	1.442	1.427	1.936	2.631	3.183	3.219	2.400	2.634	3.446
	%	4,8	5,5	11,3	10,2	8,1	9,3	11,6	11,7	12,1	10,2	11,4	12,6

*) Datenquelle: Jahresstatistiken Bundesamt für Justiz.

1) Abfragen können neben retrograden zusätzlich auch künftig anfallende Daten umfassen.
2) Abfragen ausschließlich künftig anfallender Daten.

Tabelle 10b | Erfolglose Abfragen wegen Nichterreichbarkeit von Daten*

		2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Daten ganz oder teilweise nicht (mehr) verfügbar	N	931	558	1.937	2.442	3.738	3.330	3.355	3.568	2.783	4.915	8.538	7.569
	%	7,0	3,6	17,4	19,2	23,1	17,5	16,7	14,9	12,0	23,1	36,9	27,6

*) Datenquelle: Jahresstatistiken Bundesamt für Justiz.

Tabelle 11 | Veränderungen p.a. (Zu-/Abnahme in Prozent, bezogen auf das jew. Vorjahr)

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	*2009 –2019*
§ 100a StPO insgesamt (TKÜ)	23,7	0,4	3,3	9,2	-0,6	2,0	-3,4	-5,5	-12,7	4,4	-6,4	*10,7*
§ 100g StPO insgesamt (Verkehrsdaten)	16,7	-22,5	12,6	24,3	18,9	8,5	19,7	-2,4	-11,5	-2,1	18,4	*97,1*

Rückgang > 20 % ■, > 10 % ■ | Zunahme >10 % ■, >20 % ■.

Tabelle 12 | Gesamtentwicklung der Anordnungen (kumulierte Prozent*)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
§ 100a StPO insgesamt (TKÜ)	100	124	124	128	140	139	142	137	130	113	118	111
§ 100g StPO insgesamt (Verkehrsdaten)	100	117	90	102	127	150	163	195	191	170	166	197

*) 2008 = 100 %.

Tabelle 13 | Durchschnittliche Anzahl der Anordnungen pro Tag*

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
§ 100a StPO insgesamt (TKÜ)	66	81	82	84	92	92	94	90	85	75	78	73
Erstanordnungen	56	69	70	72	78	78	79	74	70	63	63	62
Verlängerungs-anordnungen	10	12	12	12	14	14	15	16	15	12	15	11
§ 100g StPO insgesamt (Verkehrsdaten)	56	65	50	57	70	84	91	109	106	95	93	110
Erstanordnungen	54	63	49	55	68	81	88	105	103	92	90	106
Verlängerungs-anordnungen	2	2	1	2	2	3	3	4	3	3	3	4

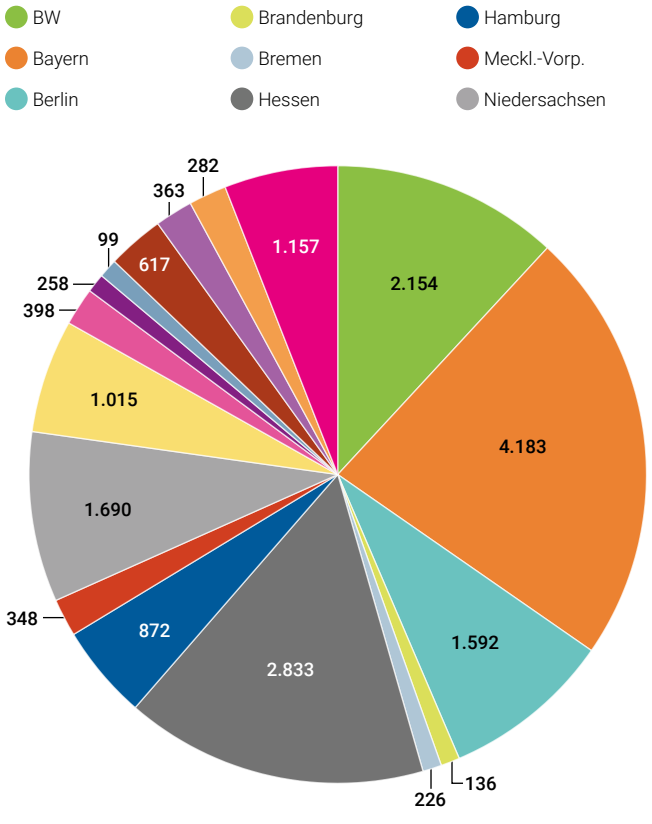
*) Berechnungsgrundlage: 250 Behördenarbeitstage. Nach vollen Zahlen auf- bzw. abgerundet.

Tabelle 14 | Anzahl der Anordnungen pro 100.000 Einwohnern*

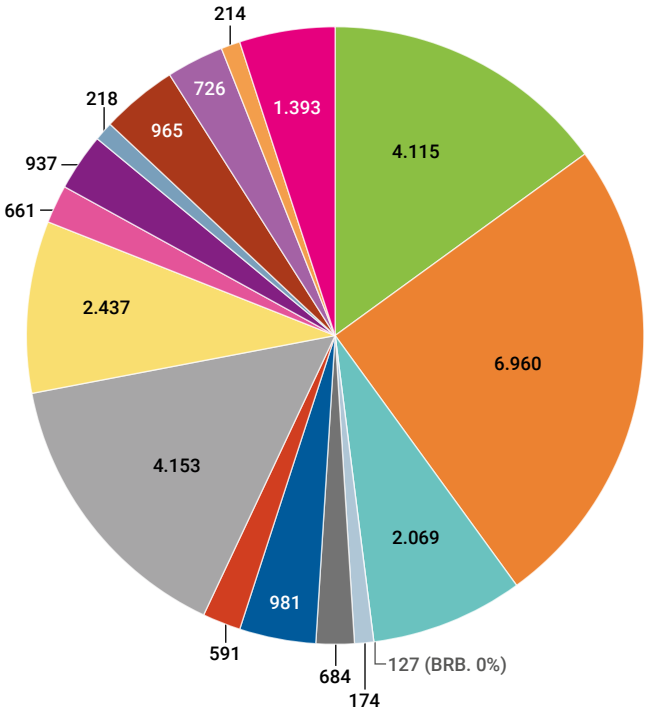
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
§ 100a StPO insgesamt (TKÜ)	24,1	29,8	29,9	31,4	34,2	33,9	34,3	32,8	30,9	26,9	28,1	26,2
§ 100g StPO insgesamt (Verkehrsdaten)	20,4	23,8	18,4	21,1	23,1	30,9	33,3	39,5	38,4	34,1	33,3	39,4

*) Bezugsgröße: Gesamtbevölkerung ab 18 Jahre; Quelle: Stat. Bundesamt.

Schaubild 11a/b | TKÜ-Anordnungen i.S.v. § 100a StPO nach Bundesländern



Verkehrsdatenabfragen i.S.v. § 100g StPO nach Bundesländern (jew. 2019)



Beispiel 2: Entwicklung der proaktiven Verdachtsanzeigen der privaten Verpflichteten an die FIU im Rahmen der Geldwäschekontrolle

(vgl. Überwachungsschema Tabelle 01: Nr. 7a/b)

Tabelle 21 | Veränderungen p.a. (Zunahmen in Prozent, bezogen auf das jew. Vorjahr)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	*2010 – 2019*
Verdachtsanzeigen	20	15,6	14,5	33,7	25,4	23,2	42,5	31,2	29,1	48,8	*1.078*

Tabelle 22 | Gesamtentwicklung der Fallzahlen (kumulierte Prozent*)

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Verdachtsanzeigen	100	120	139	159	212	266	328	467	613	792	1.178

*) 2008 = 100 %.

Tabelle 23 | Durchschnittliche Anzahl der Verdachtsanzeigen pro Tag*

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Verdachtsanzeigen	38	47	54	62	83	104	128	182	239	309	460

*) 2008 = 100 %.

Tabelle 24 | Anzahl der Anzeigen pro 100.000 Einwohnern*

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Verdachtsanzeigen	14,3	17,1	20,2	23,0	30,6	38,2	46,5	60,0	86,4	111,3	165,4

*) 2008 = 100 %.

Beispiel 3: Entwicklung der behördlichen Kontoabfragen
(ohne Nachrichtendienste, vgl. Überwachungsschema: Nr. 8a)

Tabelle 31 | Veränderungen p.a. (Zunahmen in Prozent, bezogen auf das jew. Vorjahr)

	2006	2007	2008	2009	2010	2011	2012	2013	2014
Insgesamt	47,0	13,7	-3,1	14,8	20,3	9,7	3,9	42,8	36,3
§ 93 Abs. 7 AO[1]	147,8	8,5	14,8	18,3	30,2	9,3	16,1	11,4	16,1
§ 93 Abs. 8 AO[2]	-	8,0	582,5	173,8	40,9	-0,2	11,7	704,1	106,6
§ 24c KWG[3]	30,0	15,3	-10,3	9,5	15,0	10,7	-0,1	7,3	12,3

	2015	2016	2017	2018	2019	*2006-19*
Insgesamt	21,0	23,6	67,3	13,3	-	*1.194*
§ 93 Abs. 7 AO[1]	22,5	1,3	69,1	17,2	-	*1.822*
§ 93 Abs. 8 AO[2]	35,6	26,8	102,4	14,4	-	*209.869*
§ 24c KWG[3]	-2,8	2,4	-0,2	4,4	30,6	*199*

Rückgang > 10 %, < 10 % | Zunahme >10 %, >20 %, >30 %, >50, > 100, 500 u. mehr.

Tabelle 32 | Gesamtentwicklung der Fallzahlen (kumulierte Prozent*)

	2005	2006	2007	2008	2009	2010	2011	2012	2013
Insgesamt	100	147	167	162	189	223	245	254	364
§ 93 Abs. 7 AO[1]	100	248	269	309	366	476	520	604	673
§ 93 Abs. 8 AO[2]	-	100	108	737	2.019	2.845	2.840	3.173	25.522
§ 24c KWG[3]	100	130	150	134	147	169	187	183	197

	2014	2015	2016	2017	2018	2019
Insgesamt	496	601	682	1.142	1.294	-
§ 93 Abs. 7 AO[1]	781	969	957	1.640	1.922	-
§ 93 Abs. 8 AO[2]	52.735	71.510	90.669	183.515	209.969	-
§ 24c KWG[3]	221	215	220	219	229	299

*) 2005(2006) = 100 %. § 93 Abs. 8 AO in Kraft seit April 2005.

1) Abfrage durch Finanz- und Zollbehörden.
2) Abfrage durch Polizei-, Verwaltungs-, Sozialbehörden und Gerichtsvollzieher.
3) Abfrage durch Strafverfolgungsbehörden, Finanzbehörden (Steuerfahndung etc.), Zollbehörden, u.a.

Tabelle 33 | Durchschnittliche Anzahl der Kontoabfragen pro Tag*

	2005	2006	2007	2008	2009	2010	2011	2012	2013
Insgesamt	290	427	485	470	540	649	712	740	**1.057**
§ 93 Abs. 7 AO[1]	41	101	110	126	149	194	212	247	275
§ 93 Abs. 8 AO[2]	0	1	1	8	23	33	32	36	292
§ 24c KWG[3]	250	325	374	336	368	422	468	457	491

	2014	2015	2016	2017	2018	2019
Insgesamt	1.441	1.744	1.982	**3.316**	3.758	-
§ 93 Abs. 7 AO[1]	319	391	396	669	784	-
§ 93 Abs. 8 AO[2]	603	848	**1.032**	**2.099**	2.402	-
§ 24c KWG[3]	551	536	549	547	572	746

	2005	2006	2007	2008	2009	2010	2011	2012	2013
Insgesamt	290	427	485	470	540	649	712	740	1.057
§ 93 Abs. 7 AO[1]	41	101	110	126	149	194	212	247	275
§ 93 Abs. 8 AO[2]	0	1	1	8	23	33	32	36	292
§ 24c KWG[3]	250	325	374	336	368	422	468	457	491

	2014	2015	2016	2017	2018	2019
Insgesamt	1.441	1.744	1.982	3.316	3.758	-
§ 93 Abs. 7 AO[1]	319	391	396	669	784	-
§ 93 Abs. 8 AO[2]	603	848	1.032	2.099	2.402	-
§ 24c KWG[3]	551	536	549	547	572	746

Zunahme >200 , >300 , >400 , >500 , > 600 , > 700 , > 800 , > 1.000 , > 2.000 ,> 3.000

*) Berechnungsgrundlage: 250 Behördenarbeitstage. Nach vollen Zahlen auf- bzw. abgerundet. Hervorhebungen zeigen jeweils Übergänge in höhere 1.000er-Stufen an.

1) Abfrage durch Finanz- und Zollbehörden.
2) Abfrage durch Polizei-, Verwaltungs-, Sozialbehörden und Gerichtsvollzieher.
3) Abfrage durch Strafverfolgungsbehörden, Finanzbehörden (Steuerfahndung etc.), Zollbehörden, u.a.

Tabelle 34 | Anzahl der Kontoabfragen pro 100.000 Einwohnern*

	2005	2006	2007	2008	2009	2010	2011	2012	2013
Insgesamt	107,0	156,8	177,7	172,1	197,5	237,6	265,1	274,5	390,5
§ 93 Abs. 7 AO[1]	15,0	37,1	40,2	46,1	54,6	71,0	79,0	91,4	101,4
§ 93 Abs. 8 AO[2]	-	0,4	0,5	3,1	8,5	9,0	12,1	13,5	107,8
§ 24c KWG[3]	91,9	119,2	137,1	122,9	134,5	154,4	174,0	169,6	181,2

	2014	2015	2016	2017	2018	2019
Insgesamt	529,2	633,4	717,5	1.197,1	1.353,3	-
§ 93 Abs. 7 AO[1]	117,1	141,8	143,3	214,6	282,5	-
§ 93 Abs. 8 AO[2]	221,5	297,1	375,5	758,0	865,0	-
§ 24c KWG[3]	202,3	194,6	198,7	197,6	205,8	268,5

*) Bezugsgröße: Gesamtbevölkerung ab 18 Jahre; Quelle: Stat. Bundesamt.

Tabelle 35 | Interne Zuordnung der Fälle (prozentuale Anteile per Kalenderjahr)

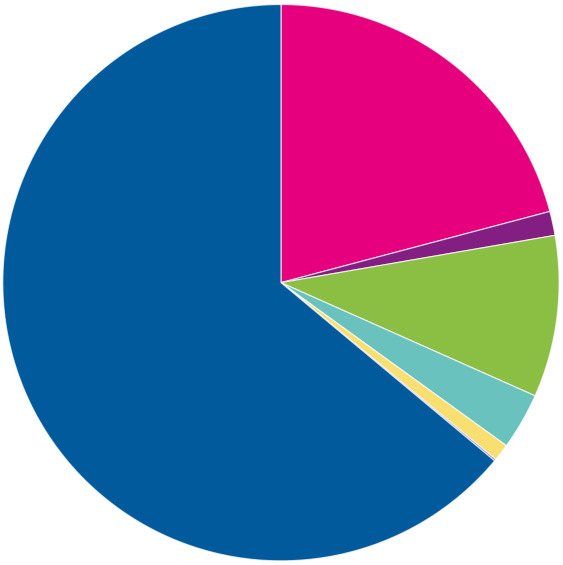
	2005	2006	2007	2008	2009	2010	2011	2012	2013
Insgesamt	14,0	23,7	22,6	26,8	27,6	29,9	29,8	33,3	26,0
§ 93 Abs. 7 AO[1]	0,0	0,3	0,3	1,8	4,3	5,0	4,6	4,9	27,6
§ 93 Abs. 8 AO[2]	86,0	76,0	77,1	71,4	68,1	65,1	65,6	61,8	46,4
§ 24c KWG[3]	91,9	119,2	137,1	122,9	134,5	154,4	174,0	169,6	181,2

	2014	2015	2016	2017	2018
Insgesamt	22,1	22,4	20,0	20,2	20,9
§ 93 Abs. 7 AO[1]	42,9	46,9	52,3	63,3	64,0
§ 93 Abs. 8 AO[2]	38,2	30,7	27,7	16,5	15,1
§ 24c KWG[3]	202,3	194,6	198,7	197,6	205,8

1) Abfrage durch Finanz- und Zollbehörden.
2) Abfrage durch Polizei-, Verwaltungs-, Sozialbehörden und Gerichtsvollzieher.
3) Abfrage durch Strafverfolgungsbehörden, Finanzbehörden (Steuerfahndung etc.), Zollbehörden, u.a.

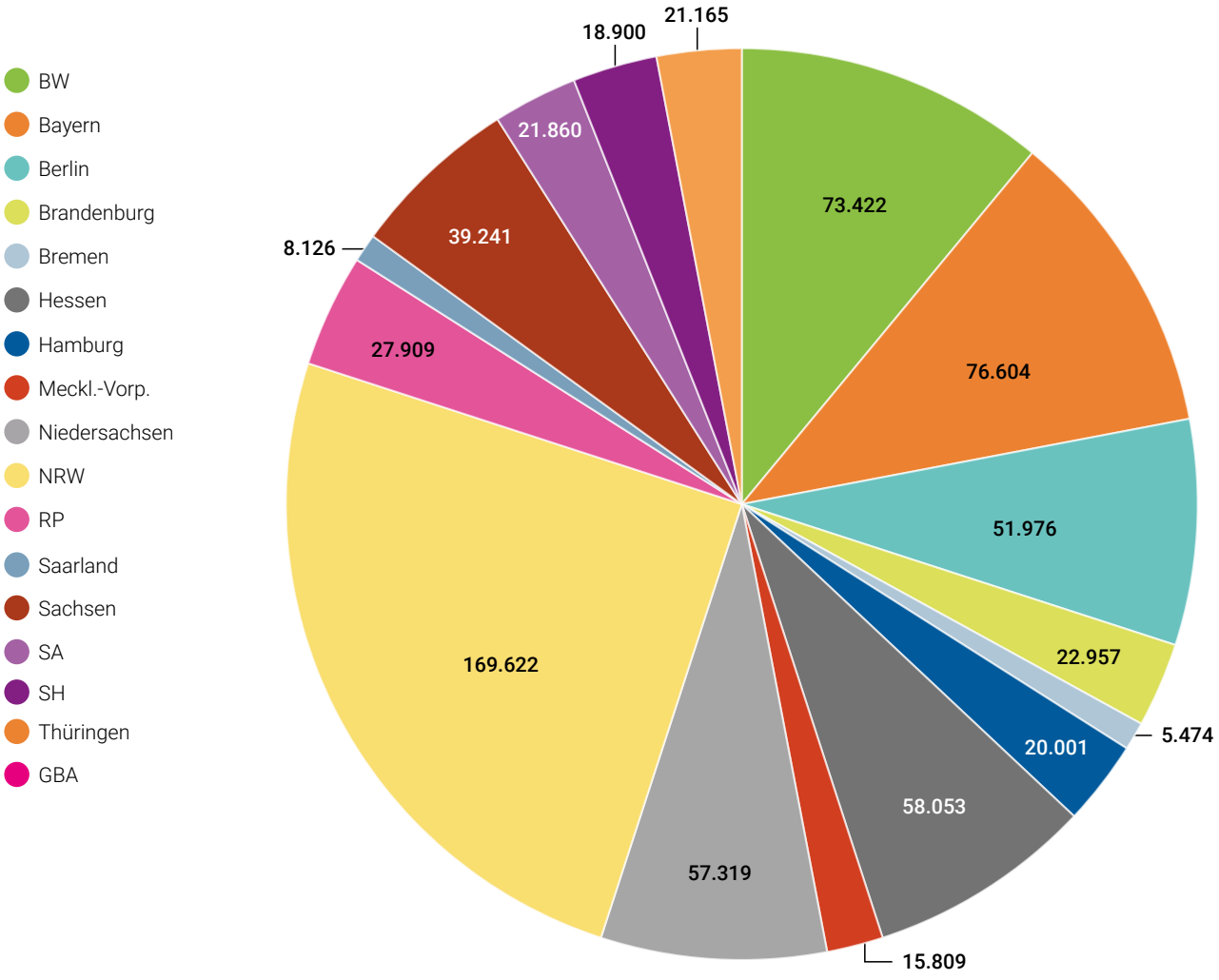
Schaubild 31 | Flächendiagramm interne Verteilung im Detail (2018)*

Finanzbehörden	196.088	20,9 %
Finanzbehörden (Steuerfahndung etc.)	13.249	1,4 %
Polizeibehörden	87.931	9,4 %
Staatsanwaltschaften	30.671	3,3 %
Zollbehörden	9.645	1,0 %
BaFin	877	0,1 %
sonstige Behörden u. Gerichtsvollzieher	601.027	64,0 %



*) Bezugsgröße: Gesamtbevölkerung ab 18 Jahre; Quelle: Stat. Bundesamt.

Schaubild 32 | Verteilung nach Bundesländern (2018)*



*) Nur Abfragen gem. § 93 Abs. 7 u. 8 AO; verwertbare Angaben aus 86 % aller Fälle (N = 688.438); BT-Drucks. 19/9177, S. 2.

Beispiel 4: Entwicklung der behördlichen Abfragen bei IT-Providern

(rechtliche Zuordnung der Abfragen und Kategorisierung der abgefragten Daten im gegenwärtigen Stadium noch nicht möglich)

Tabelle 40 | Behördliche Auskunftsersuchen bei drei marktführenden IT-Providern* betreffend Nutzer- bzw. Inhaltsdaten

	2013	2014	2015	2016	2017	2018	2019	*2013-2019*
Microsoft	10.389	9.375	8.433	7.713	6.854	5.924	7.084	*55.772*
Apple	6.344	13.999	21.852	25.010	27.108	29.356	30.158	*153.827*
Google	4.971	6.452	11.394	18.713	14.741	15.976	21.171	*93.418*
Insgesamt	21.704	29.826	41.679	51.436	48.703	51.256	58.413	*303.017*

Datenquellen: Transparenzberichte/Law Enforcement Reports der betroffenen Unternehmen.

*) Amazon hat erstmals für das 2. Halbjahr 2020 länderspezifische Daten veröffentlicht. Danach wurden von deutschen Behörden insgesamt 11.779 Auskunftsersuchen zugestellt, davon 44 bezogen auf cloud-gespeicherte Daten (1.7. – 31.12.2020); https://d1.awsstatic.com/certifications/Information_Request_Report_December_2020.pdf.
Die verfügbaren Daten aus früheren Zeiträumen sind nicht vergleichbar; www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF.

Tabelle 41 | Veränderungen p.a. (Zu-/Abnahmen in Prozent, bezogen auf das jew. Vorjahr)

	2013	2014	2015	2016	2017	2018	2019	*2014-2019*
Microsoft	-9,8	-10,0	-8,5	-11,1	-13,6	19,6	-31,8	*55.772*
Apple	120,7	56,1	14,5	8,4	8,3	2,7	375,3	*153.827*
Google	29,8	76,6	64,2	-21,2	8,4	32,5	325,9	*93.418*
Insgesamt	37,4	39,7	23,4	-5,3	5,2	14,0	169,1	*303.017*

Tabelle 42 | Gesamtentwicklung der Fallzahlen (kumulierte Prozent*)

	2013	2014	2015	2016	2017	2018	2019
Microsoft	100	90	81	74	66	57	68
Apple	100	220	344	394	427	463	475
Google	100	130	229	376	297	321	426
Insgesamt	100	137	192	237	224	236	269

*) 2013 = 100 %.

Tabelle 43 | Durchschnittliche Anzahl der Anfragen bei den drei Unternehmen pro Tag*

	2013	2014	2015	2016	2017	2018	2019
Microsoft	42	38	34	31	27	24	28
Apple	25	56	87	100	108	117	121
Google	20	26	46	75	59	64	85
Insgesamt	87	119	167	206	195	205	234

*) Berechnungsgrundlage: 250 Behördenarbeitstage. Nach vollen Zahlen auf- bzw. abgerundet.

Tabelle 44 | Anzahl der Anfragen pro 100.000 Einwohnern*

	2013	2014	2015	2016	2017	2018	2019
Microsoft	15,3	13,8	12,2	11,2	9,9	8,5	10,2
Apple	9,4	20,6	31,7	36,2	39,1	42,3	43,4
Google	7,3	9,5	16,5	27,1	21,3	23,0	30,5
Insgesamt	32,1	43,8	60,5	74,5	70,3	73,8	84,5

*) Bezugsgröße: Gesamtbevölkerung ab 18 Jahre; Quelle: Stat. Bundesamt.

Tabelle 45 | Interne Verteilung der Fälle auf die Unternehmen (prozentuale Anteile per Kalenderjahr)

	2013	2014	2015	2016	2017	2018	2019
Microsoft	47,9	31,4	20,2	15,0	14,1	11,6	12,1
Apple	29,2	46,9	52,4	48,6	55,7	57,3	51,6
Google	22,9	21,6	27,3	36,4	30,3	31,2	36,2

5. Zukunftsperspektive: Weiterentwicklung und Implementation

Die Idee der Einrichtung eines periodischen Überwachungsbarometers als politisch unabhängiges, wissenschaftlich basiertes Langzeitvorhaben hat bereits einige Zustimmung erfahren. Unterstützend hat sich unter anderem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit geäußert.[89] Der Koalitionsvertrag der neuen Bundesregierung hebt die Bedeutung der Überwachungs-Gesamtrechnung für eine vorausschauende, evidenzbasierte und grundrechtsorientierte Sicherheits- und Kriminalpolitik ebenfalls hervor.[90] Die erstmalige Implementation des kompletten Überwachungsbarometers sowie seine Administration und Weiterführung sind längerfristige Aufgaben, deren personeller und finanzieller Ressourcenbedarf den einer auf zeitnahe Ergebnisse ausgerichteten explorativen Studie deutlich übersteigt. Das entwickelte Konzept bringt erheblichen Arbeitsaufwand mit sich und erfordert eine auf einen längeren Zeitraum angelegte vertragliche Grundlage, ausreichende finanzielle Ressourcen sowie verlässlichen administrativen Support durch die datenführenden Behörden, ggf. auch in förmlicher Kooperation.

Der qualitative Teil des Barometers (Berechnung der Intensitätswerte) kann kurzfristig und ohne zeitliche Zäsur bereits im nächsten Arbeitsschritt flächendeckend für alle in *Tabelle 01* erfassten Überwachungsszenarien durchgeführt werden. Die konkreten Basiswerte müssten dann kontinuierlich überprüft und für jeden neuen Berichtszeitraum gegebenenfalls aktualisiert werden, um zwischenzeitliche Veränderungen der rechtlichen und technischen Rahmenbedingungen entsprechend einzuordnen.

Das Spektrum der berechenbaren endgültigen Überwachungsindizes wird sich mit dem Anwachsen des verfügbaren Datenbestandes kontinuierlich erweitern.

In der Anfangszeit können Längsschnittanalysen der Entwicklung im vergangenen Zehnjahreszeitraum erst mit zeitlicher Verzögerung präsentiert werden. Dies betrifft beispielsweise die auf der Grundlage der neuen polizeigesetzlichen Bestimmungen erhobenen Daten.

Das Konzept ist, wie eingangs erwähnt, so angelegt, dass es inhaltlich erweitert werden kann. Perspektivisch könnte ein EU-weites Anschlussprojekt entwickelt werden. Entsprechendes Interesse könnte etwa in den Fachgremien des Europaparlaments erwartet werden sowie auf mitgliedsstaatlicher Ebene – jedenfalls in den Ländern, die auch sonst auf umfassende Transparenz der staatlichen Verwaltungspraxis setzen. Ein zusätzlicher Mehrwert einer solchen Erweiterung könnte sich auch daraus ergeben, dass eine bessere Datenlage in einigen Mitgliedsstaaten Vorbildcharakter haben und möglicherweise sogar mit zu einer Beschleunigung beim Ausbau der Berichtspflichten in Deutschland beitragen könnte.

Intensiver untersucht werden soll im weiteren Verlauf des Projektes schließlich die noch nicht umfassend geklärte rechtliche Einordnung der Informations- und Berichtspflichten der Sicherheitsbehörden gegenüber der Legislative und der Öffentlichkeit, deren Notwendigkeit das Bundesverfassungsgericht wie beschrieben unmittelbar aus dem Grundsatz der Verhältnismäßigkeit ableitet.[91] Ob und wie sich darüber hinaus auch aus den (einfach-)gesetzlichen Informationsansprüchen weitergehende Berichtspflichten zu den hier im Fokus stehenden sicherheitsbehördlichen Maßnahmen ableiten lassen, von denen auch das Überwachungsbarometer profitieren könnte, wird dabei zu diskutieren sein.

Das Überwachungsbarometer einschließlich der Kartographie soll der interessierten Öffentlichkeit leicht zugänglich sein. Sobald validierte Daten und weitere Informationen verfügbar sind, sollen diese in einer webbasierten Datenbank[92] zur Verfügung gestellt werden.

Abschließend ist noch einmal auf die Zielsetzung des Vorhabens und seinen daraus resultierenden spezifischen Aussagewert hinzuweisen. Das Überwachungsbarometer versteht sich, wie oben dargestellt, als Instrument zur objektiven Darstellung der Überwachungssituation in einem bestimmten Zeitraum nach klar definierten (grund-)rechtlichen und empirischen Kriterien. Ziel ist *nicht* die qualitative Bewertung einzelner Maßnahmen. Hierfür wäre die Erhebung sensibler personenbezogener Informationen erforderlich – was gerade nicht beabsichtigt ist (und abgesehen davon auch gar nicht möglich wäre). Inhaltlicher Bezugspunkt ist mithin stets (und ausschließlich) der abstrakte rechtliche Rahmen der untersuchten Maßnahmen und ihre Häufigkeit, *bezogen auf die Gesamtbevölkerung*. Aussagen zur spezifischen Betroffenheit bestimmter Bevölkerungsgruppen können auf der zur Verfügung stehenden Datengrundlage nicht getroffen werden. Das schließt jedoch keineswegs aus, dass die Daten des Überwachungsbarometers – gerade wegen ihrer objektiven wissenschaftlichen Evidenz – die rechtspolitische Diskussion um Überwachungsarten und -routinen befruchten und intensivieren werden.

89 Siehe beispielsweise die Stellungnahme zur öffentlichen Anhörung des Bundestagsausschusses für Inneres und Heimat vom 22. Februar 2021, Drucksache 19(4)732 A.

90 Siehe S. 108 des Koalitionsvertrags zwischen SPD, Bündnis 90/Die Grünen und FDP (2021); abrufbar unter: https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800 [letzter Zugriff am 03.01.2022].

91 Siehe oben Fn. 72.

92 Künftig abrufbar unter: https://www.ueberwachungsbarometer.de/.

6. Rechtspolitische Forderungen

Die Einrichtung und erfolgreiche Implementation des Überwachungsbarometers im Sinne des hier vorgelegten Konzepts kann – und sollte – durch die Rechtspolitik unterstützend flankiert werden. Der Zeitpunkt ist günstig, da sich im Hinblick auf die neuere Rechtsprechung des Bundesverfassungsgerichts zu der verfassungsrechtlichen Bedeutung der Dokumentationspflichten ohnehin gesetzgeberischer und organisatorischer Handlungsbedarf ergibt. Neben einer verlässlichen Unterstützung der verantwortlichen Akteure in den betreffenden Behördenzweigen auf Bundes- und Länderebene beim Datenzugang erscheint diesbezüglich auch eine Hilfestellung der Gesetzgeber im Hinblick auf einen Datenzugang dringlich. Die derzeit existierenden Forschungsklauseln sind insoweit nur eine Hilfslösung, die keine flächendeckende Erfassung aller interessierenden Daten garantiert.

Unterstützung für das Projekt kann auf der Ebene der Parlamente, jedenfalls für eine Übergangszeit, ergänzend dadurch geleistet werden, dass statistisch bislang nicht erfasste Überwachungssachverhalte mit dem Instrument der parlamentarischen Anfragen regelmäßig näher beleuchtet werden. Die Ergebnisse könnten dann wiederum in den Datenpool des Überwachungsbarometers einfließen.

Auf legislativer Ebene erscheinen die folgenden Punkte vordringlich:

- → Erweiterung der Informationspflichten bei präventiv-polizeilichen Anwendungen auf alle potenziell relevanten Zugriffstatbestände;
- → ihre sachliche Vereinheitlichung, um eine Vergleichbarkeit der statistischen Daten zur Anwendungshäufigkeit sicherzustellen, dies betrifft etwa die Art der Daten, den Turnus der Veröffentlichung von Daten und die Verfügbarmachung als solche;
- → soweit erforderlich ein Umstieg auf einen einheitlichen Ein-Jahres-Turnus; gerade der Bundesgesetzgeber agiert hier im Hinblick auf das Bundeskriminalamtsgesetz (BKAG) und die ursprünglich geplante Novellierung des Bundespolizeigesetzes (BPolG) mit der 2-Jahres-Frist zögerlicher als zahlreiche Bundesländer; nachdem zuletzt keine Zustimmung des Bundesrates erreicht werden konnte, eröffnet sich die Chance für eine entsprechende Anpassung in der kommenden Legislaturperiode;
- → Erweiterung der Informationspflichten auch im repressiven Anwendungsbereich;
- → inhaltliche Erweiterung der Statistikklauseln um einige grundlegende inhaltliche Parameter, die die Bewertung der Erhebungspraxis erleichtern würden; Vorbild könnten hier beispielsweise § 107 SächsPVDG oder partiell auch § 101b StPO sein; beide enthalten zumindest Anlass, Zweck, Dauer und Ergebnis der betroffenen Maßnahmen sowie die Benachrichtigung der Betroffenen und die Löschung der personenbezogenen Daten sowie ergänzend weitere inhaltliche Kriterien;
- → bessere Transparenz: In einigen Bundesländern ist teilweise detektivische Recherchearbeit notwendig, um Daten zu finden, die auf der Grundlage bereits existierender Statistikklauseln erhoben wurden; eine zentrale Bereitstellung über das GovData-Portal (ggf. zusätzlich zu anderen Bereitstellungsorten) wäre anzustreben;
- → generell sollte überall dort, wo Informationspflichten oder Statistikklauseln bestehen, auch eine explizite Bestimmung für den einfachen Datenzugang für Forschungszwecke ergänzt werden;
- → Ergänzung von Forschungsklauseln auch in anderen Sachbereichen, die aktuell noch keine entsprechende Regelung kennen; gegebenenfalls wäre über eine universelle gesetzliche Regelung zu denken, die alle potenziell relevanten Bereiche abdeckt;
- → im Übrigen könnten nicht nur das Überwachungsbarometer, sondern die wissenschaftliche Evaluationsforschung insgesamt von einer Verständigung im Rahmen der Innen- und Justizministerkonferenz auf einheitliche oder jedenfalls vergleichbare Standards bei der statistischen Erfassung präventiver und repressiver (Überwachungs-)Maßnahmen profitieren.

Auf der Ebene der politischen Diskussion sind die folgenden Punkte wünschenswert:

- → Vor der Diskussion über neue sicherheitsrechtliche Befugnisse, die die massenhafte Erhebung oder den Zugriff auf Daten betreffen, sollten zunächst bestehende Befugnisse betrachtet und evaluiert werden und in den Gesamtkontext bereits bestehender Überwachungsbefugnisse eingeordnet werden;
- → in die Diskussion über die verfassungsrechtliche Zulässigkeit und Intensität neuer Eingriffsbefugnisse sollten stets auch die statistischen Daten über die Anwendungshäufigkeit mit einbezogen werden;
- → das vertrauensstiftende Element für staatliches Handeln, welches durch eine transparente Auswertung der Befugnisse und ihrer Anwendung geschaffen wird, sollte parteiübergreifend anerkannt und als wichtiger Wert in sicherheitspolitischen Debatten begriffen werden;
- → die Bedeutung einer unabhängigen wissenschaftlichen Auswertung durch Vorhaben wie das geplante Überwachungsbarometer, sollte anerkannt und politisch unterstützt werden.

Literaturverzeichnis

Adensamer, Angelika (Hrsg.):
[österr.] Handbuch Überwachung. Wien 2020.

Adensamer, Angelika: Aspekte einer Überwachungs-Gesamtrechnung, FIfF-Kommunikation 4/19, S. 25–28.

Albrecht, Hans-Jörg/Kilchling, Michael:
Die Überwachung von Telekommunikations-Verkehrsdaten, MPG-Jahrbuch 2008.

Albrecht, Hans-Jörg, et al.; Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Freiburg i. Br. 2011.

Albrecht, Hans-Jörg/Poscher, Ralf: Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes. BT-Drucksache 18/13031 v. 23.06.2017.

Attendorn, Thorsten: Beck'scher TKG-Kommentar, hrsg. von Geppert, Martin/Schütz, Raimund, 4. Aufl., München 2013 (zit. als Bearbeiter in Attendorn).

Bäcker, Matthias: § 28, in Herdegen, Matthias/Masing, Johannes/Poscher, Ralf/Gärditz, Klaus Ferdinand (Hrsg.), Handbuch Verfassungsrecht: Darstellung in transnationaler Perspektive, München 2021.

Bäcker, Matthias: Strategische Telekommunikationsüberwachung auf dem Prüfstand, K&R 2014, S. 556–561.

Bieker, Felix/Bremert, Benjamin/Hagendorff, Thilo:
Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden 2018, S. 139–150.

Bieker, Felix/Bremert, Benjamin: Rote Linien im Sand, bei Sturm: Die Überwachungs-Gesamtrechnung, FIfF-Kommunikation 2019(4), S. 34–37.

Biermann, Kai: BND speichert 220 Millionen Telefondaten – jeden Tag; www.zeit.de/digital/datenschutz/2015-01/bnd-nsa-metadaten-ueberwachung/komplettansicht [letzter Zugriff am 10.12.2021].

Braun, Frank/Albrecht, Florian: Der Freiheit eine Gasse? Anmerkungen zur „Überwachungsgesamtrechnung" des Bundesverfassungsgerichts, Verwaltungsrundschau 2017, S. 151–155.

Desoi, Monika/Knierim, Antonie: Intimsphäre und Kernbereichsschutz, DÖV 2011, S. 398–405.

Dünkel, Frieder/Geng, Bernd: Die Entwicklung von Gefangenenraten im nationalen und internationalen Vergleich – Indikator für Punitivität? Developments of prison rates in comparative perspective – indicators for punitivity? Soziale Probleme, 24 (2013), S. 42–65, www.ssoar.info/ssoar/handle/document/44118 [letzter Zugriff am 10.12.2021].

Hornung, Gerrit/Schnabel, Christoph: Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, Deutsches Verwaltungsblatt 2010, S. 824–833.

Huber, Bertold: Das BVerfG und die Ausland-Ausland-Fernmeldeaufklärung des BND, NVwZ-Beilage 2020, S. 3–9.

Kilchling, Michael: Die Neuregelung zur Auslandskopfüberwachung gemäß § 4 TKÜV auf dem verfassungsrechtlichen Prüfstand. Gutachten im Auftrag des VATM. Freiburg i.Br. 2006.

Körner, Thomas/Krause, Anja/ Ramsauer Kathrin: Anforderungen und Perspektiven auf dem Weg zu einem künftigen Registerzensus, in Statistisches Bundesamt (Hrsg.), WISTA, Sonderheft Zensus 2021 (2019), S. 74–87, www.destatis.de/DE/Methoden/WISTA-Wirtschaft-und-Statistik/2019/07/anforderungen-perspektiven-registerzensus-072019.pdf?__blob=publicationFile [letzter Zugriff am 10.12.2021].

Lisken, Hans/Denninger, Erhard: Handbuch des Polizeirechts, 6. Aufl., München 2018 (zit. als Bearbeiter in Lisken/Denninger).

Löffelmann, Markus: Der Schutz grundrechtssensibler Bereiche im Sicherheitsrecht, Zeitschrift für das gesamte Sicherheitsrecht 2019, S. 190–196.

Löffelmann, Markus: Die Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung – Schema oder Struktur? Zeitschrift für das gesamte Sicherheitsrecht 2019, S. 16–22.

Marxsen, Christian: Strategische Fernmeldeaufklärung – Neuerungen in den Kompetenzen des Bundesnachrichtendienstes, DÖV 2018, S. 218–229.

Moser-Knierim, Antonie: Vorratsdatenspeicherung. Zwischen Überwachungsstaat und Terrorabwehr, Wiesbaden 2014.

Pohle, Jörg: Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung. Ein Alternativvorschlag. FIfF-Kommunikation 4/19, S. 37–42.

Poscher, Ralf: Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in Gander, Hans-Helmuth, et al. (Hrsg.), Resilienz in der offenen Gesellschaft, Baden-Baden 2012, S. 167–190.

Poscher, Ralf: The Right to Data Protection, in Miller, Russell A. (ed.), Privacy and Power, Cambridge 2017, S. 129–142.

Poscher, Ralf: Artificial Intelligence and the Right to Data Protection, Max Planck Institute for the Study of Crime, Security and Law, Working Paper No. 2021/03, https://ssrn.com/abstract=3769159 [letzter Zugriff am 10.12.2021].

Reporter ohne Grenzen: Rangliste der Pressefreiheit 2020: Fragebogen, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Ranglisten/Rangliste_2020/Fragebogen_Rangliste_der_Pressefreiheit_2020_-_RSF.pdf [letzter Zugriff am 10.12.2021].

Reporter ohne Grenzen: Rangliste der Pressefreiheit 2020: Methodische Hinweise zur Erstellung, Reporter ohne Grenzen, 2020, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Ranglisten/Rangliste_2020/Methodik_Rangliste_der_Pressefreiheit_2020_-_RSF.pdf [letzter Zugriff am 10.12.2021].

Reporter ohne Grenzen: Rangliste der Pressefreiheit 20201, www.reporter-ohne-grenzen.de/rangliste/rangliste-2021 [letzter Zugriff am 10.12.2021].

Reporter ohne Grenzen: Detailed methodology, https://rsf.org/en/detailed-methodology [letzter Zugriff am 10.12.2021];

Roßnagel, Alexander: Die „Überwachungs-Gesamtrechnung", Das BVerfG und die Vorratsdatenspeicherung, Neue Juristische Wochenschrift 2010, S. 1238–1242.

Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung, DuD-Fachbeiträge, 2018.

Roßnagel, Alexander/Moser-Knierim, Antonie/Schweda, Sebastian: Interessenausgleich im Rahmen der Vorratsdatenspeicherung: Analysen und Empfehlungen, Baden-Baden 2013.

Sapienzynska, Ewa/Lagos, Claudia: Media Freedom Indexes in Democracies: A Critical Perspective Through the Cases of Poland and Chile, International Journal of Communication 2016, S. 549–570.

Sieber, Ulrich: Die Auslandsübermittlung von Daten aus der strafprozessualen Telekommunikationsüberwachung, in: Haferkamp, Rita/Kilchling, Michael/Kinzig, Jörg/Oberwittler, Dietrich/Wössner, Gunda (Hrsg.): Unterwegs in Kriminologie und Strafrecht – Exploring the World of Crime and Criminology. Festschrift für Hans-Jörg Albrecht, Berlin 2021, S. 53–69.

Starnecker, Tobias: Videoüberwachung zur Risikovorsorge, Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse, Berlin 2016.

Stubenrauch, Julia: Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten. Baden-Baden 2009.

Tschohl, Christoph/Scheucher, Ewald/Kargl, Dieter/Luksan, Julia/Czadilek, Alexander/Waloschek, Herbert/Kreissl, Reinhard/Klinger, Kilian/Hötzendorfer, Walter/Möchel, Erich: HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze, epicenter.works 2016, https://epicenter.works/sites/default/files/heat_v1.2.pdf [letzter Zugriff am 10.12.2021].

United Nations Development Programme: Human Development Report 2020, The next frontier: Human development and the Anthropocene, 2020, http://hdr.undp.org/sites/default/files/hdr2020.pdf [letzter Zugriff am 10.12.2021].

Vogel, Benjamin/Maillart, Jean-Baptiste (eds.): National and International Anti-Money Laundering Law – Developing the architecture of criminal justice, regulation and data protection, Cambridge/Antwerpen/Chicago 2020.

Winkler, Daniela: Der „additive Grundrechtseingriff": Eine adäquate Beschreibung kumulierender Belastungen? Juristische Ausbildung 2014, 881–887.

Wissenschaftliche Dienste des Deutschen Bundestages: Gesetzgebung zur Speicherung von personenbezogenen Daten. Überblick über die gesetzlichen Regelungen seit dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 – 1 BvR 256/08 – zur Vorratsdatenspeicherung. WD 3 - 3000 - 089/16.

Wissenschaftliche Dienste des Deutschen Bundestages: Gesetzgebung zur Speicherung von personenbezogenen Daten. Aktualisierung des Sachstands WD 3 - 3000 - 089/16. WD 3 - 3000 - 427/18.

Wissenschaftliche Dienste des Deutschen Bundestages: Gesetzgebung zur Speicherung von personenbezogenen Daten. Aktualisierung des Sachstands WD 3 - 3000 - 427/18. WD 3 - 3000 - 126/21.

Schaubilder- und Tabellenverzeichnis

I. TABELLEN

II. SCHAUBILDER

Anhang

Tabelle 01: Übersicht über potenziell relevante Überwachungsszenarien[93,94]

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
1.	**TK-Bestandsdaten, §§ 95, 111 TKG**				
1a.		§ 100j Abs. 1 Nr. 1 StPO	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	Staatsanwaltschaft	Strafverfolgung
1b.		§ 40 BKAG	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	BKA	Gefahrenabwehr/Strafv.
1c.		§ 22a BPolG	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	Bundespolizei	Gefahrenabwehr
1d.		§ 52 PolG BW § 20a Abs. 1 Nr. 1 PolG NRW Art. 43 Abs. 5 BayPAG (usw.)[2]	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	L'Polizeibehörden	Gefahrenabwehr
1e.		§§ 8, 8a BVerfSchG (usw.)[2]	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	Dienste	Nachr. Aufklärung
1f.		§ 93 AO	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	Steuerbehörden	Besteuerungsverf.
1g.		§§ 10 Abs. 1, 30 Abs. 1 Nr. 1 u. Abs. 2 Nr. 1 ZFdG	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	Zollbehörden	AWG/KWKG-Ermittlungen, Bekämpfung Schwarzarbeit, u.a.
1h.		§ 112 Abs.1 S. 5, 7 TKG	Priv. Provider (§§ 3 Nr.3, 95, 111-113 TKG)	Netzagentur	weitere behördliche Zwecke
2.	**TK-Verkehrsdaten, §§ 96, 113b TKG**				
2a.		§ 110g StPO	Priv. Provider (§§ 3 Nr.30, 96, 113b TKG)	Staatsanwaltschaft	Strafverfolgung
2b.		§ 52 BKAG	Priv. Provider (§§ 3 Nr.30, 96, 113b/c TKG)	BKA	Gefahrenabwehr/Strafverf.
2c.		§ 53 PolG BW § 20a Abs. 1 Nr. 2 PolG NRW Art. 43 Abs. 2 BayPAG (usw.)	Priv. Provider (§§ 3 Nr.30, 96, 113b/c TKG)	L'Polizeibehörden	Gefahrenabwehr
2d.		§ 77 ZFdG	Priv. Provider (§§ 3 Nr.30, 96, 113b/c TKG)	Zollkriminalamt	AWG/KWKG-Sachen
2e.		§§ 8, 8a BVerfSchG (usw.)	Priv. Provider (§§ 3 Nr.30, 96, 113b/c TKG)	Dienste	Nachr. Aufklärung
3.	**TK-Inhaltsdaten (TKÜ)**				
3a.		§ 100a StPO	Staatsanwaltschaft	-	Strafverfolgung
3b.		§ 51 BKAG	BKA	-	Gefahrenabwehr/Strafv.
3c.		§ 54 PolG BW §§ 20c, 33 PolG NRW Art. 42, 44 BayPAG (usw.)	L'Polizeibehörden	-	Gefahrenabwehr
3d.		*§ 27d Abs, 1 (BPolGModG 2021, vgl. BT-Drucks. 19/26541)*	*Bundespolizei*	-	*Gefahrenabwehr*
3d.		§ 72 ZFdG	Zollbehörden	-	AWG/KWKG-Sachen
3f.		§ 1 G10-G	Dienste	-	Nachr. Aufklärung

93 Genereller Überblick über den aktuellen rechtlichen Status quo. In dem explorativen Stadium kann zunächst nur eine begrenzte Auswahl einbezogen werden.
94 Die aufgelisteten Rechtsgrundlagen (Stand: Frühjahr 2021) verweisen auf die jeweiligen Grundnormen und sind nicht abschließend zu verstehen. Die Angaben zu einschlägigen Landesgesetzen sind beispielhaft zitiert; Komplementärnormen existieren häufig auch in anderen Bundesländern.

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
4.	**Verschlüsselte TK-Inhaltsdaten (Quellen-TKÜ)**				
4a.		§ 100a Abs. 1 S. 2, 3 StPO	Staatsanwaltschaft	-	Strafverfolgung
4b.		§ 51 Abs. 2 BKAG	BKA	-	Gefahrenabwehr/Strafv.
4c.		§ 54 Abs. 2 PolG BW § 20c Abs. 2 PolG NRW Art. 42 Abs. 2 BayPAG (usw.)	L'Polizeibehörden	-	Gefahrenabwehr
4d.		*§ 27d Abs, 2 (BPolGModG 2021, vgl. BT-Drucks. 19/26541)*	*Bundespolizei*	-	*Gefahrenabwehr*
4e.		*Verfassungsschutzrecht-AnpassungsG-E 2020*	*Dienste*	-	*Nachr. Aufklärung*
5.	**Intern/extern gespeicherte Computerdaten (Online-Durchsuchung)**				
5a.		§ 100b StPO	Staatsanwaltschaft	-	Strafverfolgung
5b.		§ 49 BKAG	BKA	-	Gefahrenabwehr/Strafverf.
5c.		Art. 45 BayPAG § 15c HSOG § 39 RP POG (usw.)	L'Polizeibehörden	-	Gefahrenabwehr
5d.		*Verfassungsschutzrecht-AnpassungsG-E 2020*	*Dienste*	-	*Nachr. Aufklärung*
6.	**Daten im Zusammenhang mit der Nutzung von Telemediendiensten**				
6a.	Bestandsdaten	§ 100j Abs. 1 Nr. 2 StPO	Private Provider (§§ 14, 15a TMG)	Staatsanwaltschaft	Strafverfolgung
		§ 46 Abs. 4a OWiG		Polizei-/Verw.-Beh.	OWi
		§§ 10 Abs. 1 Nr. 2; 40 Abs. 2; 63a Abs. 1, 66a Abs. 2 BKAG		BKA	Gefahrenabwehr/ Strafverf./
		§ 22a BPolG		Rechtshilfe	
		§ 52 PolG BW Art. 43 Abs. 5 BayPAG § 20a PolG NRW (usw.)		Bundespolizei	Gefahrenabwehr
		§§ 10 Abs. 1, 30 Abs. 1 Nr. 2 u. Abs. 2 Nr. 2 ZFdG		L'Polizeibehörden	Gefahrenabwehr
		§ 8d BVerfSchG (usw.)		Dienste	Nachr. Aufklärung
6b.	Passwörter, andere Zugangsdaten	§ 100j Abs. 1 S. 2 StPO	Private Provider (§§ 14, 15b TMG)	Staatsanwaltschaft	Strafverfolgung
		§§ 40 Abs. 2, 3, 63a Abs. 2, 3, 66a Abs. 2, 3 BKAG		BKA	Gefahrenabwehr/Strafverf.
		§ 22a Abs.1, 2 BPolG		Bundespolizei	Gefahrenabwehr
		§ 52 PolG BW Art. 43 Abs. 5 BayPAG § 20a PolG NRW (usw.)		L'Polizeibehörden	Gefahrenabwehr
		30 Abs. 1, 3 ZFdG		Zollkriminalamt	AWG/KWKG-Ermittlungen, Bekämpfung Schwarzarbeit, u.a.
		§ 8d Abs. 1, 3 BVerfSchG (usw.)		Dienste	Nachr. Aufklärung

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
6c.	Nutzungsdaten	§ 100k StPO	Private Provider (§§ 15, 15c TMG)	Staatsanwaltschaft	Strafverfolgung
		§ 10a BKAG		BKA	Gefahrenabwehr/Strafverf.
		§ 53 PolG BW Art. 43 Abs. 4 BayPAG § 20a PolG NRW (usw.)		L'Polizeibehörden	Gefahrenabwehr
		§ 8a BVerfSchG (usw.)		Dienste	Nachr. Aufklärung
7.	**Systematische Überwachung und Speicherung von Finanztransaktionsdaten (Geldwäschekontrolle)**				
7a.	Kundenstamm-daten Geschäfts-informationen zum Kunden Kontobewegun-gen, Transak-tionsdaten	Ermittlungspflicht: §§ 4ff. GwG Aufzeichnungs- u. **anlasslose Vorratsdaten-speicherpflicht:** § 8 Abs. 4 GwG Meldepflicht: § 43 GwG	Banken, Kreditinstitute, Finanzdienstleister, etc. (§ 2 Abs. 1 Nr. 1-6 GwG)	**Proaktive Zuliefe-rung** an FIU: General-zolldirektion Köln → nachfolgend weitere umfassende Zugriffsrechte auf weitere Datenbestän-de, §§ 29ff. GwG	Generierung von Tatverdacht
			FIU nach operativer Analyse	**Proaktive Daten-übermittlung** an andere Behörden: § 32 Abs. 1/2 GwG	Strafverfolgung Gefahrenabwehr Nachr. Aufklärung
				Datenübermittlung aufgrund Auskunfts-ersuchen an andere Behörden: § 32 Abs. 3 GwG	Strafverfolgung Gefahrenabwehr Nachr. Aufklärung Besteuerungsverf. Sozialvers., behördl. Aufsicht
7b.	Kundenstamm-daten Geschäftsinfor-mationen zum Kunden Transaktions-/ Zahlungsdetails	Ermittlungspflicht: §§ 4ff. GwG Aufzeichnungs- u. **anlasslose Vorratsdatenspeicher-pflicht:** § 8 Abs. 4 GwG Meldepflicht: § 43 GwG	Sonstige Verpflichtete nach (§ 2 Abs. 1 Nr. 7 ff. GwG: z.B. Rechtsanwälte, Notare, Wirtschaftsprüfer, Steuer-berater, Versicherungen, Immobilienmakler, u.a.)	**Proaktive Zuliefe-rung** an FIU: General-zolldirektion Köln → nachfolgend weitere umfassende Zugriffsrechte auf weitere Datenbestän-de, §§ 29ff. GwG	Generierung von Tatver-dacht, ggf. Strafverf.
			FIU nach operativer Analyse	**Proaktive Datenüber-mittlung** an andere Behörden: § 32 Abs. 1/2 GwG	Strafverfolgung Gefahrenabwehr Nachr. Aufklärung
				Datenübermittlung aufgrund Auskunfts-ersuchen an andere Behörden: § 32 Abs. 3 GwG	Strafverfolgung Gefahrenabwehr Nachr. Aufklärung Besteuerungsverf. Sozialvers., behördl. Aufsicht
8.	**Kontoabfragen**				
8a.	Informationen zu Privat-/Ge-schäftskonten (Stammdaten)	§ 24a KWG § 93 Abs. 7/8 AO § 802l ZPO	Banken, Kreditinstitute	BaFin Bundeszentralamt für Steuern	Besteuerungsverf./Steuer-strafverf./allg. Strafverf./ priv.Vollstreckungsverf./ Amtshilfe für andere Behör-den, auch Gefahrenabwehr

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
8b.	Kundendaten Kontodaten Konto-bewegungen Geldanlagen	§ 8a BVerfSchG (usw.)	Banken, Kreditinstitute	Dienste (direkt oder über Bundeszentralamt für Steuern)	Nachr. Aufklärung
9.	**Mobilitätsdaten**				
9a.	Standortdaten Mobilfunk (ggf. nach Untergruppen: Echtzeit / retrograde / zukünftige)	§ 100i StPO	Priv. Provider	Staatsanwaltschaft	Strafverfolgung
		§ 53 BKAG		BKA	Gefahrenabwehr/Strafverf.
		§ 27e Abs, 1 (BPolGModG 2021, vgl. BT-Drucks. 19/26541)		*Bundespolizei*	*Gefahrenabwehr*
		§ 55 PolG BW § 20a Abs. 1 Nr. 2a PolG NRW Art. 43 Abs.2 Nr. 3 BayPAG (usw.)		Polizeibehörden	Gefahrenabwehr
		§ 77 ZFdG		Zollkriminalamt	KWKG-/AWG-Sachen
		§ 9 Abs. 4 BVerfSchG (usw.)		Dienste	Nachr. Aufklärung
9b.	Standort-/ Bewegungs-daten aus Kfz-Navigations-systemen oder Bordcomputern	§§94/98/110 StPO	Priv. Eigentümer/Nutzer/ ggf. Kfz-Werkstätten + Serviceeinrichtungen	Staatsanw./Polizei	Strafverfolgung
9c.	Standort-/ Bewegungs-daten aus Mobilgeräten	§§94/98/110 StPO	Priv. Eigentümer	Staatsanw./Polizei	Strafverfolgung
9d.	Automat. Kfz-Kennzeichen-überwachung	§ 27b BPolG § 24d ASOG Bln § 36a BbgPolG Art. 39 BayPAG § 51 PolG BW § 32a Nds. POG (usw.)	Polizeibehörden	-	Gefahrenabwehr/ Strafver-folgung
9e.	Automat. Kfz-Kennzeichen-überwachung	§ 100h StPO	Bislang nur BKA (in Einzelfällen) und Polizei Bbg.	-	Strafverfolgung
		§ 163g StPO-E	*Bundesweit geplant für Staatsanw., vgl. BT-Drucks. 19/27654*		
9f.	Automat. Kfz-Kennzeichen-überwachung	§ 63c StVG	Polizeibehörden	-	Verkehrsüberwachung: Kontrolle von Verkehrs-beschränkungen (z.B. Diesel-Fahrverbote) Verwendung in OWi-Verf.
9g.	Kennzeichenba-sierte automat. Abschnitts-kontrolle (Streckenradar: ‚section control')	§ 32 Abs. 6 Nds. POG	L'Polizeibehörden	-	Verkehrsüberwachung

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
9h.	Elektronische Aufenthalts-überwachung (Bewegungspro-file durch GPS, etc.)	§ 56 BKAG Terrorist. Gefährder	BKA GÜL Bad Vilbel	-	Primär Gefahrenabwehr Gespeicherte Daten dürfen zur Strafverfolgung ver-wendet werden
		Art. 34 Bay PAG § 32 PolG Ba.-Wü. § 34c PolG NRW § 36c SOG LSA (usw.)	Polizeibehörden	-	Gefahrenabwehr (unterschiedl. Reichweiten) Funktionsbeeinträchtigung teilw. strafbewehrt
		§§ 68b Abs. 1 Nr. 12 StGB, 463a StPO Ehem. Straftäter in Führungsaufsicht	Fü'Aufsichtsstellen	-	Strafrechtl. Rückfallprävention Gespeicherte Daten dürfen zur Strafverfolgung verwendet werden
9i.	Fluggastdaten (§ 31a Abs. 3 Nr. 1-10 BPolG)	§ 31a BPolG	Airlines	BPolPräs.	Gefahrenabwehr, Fahndung, Strafverf., Grenzschutz
9j.	Erweiterte Fluggastdaten (§ 2 Abs. 2 Nr. 1-20 FlugDaG)	FlugDaG	Airlines	**Proaktive anlasslose Zulieferung** an BKA/ Fluggastdatenzen-tralstelle → **dort auf Vorrat gespeichert**	Gefahrenabwehr/Strafverf.
9k.	Fluggastdaten (§ 8a Abs. 2 Nr. 1 BVerfSchG)	§§ 8, 8a BVerfSchG (usw.)	Airlines, Flugbuchungsanbieter	Dienste	Nachr. Aufklärung
9l.	Digitale Einreise-anmeldung: personenbe-zogene Daten gem. § 2 Nr. 16 InfSchG: sämtliche Aufenthaltsorte 10 Tage vor und 10 Tage nach Einreise, Reiseweg/-ver-lauf	CoronaEinreiseVO'en d. BMG v. 5.11.2020, 13.1.2021, 26.3.2021 gem. § 36 Abs. 8 Nr. 2 InfSchG	Personen, die über den Land-/Luft-/Seeweg aus Risikogebieten einreisen Kontrollpflicht für Flughäfen, Häfen, Bahnhöfe u. Beförde-rungsunternehmen Kontrollbefugnis für B'Pol (§ 36 Abs. 11 InfSchG) Bei fehlender Online-Anmel-dung Erhebungspflicht bzgl. Ersatzmitteilung **Anlasslose Speicherpflicht** bzgl. Passagierdaten u. Sitz-pläne für Flug- und Schiffs-unternehmen (30 Tage)	**Proaktive Meldepflicht** an Gesundheits-behörden (über Portal bei der Deutschen Post als externer Dienstleister) → Folgemaßnahmen mögl., einschl. Bußgeldverf.	Infektionsschutz (Quarantänekontrolle, COVID-Bekämpfung) Ausdrückl. Verbot ander-weitiger Verwendung der Daten, § 38 Abs. 9 InfSchG
10.	**Daten aus dem privaten Lebensbereich**				
10a.	Akustische WRÜ	§ 100c StPO	Staatsanwaltschaft	-	Strafverfolgung
		§ 46 BKAG	BKA	-	Gefahrenabwehr
		§ 28 Abs. 2 BPolG	Bundespolizei	-	Gefahrenabwehr
		Art. 41 Abs. 1 S. 3 BayPAG § 33a BbgPolG § 50 PolG BW (usw.)	L'Polizeibehörden	-	Gefahrenabwehr
		§ 9 Abs. 2 BverfSchG (usw.)	Dienste	-	Nachr. Aufklärung

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
10b.	Optische WRÜ	§ 46 BKAG	BKA	-	Gefahrenabwehr
		§ 28 Abs. 2 BPolG	Bundespolizei	-	Gefahrenabwehr
		§ 33a BbgPolG § 50 PolG BW § 18 PolG NRW Art. 41 Abs. 1 S. 3 BayPAG (usw.)	L'Polizeibehörden	-	Gefahrenabwehr
		§ 9 Abs. 2 BVerfSchG (usw.)	Dienste	-	Nachr. Aufklärung
10c.	Gesprächs-/Verlaufsprotokolle aus technischen Assistenzsystemen im Haushalt (‚Siri', ‚Alexa', andere Smart-Home-Anwendungen mit Aufzeichnungsfunktion)	§§ 94/98/110 StPO (lokal gespeicherte Daten) *Als unzulässig erachtet wird Zugriff auf das Gerät zur gezielten WRÜ*	Private Eigentümer, Serviceprovider	Staatsanwaltschaft	Strafverfolgung
				Zulässigkeit präventiver u. nachrichtendienstl. Zugriffe (Beschlagnahme und Auslesen der Daten) str.	
10d.	*Private Äußerungen in sozialen Netzwerken*	*§ 3a NetzDG* *Inhalte, IP-Adressen, Portnummern* *Inkrafttreten: 1.2.2022*	*Netzwerkbetreiber*	***Proaktive Zulieferung*** *an BKA* *→ nachfolgend weitere Zugriffsrechte auf andere Daten,* *§§ 10, 10a BKAG* *(vgl. Nr. 6)*	*Gefahrenabwehr, Generierung von Tatverdacht, ggf. Strafverfolgung*
	Sonstige				
11.	Andere nicht nach Art. 10 od. 13 GG geschützte Datenbestände aller Art (nicht spezifiziert)	§§ 94/98/110 StPO	Privatpersonen	Staatsanwaltschaft	Strafverfolgung
				Zulässigkeit präventiver u. nachrichtendienstl. Zugriffe (Beschlagnahme und Auslesen der Daten) str.	
12.	Automat. Passbildabfrage	§ 25 Abs. 2 PAuswG	Meldebehörden	Polizeibeh. (Bund, Länder), Steuer-/Zollbeh., Dienste	Prävention OWi (Verkehr) Steuer(straf)verf. Nachr. Aufklärung
13.	**Einmalige, temporäre oder sondergesetzliche Datenzugriffe mit Streuwirkung oder sonst erheblicher Eingriffsintensität***				
13a.	Übermittlung von Meldedaten	§ 9a Abs. 2 Nr. 1-20, Abs. 3 Nr. 1-5, Abs. 4 Nr. 1-3 ZensusvorbG 2021 (eingef. d. Art. 1 ZensVorbG2021uaÄndG)	Meldebehörden	Stat. Bundesamt/ Landesämter	Zensus 2022 (Volks-, Gebäude-, Wohnungszählung)
	(aufgrund der Corona-Pandemie vorläufig gestoppt; vgl. www.zensus2022.de/DE/Aktuelles/verschiebung_beschluss.html)				

Nr.	Datenart	Rechtsgrundlage	Datenführende Stelle, Speicherort, überwachende/zuliefernde/ zulief.-pflichtige Stelle	Abfragende bzw. verfahrensführende Stelle	Überwachungsziel
13b.	Individualisierte Personendaten aus Corona-Kontaktlisten (Aufenthalte in Gaststätten, Ladengeschäften, Veranstaltungen, etc.)	Corona-VO'en der Länder	Öffentliche u. private Betreiber u. Veranstalter	Gesundheitsämter, Ortspolizeibehörden, ggf. auch Staatsanwaltschaft gem. §§ 94/98/110 StPO	Gefahrenabwehr: Infektionsschutz, ggf. auch Nutzung für Strafverfolgung *(uneinheitlich: z.B. Bay, Bremen, Hamb., Hess, Rh.-Pf.: ja / Ba.-Wü: angeblich nein, es existieren aber zahlr. Informationen über tatsächl. erfolgte Zugriffe)*
...	ggf. weitere				
...	ggf. weitere				
14.	**Analytische Zusammenführung verschiedener Datenbestände (Rasterfahndung)**				
14a.		§§ 98a/b StPO	Datenführende Stellen (öffentl./privat)	Staatsanwaltschaft	Strafverfolgung
14b.		§ 31 PolG NRW § 48 PolG BW Art. 46 BayPAG (usw.)	Datenführende Stellen (öffentl./privat)	L'Polizeibehörden	Gefahrenabwehr
14c.		§ 48 BKAG	Datenführende Stellen (öffentl./privat)	BKA	Gefahrenabwehr/Strafv.

*) Es wäre sinnvoll, in einem späteren Stadium in ein permanentes Überwachungsbarometer auch solche Einmal-Sachverhalte in einer Extra-Rubrik „Sonderereignisse" für den jeweiligen Erhebungszeitraum auszuweisen (siehe Haupttext unter 3.1.).