Kapitel B: Massenüberwachung im Verfassungsrecht: Vorratsdatenspeicherung und strategische Aufklärung

Der staatliche Umgang mit Finanzdaten, insbesondere im Rahmen der Geldwäschebekämpfung, soll umfassend aus der Perspektive des Sicherheitsverfassungsrechts betrachtet und bewertet werden. Dazu bedarf es einer Darstellung dieses Konzepts, um die Geltung für das Geldwäscherecht zu begründen.

Um die Hintergründe der Rechtsprechung zu den Maßnahmen der Massenüberwachung zu erläutern, soll zunächst der Versuch einer Erklärung unternommen werden, was unter dem Begriff der *sicherheitsrechtlichen Massenüberwachung* überhaupt verstanden werden soll. Nicht nur muss hierzu das Rechtsgebiet des Sicherheits- bzw. des Sicherheitsverfassungsrechts näher umschrieben werden. Auch mit dem Terminus der Massenüberwachung bzw. dessen Notwendigkeit und Mehrwert soll vorab eine Auseinandersetzung stattfinden.

Im weiteren Verlauf soll sodann die Rechtsprechung zu solchen Maßnahmen erläutert werden, die sich nach den vorangegangenen Überlegungen als sicherheitsrechtliche Massenüberwachung identifizieren lassen. Das sind vornehmlich die Urteile des Europäischen Gerichtshofs (EuGH) und des Bundesverfassungsgerichts (BVerG) zur Vorratsdatenspeicherung und zur strategischen Aufklärung. Diese Rechtsprechung wird – ausgehend von den allgemeinen Anforderungen der Rechtsprechung an die Überwachungsmaßnahmen der Sicherheitsbehörden – den Rahmen vorgeben, anhand dessen im Zuge dieser Arbeit die Regeln zur Überwachung des Finanzverkehrs überprüft werden sollen.

I. Einführung: Der Begriff der (Massen)Überwachung

Der Begriff der (Massen-)Überwachung taucht im Zusammenhang mit dem digitalen Zeitalter spätestens seit der NSA-Affäre immer wieder als Schlagwort[43], fast schon als Kampfbegriff, auf, ohne dass dabei stets klar

43 Siehe nur *Čas/Bellanova/Burgess ua.* in Friedewald/Burgess/Čas ua. (Hrsg.), Surveillance, 2017 (1).

wird, welche konkreten Sachverhalte damit eigentlich gemeint sein sollen. In Verbindung mit Finanzdaten ist von einer Massenüberwachung nur selten die Rede.

I. Unzulänglichkeiten und Potential des Überwachungsbegriffs

Das Phänomen der *Überwachung* wird nicht nur im rechtswissenschaftlichen, sondern auch im sozialwissenschaftlichen Kontext besprochen – insbesondere in der Kriminologie. Dort bilden die sog. „surveillance studies"[44] mittlerweile ein eigenständiges Forschungsfeld, auf dem insbesondere um eine Definition des Überwachungsbegriffs gerungen wird.

a. Der Überwachungsbegriff der „surveillance studies"

Nach *Lyon*, einem Vorreiter der surveillance studies, lässt sich Überwachung definieren als *„gezielte, systematische und routinemäßige Betrachtung persönlicher Umstände für Zwecke der Einflussausübung, Management, Schutz oder Direktion."*[45] Aufgrund dieser weiten Beschreibung bemerkt er, dass *Überwachung* mit einer ausgesprochenen Ambiguität verbunden ist. Der Begriff umfasst eine Fülle an Verhaltensweisen, die – je nach Kontext – eine völlig unterschiedliche Bewertung sowohl im Rahmen einer sozialen als auch rechtlichen Betrachtungsweise erfahren müssen.[46] Es macht offensichtlich einen Unterschied, ob bspw. eine Mutter ihr Kind auf dem Spielplatz beobachtet oder ob ein Polizeibeamter die Telefongespräche eines Verdächtigen abhört. Selbstverständlich können diese beiden Fälle der *Überwachung* daher auch keinem gemeinsamen Normregime unterliegen.

---

44 Vgl. *Lyon,* Surveillance Studies, 2012; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18 *ders.,* The electronic Eye, 1994; *Zurawski* in Zurawski (Hrsg.), Surveillance Studies, 2007, S. 7; s.a. *Adensamer,* Hdb. Überwachung, 2020, S. 24 ff.

45 *Lyon,* Surveillance Studies, 2012, S. 14; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18 (19); *J. Pohle* FIfF-Kommunikation 2019(4), 37 (37).

46 *Lyon,* Surveillance Studies, 2012, S. 14; *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (73) *Adensamer,* Hdb. Überwachung, 2020, S. 24; *Kreissl/Norris/Krlic ua.* in Wright/Kreissl (Hrsg.), Surveillance, 2015, S. 150 (155 f.).

Für eine ergiebige wissenschaftliche Auseinandersetzung gleich welcher Disziplin muss also stets die konkrete Form bzw. die Maßnahmen bestimmt werden, in denen sich die Überwachung manifestiert.[47]

b. Der Überwachungsbegriff im Recht

Für die rechtliche Betrachtung ist es von erheblicher Bedeutung, durch wen die *Überwachung* erfolgt, und aus welchem Grund, da einerseits die Wirkung der Grundrechte – der äußersten Schicht des Schutzes vor Überwachung – von der Person des *Überwachenden* abhängig ist, Art 1 Abs. 3 GG, und andererseits das Datenschutzrecht zwischen öffentlichen und nicht-öffentlichen Stellen unterscheidet[48], §§ 23, 24 BDSG.

Trotzdem widmen weder das deutsche noch das europäische Recht dem Überwachungsbegriff eine eigene Definition, wenngleich diese Rechtsordnungen an einigen Stellen explizit von Überwachung sprechen.

So kennen wir etwa die Videoüberwachung, z. B. § 4 BDSG, die Telekommunikations*überwachung* (TKÜ), z. B. §§ 54 PolG BW, 51 BKAG, 100a StPO, die akustische Wohnraum*überwachung*, § 100c StPO, oder die Pflicht zur *Überwachung* von Geschäftsbeziehungen, Art. 13 Abs. 1 lit. d) der EU-Geldwäscherichtlinie (GWRL)[49]. An anderen Stellen wird hingegen auf die Bezeichnung als Überwachung verzichtet – etwa bei den automatisierten Kennzeichen*erfassungssystemen* (z. B. Art. 39 BayPAG).[50]

Dass das Recht den Überwachungsbegriff nicht ausreichend reflektiert, zeigt sich etwa in § 100a StPO – der Vorschrift über die strafprozessuale TKÜ. Dort heißt es, dass *auch ohne Wissen der Betroffenen die Telekommunikation überwacht und aufgezeichnet werden darf.*

Hier wird semantisch zwischen der *Überwachung* und der *Aufzeichnung* getrennt. Man könnte also meinen, dass diese Norm von einem Überwachungsbegriff ausgeht, der allein auf die staatliche Wahrnehmung bestimm-

47 Vgl. *Kreissl/Norris/ Krlic ua.* in Wright/Kreissl (Hrsg.), Surveillance, 2015, S. 150 (155 f.).

48 Dazu *Masing*, NJW 2012, 2305 (2306 ff.).

49 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43; konsolidierte Fassung der 4. und 5. GWRL, Dok. 02015L0849-20210630.

50 Das BVerfG spricht auch von „*Kennzeichenkontrolle*", siehe BVerfGE 150, 244 – Autom. Kennzeichenkontrolle II.

ter Informationen gerichtet ist. Aus Sicht des Betroffenen wird aber regelmäßig die Aufzeichnung das größere Problem darstellen, da die spätere Beweisführung gegen ihn gerade auf der Perpetuierung seiner Kommunikation beruht. Schon hier zeigt sich somit eine erste Unzulänglichkeit des allgemeinen Überwachungsbegriffs. Erblickte man dessen Fokus allein in der fremden Wahrnehmungshandlung, könnte nur in bestimmten Situationen erklärt werden, wieso eine Überwachung als negativ oder als Eingriff empfunden wird.

Der Betroffene kann die Wahrnehmung ihn betreffender Informationen schließlich nicht grundsätzlich kontrollieren und ist daher vielfach auf das Interesse beschränkt, über die reine (Fremd-)Wahrnehmung hinausgehende Handlungen in Bezug auf solche Informationen abzuwehren.[51] In der Literatur zu § 100a StPO wird der Befugnis zur *Aufzeichnung* deshalb zu Recht kein eigenständiger Wert beigemessen. Sie geht in der *Überwachung* schon deshalb mit auf, weil in den meisten Fällen keine Echtzeitabhörung der Kommunikation stattfindet, sondern allein eine technische Aufzeichnung, die später gesichtet wird.[52]

Somit zeigt sich, dass im Bereich staatlicher Maßnahmen weniger die Wahrnehmung bestimmter Sachverhalte für die Überwachung entscheidend ist, als die technischen Instrumente[53], mit denen sie erfolgt und manifestiert wird.

Auch im Datenschutzrecht sucht man vergeblich nach einer Definition der Überwachung. Der Begriff scheint in diesem Rechtsgebiet nur beiläufig vorzukommen, etwa in § 4 BDSG, der die private Video*überwachung* reglementiert. Im Kern hängt sich das (europäische) Datenschutzrecht stattdessen am Begriff der „Datenverarbeitung" auf, unter dem sämtliche informationsbezogenen Handlungen zusammengefasst werden.

Dabei muss genau genommen zwischen Informationen und Daten unterschieden werden, wobei jeweils verschiedene Definitionen bzw. Abgren-

51 *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (16 f.); *dies.,* Informationelle Selbstbestimmung, 2005, S. 113 ff., 437 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (S. 136 ff.); *Placzek,* Informations- und Datenschutz, 2006, S. 92 ff.; *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, 2.5 Rn. 19; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121).

52 *Günther* in MüKo StPO, § 100a Rn. 86.

53 Zum Begriff des "Instruments" in Bezug auf Maßnahmen der Geldwäscheprävention vgl. *Favarel-Garrigues/Godefroy/Lascoumes* in Svedberg Helgesson/Mörth (Hrsg.), Securitization, 2012, S. 88 (91 ff.).

zungen vorgeschlagen werden.[54] Für die in dieser Arbeit behandelten Fragen reicht es allerdings völlig aus, Daten als *zeichenhafte Darstellung von Informationen* zu verstehen.[55]

Auch der Anwendungsbereich der DSGVO, die „Daten" mit „Informationen" in Art. 4 Abs. 1 Nr. 1 gleichsetzt, ist nach Art. 1 Abs. 1 nur eröffnet, wenn personenbezogene Informationen verarbeitet werden, was wiederum irgendeine Verkörperung dieser Informationen voraussetzt.[56]

Verarbeitung in diesem Sinne meint nach Art. 4 Nr. 2 DSGVO *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung"*. Jeder Einzelne dieser Vorgänge muss für sich stets den datenschutzrechtlichen Anforderungen entsprechen, Art. 5, 6 DSGVO.

Für das über der DSGVO stehende europäische Primärrecht, insbesondere Art. 7, 8 der EU-Charter, sind die Begriffsbestimmungen des Datenschutzrechts aber selbstverständlich nicht abschließend, da auch auf europäischer Ebene gilt, dass das einfache Recht nicht den Inhalt des Primärrechts abschließend bestimmen kann.[57] Für Eingriffe in die Grundrechte auf Privatleben und Datenschutz nach Art. 7, 8 EU-Charter muss der EuGH daher nicht die Begriffsbestimmung des Art. 4 Nr. 2 DSGVO bemühen. Er kann unmittelbar anhand des Schutzbereichs der Grundrechte prüfen, ob eine Maßnahme einen Eingriff in diese darstellt.[58] Die Datenverarbeitungs-

54 Übersicht bei *Albers,* Informationelle Selbstbestimmung, 2005, S. 87 ff.; *Placzek,* Informations- und Datenschutz, 2006, S. 92 f.

55 Siehe nur *Sieber*, NJW 1989, 2569 (2572); *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (23); *Bäcker*, Der Staat 2012, 91 (92); *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, 2.5 Rn. 17

56 *Karg* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 25.

57 Vgl. *J.-P. Schneider*, Die Verwaltung 2011, 499 (515) mit Verweis auf EuGH, Urteil v. 20.5.2003, C-138/01, C-139/01 (Österreichischer Rundfunk), Rn. 68 ff = EuR 2004, 276.

58 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 121 ff. – PNR Canada = ZD 2018, 23

schritte der DSGVO taugen dem Gerichtshof jedoch als Ansatzpunkt.[59] Da die DSGVO letztlich dem Schutz der Grundrechte aus Art. 7, 8 der EU-Charter dient[60], liegt jedenfalls immer dann ein Eingriff in diese Rechte vor, wenn eine grundrechtsgebundene Stelle eine Datenverarbeitung i. S. d. Art. 4 Nr. 2 DSGVO vornimmt.[61]

Jedenfalls aber kennt auch der EuGH keinen Überwachungstatbestand per se, sondern beschreibt stets – wie auch die DSGVO – einzelne Verhaltensweisen als konkrete Eingriffe bzw. Datenverwendungstatbestände, anstatt einheitlich von einer *Überwachung* zu sprechen.[62]

c. Überwachung als final ausgerichtete Kombination verschiedener Datenverarbeitungsschritte

Es scheint somit, als ob der Überwachungsbegriff nicht von eigenständiger rechtlicher Bedeutung ist, da die einzelnen Maßnahmen, die die jeweilige *Überwachung* konstituieren, Datenverarbeitungsmaßnahmen darstellen und daher dem Datenschutzrecht unterfallen – dem Verfassungsrecht sowieso.

Es lässt sich aber nicht leugnen, dass dem Begriff eine gewisse Konnotation inhärent ist, die greifbar gemacht werden muss. Eine Definition der *Überwachung* für den Kontext des Rechts könnte es erlauben, komplexere Sachverhalte abzugrenzen und miteinander zu vergleichen. Die einzelnen Datenverarbeitungsvorgänge sind nämlich mitnichten unabhängig voneinander, sondern eng verknüpft.[63] Sie können sich gegenseitig bedingen und vielgestaltig so kombiniert werden, dass die einzelnen Verarbeitungsschrit-

59 Etwa EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 = NJW 2021, 531; siehe dazu *Marsch,* Datenschutzgrundrecht, 2018, S. 130 f.; *Schiedermair* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO, Einl. Rn. 169 ff.

60 Erwägungsgrund 1, DSGVO; *Schantz* in BeckOK Datenschutzrecht, DSGVO Art. 1 Rn. 5; *Sydow* in Sydow DSGVO, Einl. Rn. 7.

61 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 13.

62 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 134 ff. = NJW 2021, 531; EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 154 ff. – PNR Canada = ZD 2018, 23; siehe auch BVerfGE 125, 260 (310 ff.) – Vorratsdatenspeicherung.

63 *Albers,* Informationelle Selbstbestimmung, 2005, S. 125 f.

te auf die Auswirkungen der jeweils anderen intensivierend wirken. So geht etwa das BVerfG bei Datenerhebungen durch Sicherheitsbehörden davon aus, dass allein die Möglichkeit der Weitergabe bereits die Intensität der ursprünglichen Erhebung erhöht.[64] Durch die Betrachtung bestimmter Handlungen als Verknüpfung von Datenverarbeitungsvorgängen lässt sich darstellen, weshalb manche *Überwachungs*phänomene in Bezug auf persönliche Daten von besonderer, auch rechtlicher, Problematik sind.

Ausgehend von diesem Verständnis lässt sich aus dem Begriff der (Massen)Überwachung ein Mehrwert für die rechtliche Beurteilung ziehen. Mit ihm lassen sich bestimmte Kombinationen von Datenverarbeitungsschritten bzw. den dahinterstehenden rechtlichen Grundlagen beschreiben, deren individuelle rechtliche Relevanz bzw. Eingriffsintensität sich gerade danach bestimmt, dass sie Teil einer solchen Kombination sind. Der Überwachungsbegriff befreit also nicht davon, einzelne Datenverarbeitungsschritte grundsätzlich als eigenständige Grundrechtseingriffe zu begreifen. Er kann aber für die jeweilige Bewertung der einzelnen Verarbeitungen ausschlaggebend sein.

Um dieses Begriffsverständnis zu erläutern, kann auf die Rechtsprechung zur Vorratsdatenspeicherung zurückgegriffen werden – eines der Phänomene, die hier als Form der Massenüberwachung vorgestellt werden sollen.

Unter einer Vorratsdatenspeicherung kann man allgemein die Kombination aus einer Verpflichtung zur Datenerhebung und Speicherung einerseits und Befugnisnormen zum Abruf der gespeicherten Daten andererseits verstehen.[65] Zwar belasten diese Schritte den Betroffenen nur teilweise auch tatsächlich. Die Intensität jeder einzelnen Beeinträchtigung ergibt sich aber daraus, dass sie Teil einer Kombination von aufeinanderfolgenden Datenverarbeitungspflichten und -rechten ist.

Mängel in der Regelung bzw. gesetzlichen Gestaltung eines Datenverarbeitungsschritts können deshalb auf weitere Datenverarbeitungsschritte durchschlagen und deren Verhältnismäßigkeit beeinflussen, obwohl jede Verarbeitung einen eigenen Grundrechtseingriff darstellt und deswegen separat geprüft werden könnte.

64 BVerfGE 100, 313 (384) – strategische Fernaufklärung.; BVerfGE 110, 33 (70); dazu *Löffelmann*, GSZ 2019, 16 (18 f.).

65 Vgl. *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 117; *dies.* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (80 ff.) vgl. auch *Europäische Kommission,* Informationsgesellschaft, KOM(890) endg, 26.01.2001, S. 20.

Schon die Speicherung bestimmter Daten kann daher eine erhebliche Rechtsverletzung darstellen, wenn die Voraussetzungen des Zugriffs unzureichend geregelt worden sind.[66] Die Verhältnismäßigkeit des Zugriffs hängt wiederum davon ab, ob damit umfassende Übermittlungspflichten einhergehen, und ob auf Daten zugegriffen wird, deren Speicherung schon einen erheblichen Grundrechtseingriff darstellt.

Zwischen sämtlichen Datenverarbeitungsschritten, die Teil eines Überwachungskomplexes sind, besteht also eine *synergetische Wechselwirkung*. Die Verhältnismäßigkeit kann zwar für jeden Eingriff bzw. Datenverarbeitungsschritt separat geprüft, aber ohne Betrachtung der übrigen Eingriffe nicht in ihrer rechtlichen Bedeutung erfasst werden.

2. Elemente staatlicher (Massen)Überwachung

Für einen rechtlich tragfähigen Begriff der Überwachung kommt es also weniger darauf an, dass überhaupt verschiedene Datenverarbeitungsschritte kombiniert werden – dies findet andauernd statt –, sondern auf die konkreten Wirkungen und Hintergründe dieser Kombination. Insofern kommt die von *Lyon* im Rahmen der surveillance studies angesprochene Ambiguität erneut zum Tragen.[67]

Im rechtlichen Kontext muss es darauf ankommen, konkret jene Formen herauszuarbeiten, die einer besonderen rechtlichen Würdigung bedürfen.[68] Dabei kann auf bestimmte Überwachungskomponenten oder -elemente[69] zurückgegriffen werden, die hier kurz vorgestellt werden sollen.

66 BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung; dazu *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 159; EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 = NJW 2014, 2169; dazu *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.); s.a. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; dazu auch VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI, Rn. 73 „funktionale Einheit".

67 *Lyon,* Surveillance Studies, 2012, S. 14.

68 Ähnlich *Timan/Galič/Koops* in Brownsword/Scotford/Yeung (Hrsg.), Oxford Hdb. Law Regulation Tech, 2017, S. 731 (744 ff.).

69 Vgl. In Bezug auf die strategische Kommunikationsüberwachung insbesondere EGMR, Urt. v. 25.5.2021 – Nr. 58170/13, 62322/14, 24960/15, Big Brother Watch ua/ Vereinigtes Königreich, Rn. 325 = NVwZ-Beilage 2021, 11

a. Beobachten als Datenerhebung und Datenerfassung

Am Anfang jeder Überwachungshandlung steht eine finale Beobachtung, die sich (datenschutz-)rechtlich zur „Datenerhebung und -Erfassung" i. S. d. Art. 4 Nr. 2 DSGVO transkribieren lässt. Diese eng miteinander verbundenen Datenverarbeitungsvorgänge beziehen sich auf den Moment, in dem eine Information erstmals wahrgenommen und mindestens für einen Augenblick verkörpert wird.[70]

Die Auftrennung von Erhebung und Erfassung wirkt dabei oft künstlich, denn die Datenerhebung, d. h. eine Erstellung von Daten ohne anschließende, wenigstens kurzfristige Speicherung, ist als separat verstandener Vorgang praktisch irrelevant.

Aus grundrechtlicher Sicht ist die Differenzierung von Erhebung und Erfassung auch nicht von Belang. Einzelne Verarbeitungsschritte einer Überwachungsmaßnahme können als einheitlicher Eingriff verstanden werden, wenn die Vorgänge einen einheitlichen Lebenssachverhalt bilden. So hat etwa der EuGH die Speicherung von Verkehrsdaten und den Zugriff jeweils als eigenständigen Eingriff bewertet, ohne auf die datenschutzrechtliche Einteilung dieser Vorgänge jeweils einzugehen.[71] Auch im Rahmen seines Gutachtens zum geplanten Abkommen der EU mit Kanada über die Verwendung von Fluggastdaten (PNR-Abkommen[72]) wird nur zwischen den Schritten „Speicherung, Analyse und Verwendung" unterschieden,[73] obwohl der Vorgang der Speicherung zwingend verschiedene Datenverarbeitungsschritte i. S. d. Art. 4 Nr. 2 DSGVO beinhaltet.

Anders mutet insofern nur die dritte Entscheidung des EuGH zur TK-Vorratsdatenspeicherung an, *La Quadrature du Net*[74]. In diesem Urteil, in dem es auch um die automatisierte Analyse von Verkehrsdaten ging, identi-

70 *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 15 f.

71 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; vgl. auch Vgl. BVerfGE 150, 244 (265 ff.) – Automatische Kennzeichenkontrolle II.

72 Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR), COM(2013) 529 final, 2013/0251 (NLE).

73 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 154 ff. – PNR Canada = ZD 2018, 23; detailleirt EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 92 ff. = EuZW 2022, 706.

74 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531.

fizierte der Gerichtshof den Eingriff ausdrücklich ausgehend vom Begriff der *Datenverwendung* i. S. d. Art. 4 Nr. 2 DSGVO.[75]

Einen solchen Rückgriff auf die DSGVO im Rahmen der Prüfung eines Grundrechts mag man normhierarchisch kritisch beäugen.[76] Eine gewisse Einheitlichkeit des Eingriffstatbestands i. R. d. Art. 7, 8 EU-Charter und des Datenverarbeitungsbegriffs des Art. 4 Nr. 2 DSGVO, dem die grundrechtlichen Bestimmungen ja zugrunde liegen, ist aber durchaus praktikabel. Insbesondere hinsichtlich des ersten Schritts jeder Datenverarbeitung, der Erhebung und Erfassung, sind kaum Alternativen zu der datenschutzrechtlichen Definition denkbar. Es ergibt daher Sinn, auch für den grundrechtlichen Bereich, das *Beobachten* im Sinne einer gezielten Wahrnehmung mit der *Datenerhebung und -Erfassung* i. S. d. Art. 4 Nr. 2 DSGVO gleichzusetzen.

b. Analyse und/oder Speicherung erhobener Daten

Dass eine Überwachung zwangsläufig mit einer Beobachtung im Sinne einer Datenerhebung bzw. -erfassung beginnt, ist nun aber nicht viel mehr als eine Selbstverständlichkeit. Entscheidend ist, dass es nicht bei der Erhebung bestimmter Daten bleibt, sondern diese mit weiteren Verarbeitungsschritten kombiniert wird. Zwei Anschlussprozesse kommen hier in Betracht. Zum einen können die erhobenen Daten gespeichert werden, d. h. länger als für den Augenblick der Erhebung aufbewahrt werden, oder sie können analysiert werden.

Die Kombinationsmöglichkeiten sind vielfältig. So kann sich eine Analyse unmittelbar an die Erhebung anschließen und eine Speicherung oder Weiterleitung vom Ergebnis der Analyse abhängig gemacht werden, wie es etwa bei der Kennzeichenkontrolle[77] oder der strategischen Fernmeldeaufklärung[78] der Fall ist. Oder aber es erfolgt erst eine Speicherung und die Analyse wird erst später im Rahmen einer periodischen Datenspeicherrasterung vorgenommen. So arbeiten in den meisten Fällen die digitalen

75 Idem, Rn. 172.; s.a. *Kingreen* in Callies/Ruffert EUV/AEUV, EU-Charter Art. 8 Rn. 13.
76 *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 31.
77 Vgl. BVerfGE 150, 244 – Automatische Kennzeichenkontrolle II.
78 Vgl. BVerfGE 100, 313 (384) – Strategische Fernaufklärung.

Monitoringsysteme der Banken[79] (dazu Kap. D. III. 2. aa. (2)). Denkbar ist es aber natürlich auch, dass die Daten ausschließlich gespeichert werden, ohne dass unmittelbar weitere Vorgänge eingeleitet werden. In diesen Fällen werden die Speicherpflichten von Zugriffsvorschriften flankiert. Man spricht von der Vorrats(daten)speicherung.[80]

Auch den Vorgängen *Analyse* und *Speicherung* lassen sich verschiedene Datenverarbeitungsschritte i. S. d. Art. 4 Nr. 2 DSGVO zuordnen.

Das Speichern etwa ist als eigenständige Form der Datenverarbeitung explizit genannt und kann als *Aufnehmen* oder *Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung* definiert werden.[81]

Die Analyse von Datensätzen dürfte regelmäßig einen *Abgleich* i. S. d. Art. 4 Nr. 2 DSGVO darstellen, da hierunter nicht nur der Vergleich verschiedener Datensätze fällt, sondern auch das Durchsuchen von Datensätzen nach bestimmten Merkmalen.[82] Es ließe sich jedoch auch als *Auslesen* begreifen, wenn man diesen Verarbeitungsschritt als den Vorgang begreift, *ein auf einem Datenträger gespeichertes Datum zielgerichtet konkret zur Kenntnis zu nehmen*.[83] Jedenfalls aber wird eine Analyse als *Verwendung* gelten[84], die insofern als Auffangtatbestand fungiert.[85]

Weniger die Begrifflichkeiten sind entscheidend als der Inhalt der einzelnen Maßnahme. Damit bestimmte Vorgänge eine Informationsverarbeitung zur *Überwachung* machen, müssen von ihnen bestimmte Effekte ausgehen.

---

79 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 56; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (455 f.).

80 Siehe nur *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021 (117).

81 OVG Hamburg, NZI 2021, 191 (193); *Schild* in BeckOK Datenschutzrecht, DSGVO Art. 4 Rn. 42; *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 19.

82 *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 27; aA. wohl *Ernst* in Paal/Pauly DSGVO/BDSG, DSGVO Art. 4 Rn. 31; *Schild* in BeckOK Datenschutzrecht, DSGVO Art. 4 Rn. 52.

83 *Reimer* in Sydow DSGVO, Art. 4 Rn. 63; ähnlich *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 22 mit Verweis auf den englischen Begriff „retrieval".

84 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 = NJW 2021, 531.

85 *Schild* in BeckOK Datenschutzrecht, DSGVO Art. 4 Rn. 48; *Ernst* in Paal/Pauly DSGVO/BDSG, DSGVO Art. 4 Rn. 29; *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 24; aA. *Reimer* in Sydow DSGVO, Art. 4 Rn. 67.

Dabei muss man sich stets vor Augen halten, dass Datenverarbeitungsvorgänge in der modernen Kommunikationsgesellschaft alltäglich sind. Sie finden universell statt – sowohl im sozialen als auch im wirtschaftlichen und öffentlichen (Verwaltungs-)Bereich. Es ist daher illusorisch, wenn man meint, stets selbst über deren Verwendung bestimmen zu können.[86] Dass aus den Grundrechten trotzdem ein Verdikt der Datensparsamkeit[87] abgeleitet wird, ja überhaupt ein Bestimmungsrecht über bestimmte Informationen entwickelt wurde, lässt sich weniger mit dem Schutz der Daten an sich, als aus den Risiken erklären, die die Datenverarbeitung mit sich bringen kann. Schon das BVerfG hatte dies im Volkszählungsurteil erkannt und auf diesen Verwendungszusammenhang hingewiesen.[88] Dennoch hat es grundsätzlich eine Linie eingeschlagen, die das Recht auf informationelle Selbstbestimmung als eigentumsähnliche Entscheidungsbefugnis über Preisgabe *und* Verwendung persönlicher Daten propagiert (s. unten II.2.).[89] Wie man sich eine solche Hoheit vorstellen soll, hat das Gericht aber nie überzeugend klären können.[90]

Um staatliche Überwachung daher als eigenständiges rechtliches Phänomen zu begreifen, muss die Bewertung verschiedener Datenverarbeitungskonstellationen vom Ende hergedacht werden, mithin vom Verwendungszweck der Maßnahmen.

86 *Schlink*, Der Staat 1986, 233 (243); *Hoffmann-Riem*, AöR 123 (1998), 513 (527 ff.); *Ladeur*, DÖV 2009, 45 (48 f.) *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121).

87 Vgl. *Schantz* in BeckOK Datenschutzrecht, DSGVO Art. 5 Rn. 24 ff.

88 BVerfGE 65, 1 – Volkszählung.

89 Vgl. Idem, (45 f.).; dazu *Vogelgesang,* Informationelle Selbstbestimmung, 1987, S. 139 ff. *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (132 f.); *Trute*, JZ 1998, 822 (825); aA. *Albers,* Informationelle Selbstbestimmung, 2005, 158 f., die eine solche Intention des BVerfG nicht erkennen mag; Übersicht bei *Placzek,* Informations- und Datenschutz, 2006, S. 80 ff.

90 Insbesondere *Albers,* Informationelle Selbstbestimmung, 2005, S. 236 ff; 280 ff.; s.a. *Hoffmann-Riem*, AöR 123 (1998), 513 (527 ff.); *Ladeur*, DÖV 2009, 45; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (131 ff.).; zum internationalen Kontext *Fairfield/Engel* in Miller (Hrsg.), Privacy and Power, 2017, S. 95 (104 ff.).

c. „Sicherheitsrechtliche“ Zwecke als Kern des Überwachungsbegriffs

Der maßgebliche Zweck einer jeden Überwachung im sozialwissenschaftlichen Sinn[91] hängt zunächst von der Person des Überwachenden ab. Die zeitgenössische Auseinandersetzung mit Überwachung betrifft nicht nur staatliche Überwachungsmaßnahmen, sondern adressiert immer mehr die *Überwachung* durch Private, insbesondere Internetkonzerne, die ihrer Natur nach auf eine große Menge persönlicher Daten Zugriff haben. Diese Form der Überwachung dürfte vornehmlich wirtschaftlichen Zwecken dienen.[92] Sie steht daher nicht im Fokus dieser Arbeit.

Staatliche Überwachungsmaßnahmen können verschiedene Zwecke verfolgen, insbesondere aber den Schutz der äußeren und inneren Sicherheit.[93] Es sind diese *sicherheitsrechtlichen* Fälle der Gewinnung, Vorhaltung und Analyse von Daten, die hier als eigenständiges Phänomen rechtlich gewürdigt werden sollen. Um sie von anderen Formen der Datenverarbeitung, insbesondere im Rahmen der Fachverwaltung, abzugrenzen, ist es sinnvoll, einen eigenen Terminus mit einer sensiblen Konnotation zu nutzen. Wenn hier von *Überwachung* die Rede ist, ist also allein die sicherheitsrechtliche Überwachung gemeint. Sie kann als Einzelmaßnahme erfolgen, wenn ein individueller Anlass vorliegt, oder systemisch ohne Anlass. In letzterem Fall kann von Massenüberwachung gesprochen werden. Was kein Gesetz vorsieht – und wegen des Willkürverbots auch nicht vorsehen dürfte – wäre eine individuell ausgerichtete Maßnahme ohne entsprechend konkreten Anlass. Wenn aber *sicherheitsrechtliche* Zwecke ausschlaggebend für die Bewertung bestimmter Kombinationen staatlicher Datenverarbeitungsvorgänge als Überwachung sind, sollte der Begriff des Sicherheitsrechts auch definiert werden.

Von diesem Rechtsgebiet ist – auch in dieser Arbeit – immer öfter die Rede, weshalb verschiedene Autoren sich jüngst nicht nur um eine Begriffs-

91 *Lyon,* Surveillance Studies, 2012, S. 14; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18 (19).

92 Dazu *Picot/Berchtold/Neuburger* in Kolany-Raiser/Heil/Orwat ua. (Hrsg.), Big Data & Gesellschaft, 2018, S. 309; *Skyrius/Giriūnienė/Katin ua.* in Srinivasan (Hrsg.), Big Data, 2018, S. 451; *Amnesty International,* Surveillance Giants, 2019, S. 8 ff.

93 Zum staatsrechtlichen Sicherheitsbegriff *Möstl,* Öfftl. Sicherheit, 2002, S. 3 ff., 126 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 11 ff.; *Bantlin,* Nachrichtendienste, 2021, S. 25 ff.

bestimmung bemüht haben, sondern auch um eine Erklärung, weshalb eine solche Definition notwendig ist.[94]

Einigkeit besteht darin, dass unter dem Begriff *Sicherheitsrecht* das Recht der Polizei, der Nachrichtendienste sowie das spezielle Ordnungsrecht, etwa das Versammlungs-, Melde- und Waffenrecht, zu subsumieren sind.[95] Korrekterweise ist aber auch das Straf- und Strafverfahrensrecht, das immer stärker mit dem Polizeirecht verzahnt wird, zum Sicherheitsrecht zu zählen.[96]

Von den verschiedenen Unterfangen zur Bestimmung des Sicherheitsrechts soll hier insbesondere jenes von *Gusy* kurz herausgestellt werden.[97] Nach ihm setzt sich das Sicherheitsrecht als Rechtsgebiet zusammen aus der *„Summe der Gesetze, welche Organisation und Handeln staatlicher oder privater Akteure auf dem Gebiet der Sicherheitsgewährleistung regeln"*.[98]

Der Begriff sei eine Sammelbezeichnung, über die ein Streit nicht lohne, da ein besserer Begriff noch nicht gefunden sei.[99] Gewinnbringend sei die Begriffsbestimmung nur dann, wenn aus der Einteilung bestimmter Normen in ein Rechtsgebiet auch etwas folge.[100]

Ob das für die hier angestrengte Untersuchung des Überwachungsbegriffs der Fall ist, könnte man zunächst bezweifeln, da von der Begriffsbestimmung wiederum nur die Begrifflichkeit der *Überwachung* abhängt, die selbst ja gerade nicht für die Sensibilität der hiermit beschriebenen Grundrechtsbeeinträchtigung ausschlaggebend ist. Die Notwendigkeit eines eigenen Begriffs der Überwachung ist gerade umgekehrt dem Bedürfnis einer semantischen Zusammenfassung verschiedener kritischer Verhaltensweisen geschuldet. Mit anderen Worten: Die TK-Vorratsdatenspeicherung wäre auch dann ein erheblicher Grundrechtseingriff, wenn man sie nicht als

94 *Graulich*, DVBl 2013, 1210; *Gärditz*, GSZ 2017, 1; *Gusy* in Dietrich/Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 9.

95 *Graulich*, DVBl 2013, 1210.

96 *Danne,* Prävention und Repression, 2022, S. 21 ff.; *Dietrich* in Dietrich/Fahrner/Gazeas ua. (Hrsg.), Hdb. Sicherheits- und StaatsschutzR, 2022, § 6 Rn. 49; *Götz* in Isensee/Kirchhof (Hrsg.), HdB StR Bd. IV, 3. Aufl. 2006, § 85 Rn. 5 f. *Gärditz*, GSZ 2017, 1 (2) mit Verweis in Fn 12 auf *Bäcker,* Kriminalpräventionsrecht, 2015; *Zöller,* Informationssysteme, 2002; aA *Graulich*, DVBl 2013, 1210, der allein auf den Zuständigkeitsbereich des 6. Senats des Bundesverwaltungsgerichts abstellt.

97 *Gusy* in Dietrich/Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 9.

98 Idem, (11).

99 Ibid.

100 Idem, (12 ff.).

Überwachung bezeichnete, und sie könnte mit der Fluggastdatenspeicherung auch dann verglichen werden, wenn man diese Maßnahmen nicht *a priori* einem einheitlichen Rechtsgebiet zugeordnet hätte. Im Gegenteil: Aus der Ähnlichkeit folgt letztlich die einheitliche Zuordnung.

Die Begriffsdiskussion um den Bereich des Sicherheitsrechts zur Klärung des Überwachungsbegriffs erscheint tautologisch, wenn man die sicherheitsrechtliche Relevanz zu dessen Komponente erhebt. Durch die gemeinsame Bezeichnung etwa verschiedener Maßnahmen als *Überwachung* kann aber doch eine gewisse Vorstellung über die Gemeinsamkeiten provoziert werden.

Auch Gusy sieht den Mehrwert der Einteilung von Rechtsnormen in Rechtsgebiete darin, dass sie den Vergleich verschiedener Normenkomplexe erleichtert.[101] Er schlägt drei Konzepte vor, nach denen sich Rechtsgebiete einteilen lassen könnten – darunter ein „deskriptives", das den gerade angestellten Überlegungen am ehesten Rechnung trägt. Danach bestimmt nicht das Rechtgebiet den Gegenstand, sondern der Gegenstand das Rechtsgebiet.[102] Es entstünden deskriptiv Perspektiven auf Vergleichbares und Unvergleichbares, was vor Verallgemeinerung schütze.[103] Das Sicherheitsrecht könne so der Vielfalt der ihm zugeordneten Rechtsnormen Rechnung tragen. Allerdings bleibe damit der Erkenntnisgewinn der Rechtseinteilung stets limitiert, da sich die entsprechenden Erkenntnisse unmittelbar auch aus den jeweiligen Gegenständen ableiten lassen könnten. [104]

Darin besteht aber kein Nachteil, wenn man den Nutzen der Rechtsgebietszuteilung in der Herstellung einer, auch semantischen, Ordnung erkennt[105] – gewissermaßen als sprachliche Indikation, mit der gewisse Erkenntnisse von vorneherein aufgedrängt werden.[106] Solche Erkenntnisse sind hier etwa, dass der sicherheitsrechtlich geprägte Überwachungsbegriff sowohl die Fachverwaltung als auch privatwirtschaftliche Datenverarbeitungsvorgänge ausschließt. Es muss nicht mehr im Einzelnen erläutert werden, wieso die gefahrenabwehrrechtliche Telekommunikationsüberwa-

101 Idem, (13 f.).
102 Idem, (17 ff).
103 Idem, (19).
104 Idem, (20).
105 Vgl. *Tanneberger,* Sicherheitsverfassung, 2014, S. 12; allg. *Schmidt-Aßmann,* Verwaltungsrecht, 2. Aufl. 2006, S. 8 f.
106 Ähnlich den Familienähnlichkeiten von *Wittgenstein,* Philosophische Untersuchungen, 1971, S. 56 ff; lfd. Nr. 65 ff.; dazu *Wennerberg* in Savigny (Hrsg.), Wittgenstein's PU, 2. Aufl. 2011, S. 33.

chung mit jener der Strafverfolgungsbehörden oder der Zollfahndung vergleichbar ist und rechtlich entsprechend gewürdigt werden kann, während sie sich von der Speicherung i. R. d. Wirtschafts- oder (Fach-)Verwaltung unterscheidet. Die Vergleichbarkeit wird durch die einheitliche Zuordnung stipuliert und kann von dem Adressaten der Aussage notfalls überprüft werden.

3. Zusammenfassung

Wenn der Begriff der Überwachung als Umschreibung verschiedener, rechtlich besonderes relevanter Kombinationen von Datenverarbeitungsschritten verwendet werden soll, muss er stets bestimmte Elemente enthalten. Dies ist notwendig, da *Überwachung* als sozialwissenschaftliches Phänomen eine Vielzahl verschiedener Lebenssachverhalte beschreiben kann, die keiner einheitlichen rechtlichen Betrachtung unterliegen. So unterscheiden sich private Überwachungsmaßnahmen großer Unternehmen grundlegend von jenen der staatlichen Sicherheitsapparate. Natürlich geht es in beiden Fällen darum, wer was über wen weiß, doch die Vorstellung, den gesellschaftlichen Informationsfluss einheitlich verrechtlichen zu können, ist schon im Grundsatz illusorisch.[107] Die verschiedenen Datenverarbeitungsvorgänge sind daher nach ihrem Zweck zu trennen, um sie dann im Rahmen der jeweiligen Rechtsgebiete würdigen zu können.

Die sicherheitsrechtlich motivierte Datenerhebung mit anschließender Analyse und/oder Speicherung der gewonnenen Daten muss daher als eigenständige Überwachungsform behandelt werden. Der Begriff des Sicherheitsrechts ist dabei deskriptiv zu verstehen.[108] Ob eine Maßnahme ihren sicherheitsrechtlichen Zweck verfolgt, ergibt sich nicht daraus, dass die dahinterstehende gesetzliche Regelung a priori dem Sicherheitsrecht zugeordnet wird, sondern aus der Ähnlichkeit und der damit einhergehenden Vergleichbarkeit zu anderen sicherheitsrechtlichen Maßnahmen. Dazu zählen insbesondere das Recht der Nachrichtendienste, das Polizeirecht und das Strafverfahrensrecht, deren Überwachungsmaßnahmen sich diese Arbeit widmet.

---

107 Vgl. *Hoffmann-Riem*, AöR 123 (1998), 513 (527 ff.); *Ladeur*, DÖV 2009, 45 (48 f.) *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121) .

108 *Gusy* in Dietrich/Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 9 (S. 17 ff.).

II. Kurzübersicht: Schutz vor Überwachung im Grundgesetz

Sicherheitsrechtliche Überwachungsmaßnahmen sind heute als eine grundrechtsrelevante Form der Eingriffsverwaltung vollständig anerkannt. Es steht nicht infrage, ob sie in Grundrechte eingreifen, sondern in welche.

Da das Grundgesetz die Privatheit per se nicht ausdrücklich schützt, hat das BVerfG in seiner Rechtsprechung erst herausarbeiten müssen, inwiefern die Grundrechte vor Überwachung schützen. Dabei hat sich eine zweigeteilte Systematik entwickelt, die aus einem bereichsspezifischen und einem allgemeinen Schutz vor Informationseingriffen besteht.[109]

1. Bereichsspezifischer Überwachungsschutz: Art. 10 Abs. 1 GG, 13 Abs. 1 GG und das „IT-Grundrecht"

Beziehen sich Überwachungsmaßnahmen auf bestimmte Informationen bzw. Lebensbereiche, die eigens von den Grundrechten geschützt sind, kann von einem bereichsspezifischen Überwachungsschutz gesprochen werden. Der Grundrechtsschutz bezieht sich hier nicht unmittelbar auf Informationen, sondern auf die Sphäre, in der die Informationen offenbart werden.

Zum bereichsspezifischen Überwachungsschutz zählen das Brief-, Post- und Fernmeldegeheimnis nach Art. 10 Abs. 1 GG, die Wohnung nach Art. 13 Abs.1 GG[110]und die Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (im Folgenden „IT-Grundrecht").[111]

109 *Bäcker*, Der Staat 2012, 91 (94 ff.).

110 „spezielle Gewährleistung der Privatsphäre" BVerfG, NJW 2016, 3508 (3511 Rn. 42); zur Verbindung in dieser Hinsicht von Art. 10 Abs.1 und Art. 13 Abs. 1 GG *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 19 Rn. 965; s.a. *Albers,* Informationelle Selbstbestimmung, 2005, 370 ff.

111 So *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (118 ff.); *Hauser,* IT-Grundrecht, 2015; s.a. *Dreier* in Dreier GG, Art. 2 Abs. 1 Rn. 82, Fn 386 mwN; krit. zum Begriff *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 22.

a. Allgemeine Reichweite des bereichsspezifischen Überwachungsschutzes

Art. 10 Abs. 1 GG schützt die zwischenmenschliche Kommunikation unter Abwesenden.[112] Grund des Schutzes ist also nicht unmittelbar das Interesse der Betroffenen an der Privatheit des Kommunikationsinhalts, wenngleich dieser natürlich subsidiär mitgeschützt wird, sondern das Vertrauen auf die Integrität des technisch unterstützten Kommunikationsvorgangs bzw. -mediums.[113] Geschützt werden alle tatsächlichen Teilnehmer des Kommunikationsvorgangs.[114]

Dabei handelt es sich beim Brief-, Post- und Fernmeldegeheimnis nach herrschender Auffassung nicht um ein Grundrecht, sondern drei nebeneinander bestehende Grundrechte mit jeweils eigenem Schutzbereich, die aber eng miteinander verwandt sind.[115] Sie alle haben gemeinsam, dass allein die Kommunikationsübertragung geschützt wird.

Die Schutzbereiche zeichnen sich also durch ein zeitliches Element aus. Der Schutz beginnt in dem Moment, in dem das Kommunikationsobjekt den Herrschaftsbereich des Absenders verlässt, und endet, sobald er sich gesichert im Herrschaftsbereich des Empfängers befindet.[116] Bei der Eingriffsbestimmung stellt das BVerfG allerdings allein darauf ab, dass sich der Eingriff auf Informationen bezieht, die im Rahmen der Übertragung angefallen sind, auch wenn sich seine Folgen erst nach der Übertragung verwirklichen.[117] Die Abfrage von Telekommunikationsdaten beim Dienstеanbieter stellt daher stets einen Eingriff in Art. 10 Abs. 1 GG dar.[118]

Eine weitere Form bereichsspezifischen Schutzes vor Überwachung gewährleistet Art. 13Abs. 1 GG, der die Unverletzlichkeit der Wohnung sta-

112 *Gusy* in v. Mangoldt/Klein/Starck GG, Art. 18 Rn. 44; *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 10 Rn. 1.

113 BVerfGE 100, 313 (358 f.) – Strategische Fernmeldeaufklärung; *Hermes* in Dreier GG, Art. 10 Rn. 33; *Albers,* Informationelle Selbstbestimmung, 2005, S. 371.

114 OVG Münster, NJW 1975, 1335; *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 129.

115 *Gusy* in v. Mangoldt/Klein/Starck GG, Art. 10 Rn. 45; *Hermes* in Dreier GG, Art. 10 Rn. 25 mwN; aA. *Schoch* JURA 2011, 194 (195).

116 Vgl. BVerfGE 115, 166 (183); Problematisch insbesondere bei Emails, dazu *Graf* in BeckOK StPO, § 100a Rn. 51 ff.; *Brodowski*, JR 2009, 402.

117 BVerfGE 120, 274 (307 f.) – Online-Durchsuchung; *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 85.

118 BVerfGE 107, 299 (313 f.); E 125, 260 (309 ff.) – Vorratsdatenspeicherung *Sieber/Brodowski* in Hoeren/Sieber/Holznagel (Hrsg.), Hdb. Multimedia-Recht, 2020, Teil 19.3 Rn. 120 mwN.

tuiert. Auch hier handelt es sich nicht unmittelbar um den Schutz von Informationen, sondern um einen speziellen Bereich, in den grundsätzlich nicht zur Gewinnung von Informationen eingedrungen werden soll, eine Art „räumlicher Privatsphäre".[119]

b. Überwachungsschutz von Finanzinformationen i. R. d. bereichsspezifischen Überwachungsschutzes

Für die hier untersuchten Finanzinformationen sind Art. 10 Abs. 1, Art. 13 Abs. 1 GG und das IT-Grundrecht von geringer Bedeutung, da diese gerade nicht den allgemeinen Datenschutz, sondern nur konkrete Übertragungswege und die Wohnung bzw. IT-Geräte als räumliche Sphäre schützen.

Die Unverletzlichkeit der Wohnung ist denkbar nur betroffen, wenn verkörperte Finanzdaten, etwa Kontoauszüge in Papierform, oder digitale Speichermedien aus einem nach Art. 13 Abs. 1 GG geschützten Raum beschlagnahmt werden. Dazu zählen auch die nicht allgemein zugänglichen Geschäftsräume, solange sich dort Menschen regelmäßig aufhalten. Beschlagnahmungen bzw. Durchsuchungen bei einer Bank beeinträchtigen das Bankunternehmen also in Art. 13 Abs. 1 GG (i. V. m. Art. 19 Abs. 3 GG)[120] – nicht jedoch den (mit)betroffenen Kunden. Bei Bankschließfächern handelt es sich von vorneherein nicht um Wohnungen, da es am regelmäßigen Aufenthalt fehlt.[121]

Vor der Einführung des Rechts auf die Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (dazu gleich) war noch umstritten, ob Art. 13 Abs. 1 GG auch vor einem technischen Zugriff auf sich in der Wohnung befindende Speichermedien schützt.[122] Das BVerfG hat dies abgelehnt.[123] Digitale Kontodaten, die sich auf einem Medium in einer Wohnung befinden, können also nur über Art. 13 Abs. 1 GG Schutz

119 BVerfGE 65, 1 (40) – Volkszählung; E 109, 279 (309, 325) – Großer Lauschangriff; *Papier* in Dürig/Herzog/Scholz GG, Art. 13 Rn. 4; *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 22 Rn. 1086.

120 Vgl. *Krepold/Zahrte* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 8 Rn. 231 ff.

121 BVerfG, Beschl. v. 16.10.2002 - 2 BvR 1306/02.

122 So etwa *Rux*, JZ 2007, 285 (292 ff.); *Kutscha*, NJW 2007, 1169 (1170 ff.) *Buermeyer*, HRRS 2007, 329 (332 ff.); *Hornung*, JZ 2007, 828; aA. *Germann,* Internet, 2000, S. 540 ff.; *Beulke/Meininghaus*, StV 2007, 60 (64).

123 BVerfGE 120, 274 (310 f.) – Online-Durchsuchung.

erfahren, wenn das körperliche Medium aus der Wohnung beschlagnahmt wird.

Wenn mittels einer Online-Durchsuchung auf gespeicherte Finanzinformationen zugegriffen wird, liegt ein Eingriff in das IT-Grundrecht vor. Aufgrund der hohen Anforderungen hat die Online-Durchsuchung in diesem Bereich aber keine große praktische Bedeutung. Stattdessen werden die Daten direkt von den kontoführenden Finanzdienstleistern abgegriffen, was mit deutlich weniger strengen Maßnahmen möglich ist[124] (dazu unten Kap. E.).

Nur geringe Spielräume bestehen auch für eine Anwendung des Art. 10 Abs. 1 GG in Bezug auf Kontodaten. Werden diese postalisch an den Kunden versandt, kommt eine Verletzung des Briefgeheimnisses in Betracht, wenn der Brief abgefangen und geöffnet wird oder beim Boten oder dem Absender Auskünfte über die Sendungen eingeholt werden. Auch aufgrund der immer stärkeren Verwendung von Online-Banking[125] dürften postalisch versandte Kontoauszüge aber eine immer geringere Rolle spielen und sind auch schwierig abzufangen.

Da die Finanzinformationen stets beim Absender verbleiben, ist ein Datenzugriff ohnehin stets auch unmittelbar bei den Instituten möglich. Die dortigen Dateibestände bestehen unabhängig von der Übermittlung an die Kunden und sind daher nach herrschender Auffassung nicht durch das Fernmeldegeheimnis geschützt.[126]

Das muss man nicht zwingend für überzeugend halten. Man könnte durchaus Speicherpflichten über den Zahlungsverkehr und damit einhergehende staatliche Zugriffe als Eingriff in das Fernmeldegeheimnis deuten, wenn man Zahlungen grundsätzlich als (geschützte Fern-)Kommunikation begreifen würde.[127]

Eine Überweisung ist nichts anderes als eine Reihe kommunikativer Vorgänge, die im digitalen Zahlungsverkehr über Signale abgewickelt wer-

124 Siehe nur *F. Jansen,* Bankauskunftsersuchen, 2010; *Kahler,* Kundendaten, 2017; *Reichling*, JR 2011, 12; *Wonka*, NJW 2017, 3334.

125 Vgl. *Deutsche Bundesbank,* Zahlungsverhalten in Deutschland, 2017, S. 8 ff.; *Borges* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 11 Rn. 6.

126 Vgl. BVerfG, NJW 2009, 1405.

127 So für das Online-Banking *Singelnstein*, NStZ 2012, 593 (594 f.); aA. *Böckenförde*, JZ 2008, 925 (937 f.).

den.[128] Bei einer Kartenzahlung vor Ort weist bspw. der Zahler seine Bank an, eine Überweisung an ein bestimmtes Institut zu einem gewissen Zweck zu tätigen. Dabei müssen zwangsweise persönliche Informationen wie der Name von Zahler und Begünstigte sowie der Verwendungszweck, Datum etc. übermittelt werden (zur EU-ZahlungsdiensteRL[129], GeldtransferVO[130] und der SEPA-VO[131] siehe Kap. D. II. 2.). Die Überweisung zwischen den Banken ist ebenfalls ein kommunikativer Akt, bei dem Informationen über die jeweils zwischen den Banken bestehenden Salden ausgetauscht werden.[132] Auch Bareinzahlungen an einem Automaten sind ein kommunikativer Akt, bei dem der Kunde sein Institut anweist, einen gewissen Betrag seinem Konto gutzuschreiben. Dass es sich hierbei vor allem um wirtschaftlich relevante Informationen handelt, spielt für den inhaltsindifferenten Art. 10 GG keine Rolle.[133]

Im Ergebnis dürfte der Rechtsprechung, die digitale Bankvorgänge nicht unter den Schutz des Art. 10 Abs. 1 GG stellt, jedoch zuzustimmen sein. Der automatisierte Zahlungsprozess ist gerade dazu gedacht, eigentlich notwendige Kommunikation obsolet zu machen. Anstatt dem Bankmitarbeiter mitzuteilen, er solle eine Zahlung an das Konto einer bestimmten Person „X" mit dem Verwendungszweck „Y" veranlassen, reicht es, diese Informationen in ein technisches Zahlungssystem einzugeben und den

128 *Köndgen*, JuS 2011, 481; *Korff* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 45 Rn. 11 ff.

129 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG, ABl. 2007 L 319/1; neu gefasst durch Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/E, ABl. 2015, L337/35.

130 Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006, Abl. 2015, L 141/1.

131 Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009, ABl. 2012 L 94/22.

132 *Korff* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 45 Rn. 69 ff.

133 BVerfGE 67, 157 (172) – G-10; *Hermes* in Dreier GG, Art. 10 Rn. 41.

Informationsaustausch den Rechnern zu überlassen.[134] Man befindet sich also in einem Zwischenbereich von menschlicher Kommunikation und automatisierter Datenverarbeitung.[135]

Informationen sind dabei stets das Ergebnis von Kommunikation.[136] Auch verschiedene Speicherpflichten betreffen Informationen, die die jeweiligen Institute durch einen kommunikativen Akt erhalten, etwa eine Kontoeröffnung oder ein Telefonvertragsschluss, die beide eine Speicherung der Vertragsdaten nach sich ziehen. Geschieht dies nun unter Abwesenden könnte man auch hier das Fernmeldegeheimnis in Stellung bringen, denn verarbeitet werden zwangsweise die (fern-)kommunizierten Daten.

Das BVerfG ist diesen Weg zu Recht nicht gegangen[137], denn er ließe eine Abgrenzung von reinem Informationsschutz und spezifischem Kommunikationsschutz kaum mehr zu. Dem Versuch, jedwede Information auf ihren Ursprung als Kommunikationsergebnis zu rekonstruieren, um den Schutzbereich des Art. 10 Abs. 1 zu eröffnen, muss man widerstehen. Jede Speicherpflicht ließe sich ansonsten als Verarbeitung eines Kommunikationsumstands oder -inhalts darstellen. Der damit einhergehende universale Kommunikationsschutz würde den Schutzzweck des Fernmeldegeheimnisses sprengen. Art. 10 Abs. 1 GG schützt das Vertrauen in die Integrität bestimmter Kommunikationsvorgänge und nicht allgemein vor dem medialen Festhalten bestimmter alltäglicher Vorgänge, auch wenn sich diese als digitale Kommunikationsakte darstellen lassen. [138] Speicherpflichten über Zahlungsvorgänge oder Kontoeröffnungen sind daher nicht dem Schutz des Fernmeldegeheimnisses zu unterstellen, auch wenn sie mit digitalen Mitteln vollzogen werden.

134 Zum Kartenzahlungssystem *S. Kröger* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 47 Rn. 17 ff.
135 *Singelnstein*, NStZ 2012, 593 (594 f.).
136 *Albers,* Informationelle Selbstbestimmung, 2005, S. 87 f.
137 BVerfGE 118, 168 (183 ff.) – Kontostammdaten; E 130, 151 (181 f.) – Bestandsdatenauskunft I; E 155, 119 (168 f.) – Bestandsdatenauskunft II; *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 113.
138 *Böckenförde*, JZ 2008, 925 (937 f.).

2. Allgemeiner Überwachungsschutz: Die informationelle Selbstbestimmung

Allgemeinen Schutz vor Überwachung bietet das Recht auf informationelle Selbstbestimmung, bei dem es sich um einen Unterfall[139] des Allgemeinen Persönlichkeitsrechts (APR) aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1[140] GG handelt.

Das APR ist ein Rahmenrecht, das verschiedene (Teil-)Gewährleistungen umfasst.[141] Zusammenfassend lässt es sich als Recht der Grundrechtsträger beschreiben, ihre Persönlichkeit möglichst frei zu entfalten. Hierfür ist ein Rückzugsraum und die Möglichkeit, „für sich zu sein"[142] unerlässlich (Privatheitsschutz).[143] Außerdem sollen die Grundrechtsträger selbstbestimmt über die öffentliche Darstellung ihrer Persönlichkeit entscheiden können (Selbstdarstellungsschutz).[144]

Im Volkszählungsurteil[145] hat das BVerfG diesen Aspekt der Selbstbestimmung auf Daten erweitert und wie folgt argumentiert. Moderne Datenverarbeitungssysteme beherbergten die Gefahr, persönliche Daten so zu kumulieren, dass umfangreiche Persönlichkeitsprofile erstellt werden könnten. Solche Profile öffneten der Manipulation Tür und Tor, die faktisch ein selbstbestimmtes Leben vereitelten. Insofern käme es zu einem typischen Übergang[146] von Selbstdarstellung zu Selbstbestimmung[147]. Die (psychologischen) Effekte der Fremdwahrnehmung durch Datenverarbeitung beeinträchtigten die Freiheit zum selbstbestimmten Handeln.

---

139 BVerfGE 65, 1 (41 ff.) – Volkszählung.

140 Zur Verortung krit. *Lorenz*, JZ 2005, 1121 (1124 f.); *Kube* in Isensee/Kirchhof (Hrsg.), Hdb. StR Bd. VII, 3. Aufl. 2009, § 148 Rn. 31 ff. *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 52 mwN; nach *Dreier* in Dreier GG, Art. 2 Rn. 69 Fungiert Art. 1 Abs. 1 GG als „programmatische Leit- und Auslegungsrichtlinie"; ähnlich *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 89.

141 *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 147 f.; *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 53; *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 8 Rn. 511 ff.

142 *Kube* in Isensee/Kirchhof (Hrsg.), Hdb. StR Bd. VII, 3. Aufl. 2009, § 148 Rn. 129.

143 BVerfGE 27, 1 (6) – Mikrozensus; E 54, 148 (153 f.); *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 58 f.; „Recht der Selbstbewahrung" bei *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 8 Rn. 512 ff.

144 BVerfGE 35, 202 (220 ff.); *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 166 ff.

145 BVerfGE 65, 1 (41 ff.) – Volkszählung.

146 Vgl. *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 148.

147 Ausf. zum Zusammenhang von Selbstdarstellung und -Entfaltung *Britz,* Entfaltung durch Selbstdarstellung, 2007.

Um sich hiervor zu schützen, muss dem Betroffenen grundsätzlich das Recht zugestanden werden, „*selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*".[148] Ein Eingriff liegt deshalb immer vor, wenn staatliche Stellen persönliche Daten *verarbeiten,* also *erheben*, *speichern*, *verwenden* oder *weitergeben*,[149] wobei jeder Datenverarbeitungsschritt einen eigenständigen Eingriff darstellt (s. o.).[150]

Diese Konzeption der informationellen Selbstbestimmung wird von Teilen der Literatur aufgrund der angedeuteten Verfügungshoheit als Analogie zum Eigentumsrecht verstanden und entsprechend kritisiert.[151] Das BVerfG strebe eine Selbstbestimmung über persönliche Informationen an, die es aber naturgemäß gar nicht geben könne.[152] Informationen entstünden erst durch Kommunikation, weshalb eine Verfügungsgewalt über das Wissen Anderer – auch im Hinblick auf die Informationen über den Betroffenen – illusorisch sei. [153]

148 BVerfGE 65, 1 (43) – Volkszählung; aus der jüngeren Rspr: E 156, 11 (39) – Antiterrordatei II; *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 175 mwN; *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 17 jeweils mwN.

149 BVerfGE 115, 320 (341) – Rasterfahndung; E 130, 151 (183 f.) – Bestandsdatenauskunft I jeweils mwN; s.a. *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 76; als Ansatzpunkt kann der Verarbeitungsbegriff aus Art. 4 Nr. 2 DSGVO dienen; vgl. *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 18; *Schoch* JURA 2008, 352 (356) (zu § 3 BDSG a.F.); zum Verhältnis von Art. 4 Nr. 2 DSGVO und Art. 8 EU-Charter: *Kingreen* in Callies/Ruffert EUV/AEUV, EU-Charter Art. 8 Rn. 13.

150 BVerfGE 150, 244 (265 f.) – Autom. Kennzeichenkontrolle II; ebenso EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 124 – PNR Canada = ZD 2018, 23; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR) = EuZW 2022, 706.

151 *Vogelgesang,* Informationelle Selbstbestimmung, 1987, S. 139 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (131 ff.); *Britz* in Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.); *Placzek,* Informations- und Datenschutz, 2006, S. 80 f.; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Ladeur*, DÖV 2009, 45; *Trute*, JZ 1998, 822; *Hoffmann-Riem*, AöR 123 (1998), 513 (528); *J.-P. Schneider* in BeckOK Datenschutzrecht, Grundlagen Syst. B Rn. 25.1; keine Eigentumsanalogie erkennt *Albers,* Informationelle Selbstbestimmung, 2005, S. 158 f.

152 *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (16 f.); *dies.,* Informationelle Selbstbestimmung, 2005, S. 113 ff., 437 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (S. 136 ff.); *Placzek,* Informations- und Datenschutz, 2006, S. 92 ff.; *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, 2.5 Rn. 19; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121).

153 *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (16 f.); *dies.,* Informationelle Selbstbestimmung, 2005, S. 113 ff., 437 ff.; *Placzek,* Informations- und Datenschutz, 2006, S. 92 ff.; *Poscher* in Miller (Hrsg.),

Der Versuch, eine allgemeine Informationshoheit zu etablieren, führe in der Konsequenz dazu, dass das Datenschutzrecht als Datenverarbeitungsverbot mit Erlaubnisvorbehalt[154] konzipiert werden muss. Da die Verarbeitung von Informationen den Gegenstand jeglicher Kommunikation darstellt, würde letztlich nur der Alltag verrechtlicht und kein Grundrecht geschützt.[155]

Ausgehend von dieser Kritik werden verschiedene Alternativen zum Verständnis der informationellen Selbstbestimmung vorgeschlagen. Allen Konzeptionen gemein ist ihr Ziel, grundrechtlichen Schutz vor staatlichen Überwachungsmaßnahmen zu gewährleisten. Die Ansätze unterscheiden sich nur in der Konstruktion der Grundrechtseingriffe, kommen aber doch stets zu dem Ergebnis, dass die Grundrechte vor staatlichen Informationseingriffen schützen sollen.[156]

Auch im Ergebnis haben sich die Rechtsprechung und Literatur, soweit dort die informationelle Selbstbestimmung als systematischer Gewährleistungskomplex verstanden wird, angenähert. Das BVerfG bestimmt zwar weiterhin den Eingriff als solchen danach, ob Daten überhaupt verarbeitet werden und die Eingriffsintensität danach, welche und wie viele Daten verarbeitet werden (siehe unten III. 2. B.).[157] Es versteht aber die Verhältnismäßigkeitsprüfung nicht mehr als schlichte Rationalitätskontrolle, sondern zur konkreten Ausarbeitung formeller und materieller Voraussetzungen und anderer gesetzlicher Schutzvorkehrungen.[158] Im Rahmen dieser „Handlungsanleitungen"[159] für den Gesetzgeber manifestiert sich letztlich die Vorstellung, dass die informationelle Selbstbestimmung keine Informa-

---

Privacy and Power, 2017, S. 129 (S. 136 ff.); *Britz* in Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.); *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, 2.5 Rn. 19; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121); *Schlink*, Der Staat 1986, 233 (243).

154 *Bull,* Netzpolitik, 2013, S. 136 ff.; *Weichert*, DuD 2013, 246; „zum einfachrechtlichen Verbot mit Erlaubnisvorbehalt" *Buchner/Petri* in Kühling/Buchner DSGVO/BDSG, DSGVO Art. 6 Rn. 1; krit. dazu *Roßnagel*, NJW 2019, 1; *Albers/Veit* in BeckOK Datenschutzrecht, DSGVO Art. 6 Rn. 11.

155 *Hoffmann-Riem*, AöR 123 (1998), 513 (528); *Bull,* Netzpolitik, 2013, 136 ff.

156 Im Ergebnis auch *Thiel,* Entgrenzung, 2012, S. 264 ff.

157 Siehe nur BVerfGE 118, 168 (196) – Kontostammdaten mwN. aus der Rspr.

158 Siehe nur *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *ders.*, Die Verwaltung 2008, 345; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84; *Gurlit*, NJW 2010, 1035 (1037 ff.).

159 *Schluckebier* abw. Meinung BVerfGE 125, 260 (373).

tionshoheit realisiert, sondern einen gewissen Standard der Art und Weise staatlicher Informationsverarbeitung gewährleistet.[160]

Unabhängig vom weiterhin geführten Streit um die Dogmatik der informationellen Selbstbestimmung gilt also, dass die sicherheitsrechtliche Verwendung von Finanzdaten bestimmten Grenzen unterliegen muss, die sich kohärent aus der bestehenden Rechtsprechung zu vergleichbaren Überwachungsmaßnahmen ableiten lassen müssen.

III. Überwachungsmaßnahmen in der Rechtsprechung des BVerfG

Diesen grundgesetzlichen Überwachungsschutz hat das BVerfG in den letzten Jahren ausführlich elaboriert. Es liegt nunmehr eine ganze Reihe an Urteilen vor, in denen konkrete Maßnahmen und ganze Gesetzespakete zur Regelung der Überwachungsbefugnisse von Sicherheitsbehörden umfassend überprüft wurden. In diesen Urteilen hat das BVerfG nicht nur grundsätzliche Aussagen zur sicherheitsrechtlichen Überwachung aufgestellt, sondern im Rahmen der Verhältnismäßigkeitsprüfung ein nuanciertes Anforderungssystem für verschiedene Maßnahmen ersonnen.[161]

In jüngerer Zeit sind einige Versuche unternommen worden, die Rechtsprechung des BVerfG zu den verschiedenen Teilbereichen des Sicherheitsrechts als kohärentes System darzustellen.[162] Die Anforderungen des Gerichts – insbesondere an die materiellen Eingriffsschwellen in den einzelnen Gesetzen der Sicherheitsbehörden – legen in der Tat nahe, dass das Gericht ein einheitliches „Baukastensystem" für die Entwicklung der Sicherheitsgesetzgebung etablieren will.

160 Vgl. *Albers,* Informationelle Selbstbestimmung, 2005, 447 ff.; *dies.* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (26 ff.).

161 Siehe nur *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *ders.*, Die Verwaltung 2008, 345; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84; *Gurlit*, NJW 2010, 1035 (1037 ff.).

162 *Tanneberger,* Sicherheitsverfassung, 2014, S. 362 ff.

1. Grundlinien zu Überwachungsmaßnahmen in der Rechtsprechung des BVerfG

Bei der Bewertung der rechtlichen Zulässigkeit bestimmter Maßnahmen ist das BVerfG davon abgerückt, grundsätzliche Aussagen zu treffen. Anstatt den verschiedenen Sicherheitsbehörden aufgrund einer vermeintlichen Unverhältnismäßigkeit einzelne Befugnisse zu verbieten, ist das Gericht dazu übergegangen, aus dem Grundsatz der Verhältnismäßigkeit konkrete Schwellen und andere Anforderungen für die einzelnen Eingriffe abzuleiten.[163]

Das BVerfG hat in den letzten Jahren einen ganzen Katalog an Eigenschaften herausgearbeitet, die die Intensität einer Überwachungsmaßnahme beeinflussen.[164] Auf dessen Grundlage werden Eingriffe sodann mittels einer recht gefestigten Kasuistik in ein Stufenmodell eingeordnet.[165] Am unteren Ende stehen die „geringfügigen Eingriffe".[166] In der Mitte finden sich die Eingriffe „von erheblichem Gewicht"[167] und am schwersten wiegen die „tiefgreifenden"[168] Eingriffe bzw. Eingriffe von „hoher Intensität."[169]

---

163 Insbesondere BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84: "Operationalisierung der Verhältnismäßigkeit"; *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff.); *Volkmann*, NVwZ 2022, 1408 (1411): „Steuerungsmodell"; *Trute*, Die Verwaltung 2009, 85 (85 ff; 96 ff.); *Schoch*, Der Staat 2004, 347; *Groß* KJ 2002, 1 (9 ff.) allg. *Bumke* in Hoffmann-Riem (Hrsg.), Innovationen im Recht, 2016, S. 115 (133 ff.); *ders.,* Grundrechtsvorbehalt, 1998, 100 ff., 235 ff.; allg. krit. zur „Maßstabssetzung" des BVerfG *Lepsius* in Jestaedt/Lepsius/Möllers ua. (Hrsg.), Entgrenztes Gericht, 2011, S. 159.

164 Übersichtlich *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff.; *Poscher/Kilchling/Landerer*, GSZ 2021, 225 (230 ff.); *Löffelmann*, GSZ 2019, 16 (19); *F. Braun/F. Albrecht* VR 2017, 151 (152); *Hornung/Schnabel*, DVBl 2010, 824 (826).

165 Dreistufiges Modell nach *Rusteberg*, KritV 2017, 24 (29 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff. erkennt vier Intensitätsstufen; krit. zur Aussagekraft der Nomenklatur *Tanneberger,* Sicherheitsverfassung, 2014, S. 234 f.

166 BVerfGE 67, 157 (179) – G-10; siehe auch VGH Mannheim, NVwZ-RR 2011, 231 (233)

167 BVerfGE 150, 244 (283) – Autom. Kennzeichenkontrolle II.

168 BVerfGE 141, 220 (267 ff.) – BKA-Gesetz.

169 BVerfGE 120, 274 (322) – Online-Durchsuchung.

Primäre Intensitätsaspekte sind die verarbeitete Datenmenge und -qualität, Heimlichkeit und Streubreite einer Maßnahme.[170] Es ist ein Erfordernis des Verhältnismäßigkeitsgrundsatzes, dass diesen intensivierenden Merkmalen durch kompensierende Vorkehrungen begegnet wird. Je intensiver sich eine Maßnahme nach den beschriebenen Merkmalen darstellt, desto stärker müssen die Kompensationsvorkehrungen sein.[171]

Dieser Ansatz des BVerfG hat dazu geführt, dass die Urteile[172] zu den jüngsten Novellierungen der Sicherheitsgesetze immer umfassender geworden sind, da das Gericht letztlich die Tatbestandsvoraussetzungen einzelner Eingriffsmaßnahmen selbstständig neu aufsetzt. Anstatt sich mit der für den Einzelfall konstruierten Rationalitätskontrolle abzumühen, versteht es den Verhältnismäßigkeitsgrundsatz bzw. die Angemessenheit im Sicherheitsrechts als Auftrag zur interpretatorischen Fortentwicklung rechtlicher Überwachungsmaßstäbe.[173]

Eine rein auf die Verwerfung oder Aufrechterhaltung von Gesetzen gerichtete Vorgehensweise wäre auch nicht praktikabel. Die Anforderungen an die Ausgestaltung der sicherheitsrechtlichen Überwachungsmaßnahmen sind mittlerweile so fein, dass der Gesetzgeber etliche Anläufe bräuchte. Schon deshalb muss das BVerfG die Anforderungen, die es jeweils für eine angemessene Ausgestaltung als notwendig erachtet, konkret benennen.[174] Dies führt zwar in der Tat dazu, dass das BVerfG dem Gesetzgeber letztlich „Handlungsanleitungen" zur Gesetzgebung im Sicherheitsrecht vorlegt,

170 Übersichtlich *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff.; *Poscher/Kilchling/Landerer*, GSZ 2021, 225 (230 ff.); *Löffelmann*, GSZ 2019, 16 (19); *F. Braun/F. Albrecht* VR 2017, 151 (152); *Hornung/Schnabel*, DVBl 2010, 824 (826).

171 *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.; *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 116; früh schon *Vahle,* Aufklärung, 1983, S. 94 ff., 130.

172 Jüngst etwa; BVerfGE 154, 152 – Ausland-Ausland-Fernmeldeaufklärung; E 155, 119 – Bestandsdatenauskunft II; BVerfG, NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz;
NJW 2023, 1196 – Polizeiliche Datenanalyse.

173 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82.

174 *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. D Rn. 253; mit Verweis zur Gegenmeinung bei *Schöndorf-Haubold*, Sicherheit und Freiheit im Polizeirecht, 2014 (noch nicht veröffentlicht).

was durchaus an „judicial activism" grenzt.[175] Eine bessere Lösung, die rechtsstaatlich gebotene Abwägung von Sicherheit und Freiheit (vor Überwachung) praktikabel vorzunehmen, ist aber trotz aller Kritik noch nicht gefunden.[176]

Die „Handlungsanleitungen" drücken sich für Informationserhebungen als ausdifferenzierte Je-Desto-Formel[177] aus und sind somit eine Vorwegnahme der dem Gericht zugewiesenen Verhältnismäßigkeitsprüfung. Ausgehend von der systematisch bestimmten Intensitätsstufe einer Maßnahme wird – teilweise recht pauschal – eine Vielzahl spezifischer Anforderungen als Ergebnis der Verhältnismäßigkeitsprüfung entwickelt. So dürfen „besonders schwerwiegende Maßnahmen" nur bei konkretisierter Gefahr bzw. spezifischem Verdacht einer schweren Straftat und nur unter Richtervorbehalt angeordnet werden. Ebenso wie es Art. 13 Abs. 4 GG für den großen Lauschangriff vorsieht. Letztlich zeichnet das BVerfG also die Idee unmittelbar geltender Eingriffsanforderungen in der Verfassung nach und stützt sich bei dieser Fortbildung auf den Grundsatz der Verhältnismäßigkeit.

Eine solche Fortentwicklung ist auch für die Übermittlung von Informationen aus sicherheitsrechtlichen Überwachungsmaßnahmen erkennbar. Ausgangspunkt ist der Grundsatz, dass eine zweckändernde Datenübermittlung einen rechtfertigungsbedürftigen Grundrechtseingriff darstellt. Anstatt einer Rationalitätskontrolle im Einzelfall gelten aber auch hier konkretisiert pauschale Vorgaben durch das informationelle Trennungsprinzip und den Grundsatz der hypothetischen Datenneuerhebung, die insofern den Verhältnismäßigkeitsgrundsatz operationalisierbar machen.[178]

175 *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., 373); krit. auch *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (66 ff.); *Wolff*, ZG 2016, 361 (366 f.).

176 So auch *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 192; ähnlich positives Fazit bei *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 184 ff.

177 *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.

178 *F. Schneider*, GSZ 2022, 1 (1) Zum Grundsatz der hypothetischen Datenneuerhebung; für diesen Aspekt zum informationellen Trennungsprinzip: *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191); *Unterreitmeier*, DÖV 2021, 659 (660 ff.); *Poscher/Rusteberg* KJ 2014, 57 (68 f.); *dies.* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Reform der Nachrichtendienste, 2020, S. 145 (S. 152 ff.).

2. Massenüberwachung und Verfassungsrecht

In vielen Fällen befasste sich die Rechtsprechung[179] primär mit individuellen Überwachungsmaßnahmen, die zwar auch bei Finanzdaten eine große praktische Rolle spielen (s. Kap. E.), sich allerdings in der Funktionsweise deutlich von den Phänomenen der Massenüberwachung dadurch unterscheiden, dass kein Datenverarbeitungsschritt vorgenommen wird, bevor ein sicherheitsrechtlicher Anlass vorliegt.

Da sich diese Arbeit vornehmlich den geldwäscherechtlichen Massenüberwachungstatbeständen widmen will, soll im Folgenden dargestellt werden, wie sich die aufgestellten Grundsätze des BVerfG auf solche Maßnahmen der Massenüberwachung auswirken.

a. Formen der Massenüberwachung

Die Typisierung in der Individual- und Massenüberwachung hängt davon ab, ob die Überwachung in jedem konkret betroffenen Fall anlassbezogen erfolgt oder nicht. Es liegt in der Natur der Massenüberwachung, dass ihre Effektivität gerade davon abhängt, dass gezielt auch solche persönlichen Daten verarbeitet werden, bei denen im Moment der Verarbeitung noch nicht klar sein kann, ob sie für den verfolgten sicherheitsrechtlichen Zweck dienlich sind. Die Massenüberwachung kann insofern als Versuch des Staates verstanden werden, sich der allgemeinen Problematik des sicherheitsrechtlichen Vorfeldbereichs[180] zu widmen.

Diese besteht darin, dass gewisse Gefahren, deren Verursacher – etwa im Bereich Terrorismus[181] – gänzlich unbekannt sind, schon deshalb als stets gegenwärtig betrachtet werden müssen, da sich das Gegenteil nie beweisen ließe. Der Staat könnte letztlich immer einen Anlass zur für- bzw. vorsorglichen Überwachung vorbringen. Aufgrund dieser „stetigen Verhält-

179 Etwa BVerfGE 120, 274 – Online-Durchsuchung; E 113, 348 – TKÜ; mehrheitlich auch E 141, 220 – BKA-Gesetz; BVerfG, NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz.

180 Zur Vorfeldproblematik siehe *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999; *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *Wolff*, DÖV 2009, 597 (604).

181 *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (26 ff., 42).

nismäßigkeit“[182] stößt die Abwägungsrechtsprechung bei der Behandlung von Überwachungsmaßnahmen an ihre Grenzen.[183] Als Eingriffe, die der Gewinnung von Informationen dienen, setzen sie sinnvollerweise voraus, dass ein Informationsdefizit besteht. Die materiellen Anforderungen an ihre Zulässigkeit können daher naturgemäß nur in begrenztem Rahmen an das Vorliegen bestehender Information geknüpft werden. Stattdessen stehen prognostische Elemente im Vordergrund.[184]

Eine Überwachung ist folglich regelmäßig schon im erweiterten Vorfeld einer Gefahr zweckmäßig oder im strafprozessualen Kontext, wenn die Verwirklichung einer schweren Straftat zwar gesichert erscheint, aber noch völlig unklar ist, wer Täter sein könnte, etwa in Fällen der organisierten Kriminalität oder des Terrorismus.[185]

Aufgrund der bestehenden Anonymität kommen Individualüberwachungsmaßnahmen bei diesen Sachverhalten nicht in Betracht. Der Staat ist darauf angewiesen, die für solche Maßnahmen notwendigen Verdachtsmomente erst zu gewinnen[186] und die Voraussetzungen für die dann stattfindenden Ermittlungen zu gewährleisten. Dementsprechend haben sich zwei Formen der Massenüberwachung entwickelt: die Vorratsdatenspeicherung und die Datenanalyse. Letztere wiederum tritt in unterschiedlichen Gestaltungsformen auf: der Rasterfahndung und dem strategischen Abgleich.[187] Auch eine Kombination dieser Maßnahmen ist möglich, wenn die massenhaft gesammelten Daten nicht nur analysiert, sondern unabhängig vom Analyseergebnis vorratsmäßig gespeichert werden, wie es etwa im Rahmen der Fluggastdatenspeicherung der Fall ist.

Um einen Vergleich der Geldwäschebekämpfung mit den bereits von der Rechtsprechung behandelten Überwachungsmaßnahmen vorzunehmen,

182 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82 mit Verweis auf *Enders* in Enders/Wiederin/Pitschas ua. (Hrsg.), VVDStRL 64 (2004), 2005, S. 7 (45 f.).

183 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *ders.*, Die Verwaltung 2008, 345; s.a. *Volkmann*, JZ 2006, 918 (918 f.); *Lepsius* Leviathan 2004, 64 (78 ff.); *ders.* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23.

184 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 223 ff.; *Bonin,* Kompensation, 2014, S. 217 ff.; allg. zu Wahrscheinlichkeit im Gefahrenabwehrrecht *Poscher*, Die Verwaltung 2008, 345 (S. 352 ff.).

185 *Albers,* Determination, 2001, 111 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 35 ff.; *Lisken*, ZRP 1994, 264.

186 Vgl. zur „Verdachtsgewinnung“ schon *Bull*, FS Selmer, 2004, S. 29.

187 zur Unterscheidung vgl. *Kahler,* Kundendaten, 2017, S. 37 f.; *Petri*, StV 2007, 266.

sollen die Grundzüge der bekannten Formen von Massenüberwachungsmaßnahmen nachgezogen werden, um strukturelle Parallelen der entsprechenden Normkomplexe aufzuzeigen.

aa. Vorratsdatenspeicherung

Eine schlichte Form der Massenüberwachung stellt dabei zunächst die sogenannte Vorratsdatenspeicherung dar, bei der bestimmte Daten für einen retrograden Zugriff der Sicherheitsbehörden vorgehalten werden.

Dabei dreht sich die grundrechtliche Problematik im Kern um die Verknüpfung von Speicherpflicht und (sicherheitsrechtlicher) Zugriffsberechtigung. Allgemein nämlich stellen Speicherpflichten, bei denen die spätere Notwendigkeit der Daten im Moment der Speicherung noch nicht hinreichend bekannt ist, keine Besonderheit dar.[188] Sie finden sich an verschiedenen Orten der Rechtsordnung – etwa in behördlichen Registern[189] oder den Buchhaltungspflichten von Kaufleuten, bspw. § 147 AO, § 257 HGB.[190] Allein die Speicherung ohne jeden erkennbaren gegenwärtigen oder zukünftigen Zweck ist stets rechtswidrig.[191]

Die Diskussion um die *Vorratsdatenspeicherung* betraf vor diesem Hintergrund also weniger das Konzept *vorrätiger* Daten als solches, sondern spezifisch die universelle Speicherung von TK-Verkehrsdaten zur späteren Nutzung durch Sicherheitsbehörden.[192] Erst nachdem durch das PNR-Abkommen mit Kanada und später durch den Erlass der PNR-RL auch die Speicherung von Fluggastdaten zur Verbrechensbekämpfung etabliert wurde, wurde der Begriff der Vorratsdatenspeicherung außerhalb der Telekommunikationsdaten intensiver diskutiert.[193]

Beiden Maßnahmen ist gemein, dass der Staat eine Bevorratung von Daten – selbst oder durch Dritte – vornimmt, deren primärer Zweck

188 Vgl. BVerfGE 130, 151 (189 f.) – Bestandsdatenauskunft I; zur Schufa z.B. s. VG Wiesbaden, ZD 2022, 706.

189 *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 174 f.

190 Übersichtlich *Schober*, BC 2013, 528.

191 So schon BVerfGE 65, 1 (46) – Volkszählung.

192 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 139; vgl. auch *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 117 (117 f.).

193 *EDPS,* Stellungnahme 05/2015, PNR, 24.09.2015; *Arzt*, DÖV 2017, 1023; *A. Knierim* ZD 2011, 17.

zunächst in der Verfügbarkeit besteht.[194] Im Moment der Speicherung ist ein sicherheitsrechtlicher Anlass noch nicht vorhanden. Da der Daten-Art aber allgemein vom Staat ein hoher Nutzen für die Sicherheitsbehörden attestiert wird, werden die jeweiligen Datensätze für den Fall vorgehalten, dass die Zweckerforderlichkeit nachträglich eintritt.

Prägnant an der *Vorratsdatenspeicherung* ist also nicht der Zugriff auf retrograde Daten, denn Informationen müssen immer erst bestehen, damit sie verwendet werden können, sondern dass der Staat gewissermaßen das Vertrauen in die sicherheitsrechtliche Irrelevanz eines jeden Bürgers ablegt (dazu unten). Hingegen ist die Vorstellung fehlgeleitet, dass erst die Vorratsdatenspeicherung es dem Staat ermöglicht, Informationen abzugreifen, die vor Eintreten des sicherheitsrechtlichen Anlasses entstanden sind. Eine solche Anonymität vor Beginn der Ermittlungen existiert nicht, da es sowohl dem Staat als auch den Privaten unbenommen ist, verschiedenste Daten aus verschiedensten Gründen unter Berücksichtigung des allgemeinen Datenschutzrechts ohnehin zu speichern. Die Vorratsdatenspeicherung ist insofern nur eine Reaktion des Staates auf den Umstand, dass bestimmte Daten in der Praxis ihre ursprüngliche Zweckerforderlichkeit verlieren und deshalb eigentlich zu löschen wären, Art. 17 Abs. 1 lit. A), 5 Abs. 1 lit. B, c, e DSGVO.[195] So wurden (und werden teilweise[196]) die TK-Verkehrsdaten vor Einführung der „Flatrate-Verträge" von den Providern ohnehin aus Abrechnungszwecken für eine längere Zeit vorgehalten und im Rahmen der Ermittlungstätigkeit auch den Sicherheitsbehörden zugänglich gemacht.[197]

Bei den Finanzdaten lässt sich dies gut beobachten (dazu unten Kap. E.). Obwohl die geldwäscherechtlichen Aufbewahrungspflichten recht offensichtlich eine Vorratsdatenspeicherung vorsehen (dazu Kap. D. III. 2. D.), findet eine intensivere Diskussion weder in der deutschsprachigen Rechtswissenschaft noch in der Öffentlichkeit statt (Übersicht zur Diskussion in Kap. F.). Dieses überschaubare Interesse lässt sich angesichts der Sensibilität – gerade der Kontoinhaltsdaten – wohl nur damit begründen,

194 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 140.

195 *Wolff* in BeckOK Datenschutzrecht, Syst. A Rn. 51.

196 Vgl. *BfJ,* Statistik Verkehrsdatenerhebung, 2020, S. 4 f., https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_Verkehrsdaten_2020.pdf?__blob=publicationFile&v=4, zuletzt aufgerufen am 12.01.2025; LG Landshut, Beschluss v. 16.01.2013 - 6 Qs 309/12; LG Mannheim, ZD 2018, 223; dazu *Bär* in BeckOK StPO, TTDSG § 9 Rn. 16; *J.-D. Braun* in Geppert/Schütz Beck'scher TKG Kommentar, TKG § 96 Rn. 21.

197 *Breyer,* Vorratsspeicherung, 2005, S. 12 ff.

dass ein Zugriff auf Kontoinhalte eine seit Jahren etablierte Praxis der Staatsanwaltschaften[198] darstellt, da die Daten aus verschiedenen Gründen (Kap. D. II.) ohnehin vorliegen.

Das Bemerkenswerte an der Vorratsdatenspeicherung ist die Kombination aus Speicherung und Zugriff. Jeder dieser Datenverarbeitungsschritte stellt zwar einen eigenständigen Eingriff dar, die Bewertung hängt jedoch gerade davon ab, dass die Schritte aufeinander zugerichtet sind und absichtlich kombiniert wurden. Bei der Verhältnismäßigkeit jedes Verarbeitungsschrittes ist also die Verhältnismäßigkeit der anderen Schritte zu beachten. Sie verhalten sich insofern wechselwirkend bzw. synergetisch.

Der Staat belegt eine bestimmte Datenform mit dem Verdikt, dass diese Daten in Zukunft für Sicherheitsbehörden relevant werden können. Damit kehrt er die Grundannahme, dass Daten nur gespeichert werden sollen, wenn ihre zukünftige Nutzung für bestimmte Zwecke absehbar ist, und dann für andere Zwecke bloß zufällig vorliegen und ermittelt werden können, in das Gegenteil um.[199]

Diese Zufälligkeit bzw. Unkontrollierbarkeit der Datenverfügbarkeit stellt normalerweise ein natürliches Abwehrmittel gegen staatliche Ermittlungsmaßnahmen dar. Dieses wird dem Bürger geraubt, wenn der Staat bestimmte Daten für die Eventualität, dass sie tatsächlich für Ermittlungen notwendig werden, vorsorglich aus dem Bereich des Unkontrollierbaren herausnimmt.

bb. Datenanalyse: strategische Aufklärung und Rasterfahndung

Die zweite Form der Massenüberwachung stellen die strategischen Aufklärungsmaßnahmen und die Rasterfahndung dar, die sich dadurch auszeichnen, dass größere Datenmengen technisch analysiert werden, um dadurch Verdachtsmomente gegenüber bestimmten oder bestimmbaren Personen zu gewinnen.

Bei der Rasterfahndung erfolgt dies durch den fortlaufenden Abgleich verschiedener Datensätze, indem stets nur die Überschneidungen in den folgenden Schritten ausgewertet werden, um einen immer enger werdenden

198 Siehe nur *F. Jansen,* Bankauskunftsersuchen, 2010; *Kahler,* Kundendaten, 2017, S. 31 ff.; *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 31 ff.; *Reichling*, JR 2011, 12.

199 Krit. insofern *Szuba,* Vorratsdatenspeicherung, 2011, 192 ff.

Personenkreis zu identifizieren.[200] Da sich ein vergleichbares Instrument in der Überwachung von Finanzdaten nicht finden lässt – auch die „Operation Mikado"[201] (unten Kap. E. I. 1. C. bb.) stellte keine Rasterfahndung dar[202] –, soll diese Maßnahme hier aber nicht näher erläutert werden.[203] Von größerem Interesse ist hier das Durchleuchten einzelner Datensätze nach bestimmten Suchelementen, das mangels Abgleich verschiedener Datensätze gerade nicht als Rasterfahndung zu qualifizieren ist,[204] sondern als strategische Aufklärung bezeichnet werden kann.

Eine strategische Aufklärungsmaßnahme im hier verstandenen Sinne liegt vor, wenn auf eine massenhafte Datensammlung innerhalb eines bestimmten räumlichen und/oder zeitlichen Bereichs ein unmittelbarer Abgleich der erhobenen Daten mit einem bestimmten Datensatz erfolgt. So werden beispielsweise bei der automatisierten Kennzeichenerfassung sämtliche KFZ-Kennzeichen erfasst, die an einem gewissen Streckenabschnitt vorbeikommen, und in einem automatisierten Prozess mit einer Liste gesuchter KFZ-Kennzeichen abgeglichen.[205] Nur bei einem „Treffer" finden die Daten weitere Verwendung durch die jeweiligen Sicherheitsbehörden. „Nichttreffer" werden umgehend gelöscht.

Ein anderes Beispiel ist die strategische Fernmeldeaufklärung. Bei dieser werden große Mengen von Telekommunikationsinhalten, die auf zuvor bestimmten Telekommunikationswegen stattfinden, erhoben und auf bestimmte „Selektoren" hin durchleuchtet. Diese Selektoren können formalen Charakters sein, etwa eine bestimmte Adresse oder Anschlusskennung, oder inhaltlicher Natur, etwa bestimmte Begriffe oder Sätze.[206]

---

200 BVerfGE 115, 320 (321) – Rasterfahndung; *Gerhold* in BeckOK StPO, § 98a Rn. 9 ff.

201 BVerfG, NJW 2009, 1405

202 Idem, (1406 f.); AG Halle, DuD 2007, 464 (467); zust. *Kahler,* Kundendaten, 2017, S. 37 f.; *Petri*, StV 2007, 266, die aber eine Anwendung des § 161 Abs. 1 S. 1 Hs. 2 StPO iE. ablehnen; aA. *Schnabel*, DuD 2007, 426 (427 f.): „mittelbare Rasterfahndung"; *Brodowski*, JR 2010, 543 (547 f.).

203 Allerdings enthält auch die vorzeitige PNR-Analyse Elemente der Rasterfahndung vgl. *Arzt*, DÖV 2017, 1023 (1026 ff.).

204 Vgl. BVerfG, NJW 2009, 1405 (1406 f.); OLG Stuttgart, NStZ 2001, 158 (159); OLG Köln, NStZ-RR 2001, 31 (32); *Köhler* in Meyer-Goßner/Schmitt StPO, § 98a Rn. 8.

205 Zur Funktionsweise siehe nur *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 970; *Roggan*, NStZ 2022, 19 (21).

206 Bspe. bei *B. Huber*, NJW 2013, 2572 (2573); umfassend zu den formalen Selektoren aus der Zusammenarbeit BND-NSA *Graulich*, (1. UA des 18. Deutschen Bundestags), Fernmeldeaufklärung mit Selektoren, MAT A SV-11/2, zu A-Drs. 404, 23.10.2015, S. 23 ff., 98 ff.

Wie die Vorratsdatenspeicherung zeichnen sich die strategischen Aufklärungsmaßnahmen dadurch aus, dass von der Datenverarbeitung stets auch solche Personen betroffen sind, die im Moment der Verarbeitung keinerlei Anlass für eine sicherheitsrechtliche Überwachung geliefert haben. Ausgangspunkt ist abermals, dass der Staat, etwa aufgrund der (Omni-)Präsenz organisierter Kriminalität, allgemein davon ausgeht, dass sich aus den Informationen der Abgleichsdatensätze sicherheitsrelevante Sachverhalte ergeben könnten.[207] Je nachdem, wie spezifisch diese Daten sind, steigert sich jedoch die Eingriffsschwelle für den Abgleich. Durch die Eingrenzung der Suchbegriffe soll gewährleistet werden, dass der Abgleich nur spezifische Verdachtsmomente hervorbringt, die dem Anlass entsprechen.[208]

Die strategische Aufklärung unterscheidet sich in struktureller Hinsicht erheblich von der Vorratsdatenspeicherung. Bei der Vorratsdatenspeicherung tritt der Anlass, der die Nutzung der gespeicherten Daten erforderlich werden lässt, extrinsisch ein. Die Daten selbst werden erst bei Eintreten eines Anlasses wiederaufgegriffen, und nicht proaktiv – bevor es zu einem Verdachtsmoment gekommen ist – zur Einleitung von Ermittlungen genutzt. Gerade so verhält es sich hingegen bei den strategischen Aufklärungsmaßnahmen. Zwar stehen auch hier extrinsische Gründe hinter der Aufnahme bestimmter Selektoren in die Abgleichsdatensätze. Die Maßnahmen sollen aber unmittelbar zu weiteren Ermittlungs- oder auch Exekutivmaßnahmen führen, weshalb eine Speicherung in Nichttrefferfällen ausbleibt. Die strategische Aufklärung dient also, wie auch die Rasterfahndung[209] oder der Abgleich von PNR-Daten[210], der Gewinnung bzw. Verdichtung von vorab konkretisierten Verdachtsmomenten[211] und nicht der Förderung später (eventuell) erforderlich werdender Ermittlungen der Sicherheitsbehörden.

b. Aspekte der Intensitätsbewertung

Beide Formen der Massenüberwachung weisen verschiedene vom BVerfG entwickelte Intensitätsmerkmale auf. Sowohl bei der Vorratsdatenspeiche-

207 *Bäcker*, Kriminalpräventionsrecht, 2015, S. 53 ff.
208 BVerfGE 150, 244 (281 ff.) – Autom. Kennzeichenkontrolle II.
209 BVerfGE 115, 320 (107) – Rasterfahndung.
210 *Arzt*, DÖV 2017, 1023 (1028).
211 BVerfGE 154, 152 (245 ff.) – Ausland-Ausland-Fernmeldeaufklärung; *Roggan*, NStZ 2022, 19 (20).

rung als auch bei der strategischen Kontrolle werden die Daten einer großen Zahl von Menschen zur Förderung sicherheitsrechtlicher Ziele verarbeitet, ohne dass dies den Betroffenen im Moment der Verarbeitung stets gewahr wird.

aa. Anlasslosigkeit und Streubreite

Gerade die Betroffenheit einer Vielzahl von Personen steht sinnbildlich und namensgebend für das Phänomen der Massenüberwachung. Eine hohe „*Streubreite*" wirkt sich steigernd auf die Intensität der Grundrechtsbeeinträchtigung aus.

Bei Individualmaßnahmen sind zwar ebenfalls Dritte mitbetroffen, etwa die Kontaktpersonen einer Person, deren Telekommunikation überwacht wird. Bei solchen Maßnahmen stellt die Streubreite aber kein entscheidendes Merkmal der Intensitätsbewertung dar, sondern spielt eine untergeordnete Rolle.[212] Im Vordergrund der Individualmaßnahmen steht vielmehr, wie tief in die Privatsphäre der final betroffenen Person eingegriffen wird. Allerdings kann es hier vergleichsweise stringent gelingen, mittels Eingriffsschwellen zu gewährleisten, dass der Eingriff nur dann vorgenommen wird, wenn die Chancen auf eine sicherheitsrechtliche Relevanz der Informationen hochstehen. Die gesetzliche Grundlage der Maßnahme gewinnt hierdurch an Effektivität und wird somit *verhältnismäßig*.[213]

Bei Maßnahmen der Massenüberwachung verhält es sich umgekehrt. Sie kommen prinzipiell in Situationen zur Anwendung, bei denen gerade erst die Bewahrung oder Gewinnung von relevanten Informationen im Raum stehen. Es liegt insofern in ihrer Natur, dass sie nicht effektiv, nicht zielgerichtet, sondern universell ausgerichtet sind.

Da Massenüberwachungsmaßnahmen zwangsläufig breit streuen, sind sie nach der Bewertungsmatrix des BVerfG *stets* besonders eingriffsinten-

212 Vgl. allerdings BVerfGE 113, 348 (383) – TKÜ.

213 *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82; *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff., 127).

siv.[214] Dieser Intensität müssten nach der Je-Desto-Formel[215] (s. o. III. 1.) nun eigentlich hohe Eingriffsschwellen gegenüberstehen und damit insbesondere ein rechtfertigender Anlass. Die Anlasslosigkeit ist aber gerade die Wurzel der hohen Streubreite. Die verfassungsgerichtliche Dogmatik führt zu dem paradoxen Ergebnis, dass eigentlich gerade für solche Maßnahmen ein rechtfertigender Anlass bestehen müsste, die sinnvollerweise nur anlasslos erfolgen können.[216]

Das BVerfG steht insofern vor einem Dilemma. Zur Operationalisierung des Verhältnismäßigkeitsgrundsatzes muss das Gericht – wenn es seine Rechtsprechung im Sicherheitsrecht stringent halten will – auch für anlasslose Maßnahmen bestimmte Anforderungen aufstellen, ohne gleichzeitig deren Nutzen zu versperren.[217] Im Rahmen der Vorratsdatenspeicherung konnte es sich insofern noch mit der Trennung von Speicherung und Zugriff behelfen. Der Zugriff stellt eine Individualmaßnahme dar. Er kann daher mittels bestimmter Eingriffsschwellen eingegrenzt werden. Nach dem BVerfG kann es ergo zulässig sein, eine universale Speicherpflicht bestimmter Datenkategorien einzuführen, wenn die tatsächliche Nutzung dieser Daten durch die Behörden auf bestimmte Fälle beschränkt bleibt. Die Bewertung der Speicherung hängt somit (auch) von der Ausgestaltung der Zugriffsvorschriften ab.[218]

Bei Maßnahmen der massenhaften Datenanalyse kommt diese Möglichkeit nicht in Betracht, da die Erhebung der Daten unmittelbar durch die Sicherheitsbehörden erfolgt. Hier kam das BVerfG daher nicht umhin, schon für den ersten Verarbeitungsschritt der Überwachungsmaßnahmen bestimmte Beschränkungen aufzustellen. So muss etwa die strategische Fernmeldekontrolle auf eine begrenzte Zahl von Telekommunikationswe-

214 So schon BVerfGE 100, 313 (376, 392) – Strategische Fernmeldeaufklärung; E 115, 320 (354) – Rasterfahndung; E 150, 244 (283 f.) – Autom. Kennzeichenkontrolle II.

215 Siehe nur *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.; *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 116.

216 Vgl. *Volkmann*, NVwZ 2022, 1408 (1411).

217 Insofern krit. *Möstl*, GSZ 2019, 101 (106 ff.).

218 BVerfGE 125, 260 (320 ff.) – Vorratsdatenspeicherung; aA. der EuGH, der schon die Speicherpflicht von bestimmten Umständen abhängig macht, siehe EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

gen beschränkt werden[219], für die eine sicherheitsrechtliche Relevanz begründet werden muss und von denen wiederum nur eine begrenzte Zahl der Kommunikationsinhalte ausgelesen werden darf, §§ 5, 10 Abs. 4,5 G-10; §§ 10 Abs. 2, 8 BNDG (s. o.)).

Auch *anlasslose* Maßnahmen – in dem Sinne, dass sie gezielt auch eine große Menge sicherheitsrechtlich nicht relevanter Sachverhalte bzw. Personen erfassen – sind damit nicht gänzlich ohne Erfüllung bestimmter Voraussetzungen zulässig.

Dass das BVerfG insofern eine grundsätzlich kritische Position gegenüber Massenüberwachungsmaßnahmen eingenommen hat, wird nicht nur positiv gesehen.[220] Dem BVerfG lässt sich durchaus vorwerfen, selbstreferentiell vorzugehen, da es die hohe Intensität maßgeblich von der jeweils enormen Streubreite der Maßnahmen ableitet. Dass die Streubreite einer Maßnahme aber überhaupt intensivierend wirkt, ist keine sich aufdrängende extrinsische Erkenntnis, sondern eine (begründungsbedürftige) Feststellung des Gerichts. An dieser hält es auch bislang strikt fest. Die intensivierende Wirkung der Streubreite wird gewissermaßen als Axiom behandelt,[221] obwohl die dogmatischen Begründungen durchaus kritisiert werden.[222]

Im Ergebnis verdient das BVerfG aber Zustimmung. Das Gericht nimmt letztlich eine objektive Betrachtungsposition ein, indem es die jeweiligen Ermächtigungsgrundlagen auf ihre gesellschaftlichen Auswirkungen hin untersucht. Dogmatisch kann dieses quantitative Element als Ausprägung der objektiv-verfassungsrechtlichen Gesetzeskontrolle verstanden werden.[223]

---

219 BVerfGE 100, 313 (376 ff.) – Strategische Fernmeldeaufklärung; E 154, 152 (250 ff.) – Ausland-Ausland-Fernmeldeaufklärung

220 *Haas* abw. Meinung zu BVerfGE 115, 320 (371); *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 98 ff.; *Würtenberger*, FS Schröder, 2012, S. 285 (299 f.); *Löffelmann* – "Kaum betroffen" FAZ Online vom 29.04.2015, https://www.faz.net/aktuell/politik/staat-und-recht/gastbeitrag-kaum-betroffen-13566596-p2.html?service=printPreview, zuletzt aufgerufen am 12.01.2025; auch krit. aber iE zustimmend *Möstl* in BeckO PolR Bayern, Syst. Vorb. Rn. 41, 48.

221 Vgl. BVerfGE 154, 152 (242) – Ausland-Ausland-Fernmeldeaufklärung.

222 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 ff.; *Nettesheim* in Nettesheim/Diggelmann/Lege ua. (Hrsg.), VVDStRL 70, 2011, S. 7 (28 f.); *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 98 ff.; *ders.* in Möllers/van Ooyen (Hrsg.), BVerfG Öfftl. Sicherheit I, 2. Aufl. 2012, S. 65 (87 f.); *Trute*, Die Verwaltung 2009, 85 (98 ff.); differenziert *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.

223 So *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.; *Breckwoldt,* Grundrechtskombinationen, 2014, S. 195 ff.; *Klement*, AöR 2009, 35 (45 ff.); *Brade*, DÖV 2019, 853.

bb. Heimlichkeit

Auch deren Heimlichkeit wird bei allen Maßnahmen der Massenüberwachung als intensivierendes Element von der ständigen Rechtsprechung berücksichtigt.[224] Die intensivierende Wirkung der Heimlichkeit lässt sich sowohl mit der Unterdrückung des Rechtsschutzes im Sinne eines Abwägungsverbundes[225] der Privatheitsgrundrechte mit Art. 19 Abs. 4 GG oder einschüchternden Effekten erklären.[226] In letzterem Falle darf man aber, wie auch bei der Streubreite darauf verwiesen, den Eingriff durch das Gesetz nicht unmittelbar in der konkreten Maßnahme, die durch das Gesetz ermöglicht wird, erblicken. Stattdessen muss man auf die mittelbar-faktischen Wirkungen abstellen, die sich bei den Betroffenen durch das Wissen um die gesetzliche Maßnahme und die technischen Möglichkeiten der Sicherheitsbehörden einstellen.[227]

Trotz dieser noch offenen dogmatischen Fragen ist die intensivierende Wirkung in der Rechtsprechung etabliert und wird auch von der Rechtswissenschaft nicht mehr erkennbar angezweifelt. Es stellt sich jedoch heraus, dass die Definition der Heimlichkeit des BVerfG nicht differenziert genug ist, da es die Überwachungsmaßnahmen einheitlich begreift und nicht auf die einzelnen Datenverarbeitungsschritte abstellt. So zeichnen sich Vorratsdatenspeicherungen aufgrund ihrer Universalität ja gerade dadurch aus, dass die Speicherung nicht ohne Kenntnis des Betroffenen erfolgt, sondern diesem schon durch die Verabschiedung der gesetzlichen Grundlage bekannt wird bzw. bekannt werden kann.[228]

Auch der eventuell folgende Zugriff geschieht nicht zwangsläufig ohne Kenntnisnahme. Zwar soll der Betroffene von diesem nach der gesetzlichen Gestaltung nichts erfahren, jedenfalls bei den manuellen Zugriffsverfahren erhalten Dritte aber zwangsläufig Kenntnis von der Abfrage. Diese wiederum könnten grundsätzlich den Betroffenen informieren, etwa wenn sie

224 BVerfGE 154, 152 (241) – Ausland-Ausland-Fernmeldeaufklärung; E 150, 244 (283) – Autom. Kennzeichenkontrolle II.

225 *Breckwoldt,* Grundrechtskombinationen, 2014, S. 132 ff.; *Spielmann,* Konkurrenz, 2008, S. 173 ff.; krit. gegenüber solchen Verbundsbetrachtungen: *Kahl,* Schutzergänzung, 2000, S. 25 mwN.; Übersicht bei *Heß,* Grundrechtskonkurrenzen, 2000, S. 82 ff.

226 BVerfGE 125, 260 (320) – Vorratsdatenspeicherung.

227 Dazu Eingriffen *Oermann/Staben*, Der Staat 2013, 630 (640 ff.); krit. *Klement* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. III, 2. Aufl. 2022, § 80 Rn. 59.

228 *Schluckebier* abw. Meinung BVerfGE 125, 260 (366).

sich aufgrund eines vertraglichen Verhältnisses zu dessen Schutz verpflichtet fühlen.[229]

cc. Exkurs: Mitwirkung Privater bei der öffentlichen Sicherheitsgewährleistung

Überhaupt ist die Einbeziehung Privater in sicherheitsrechtliche Aufgaben ein Phänomen, das insbesondere bei den Maßnahmen der Massenüberwachung Bedeutung erlangt. Zwar sind auch manche Individualmaßnahmen, etwa die TKÜ, nicht ohne die Mithilfe Privater denkbar.[230] Hier reduziert sich deren Kooperationspflicht aber meist auf technische Aspekte der Datenerhebung.

Im Rahmen der Massenüberwachung nimmt die Mithilfe Privater eine neue Qualität an. Die Regelungen der TK-Vorratsdatenspeicherung nach § 176 TKG sowie die Bestandsdatenspeicherungspflichten der §§ 174 ff. TKG und §§ 24c KWG, 93b, 93 Abs. 7. 8 AO beruhen primär auf der Vorhaltung und Bereitstellung enormer Datenmengen durch Private. Auch bei der Geldwäschebekämpfung stehen Private an der Spitze. Sie müssen Kontotransaktionen überwachen und etliche Daten vorhalten (dazu Kap. D. III.).

Da die Sicherheitsgewährleistung prinzipiell dem Staat obliegt, stellt sich bei diesen Überwachungskomplexen die Frage, ob die Ausgliederung bestimmter Maßnahmen auf die grundrechtliche Bewertung einen Einfluss hat.

(1) Indienstnahme Privater und „Criminal Compliance"

Das allgemeine Phänomen, dass Private – insbesondere Wirtschaftsunternehmen – durch spezifische Pflichten in die Verhinderung von Straftaten miteingebunden werden, hat sich in den letzten Jahrzehnten immer stärker entwickelt und wird mittlerweile gar als eigenes Rechtsgebiet der „Criminal Compliance" behandelt. Im Vordergrund der Criminal Compliance steht

229 Für Banken etwa *Reichling*, JR 2011, 12 (16); *Krepold/Zahrte* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 8 Rn. 261.

230 *Rückert* in MüKo StPO, §100a Rn. 237.

grundsätzlich das Misstrauen[231] des Gesetzgebers gegenüber den Unternehmen selbst aufgrund deren originärer Nähe zu bestimmten Delikten. Primäres Anliegen der Criminal Compliance ist es mithin, bestimmte Unternehmen bzw. deren Mitarbeiter durch gesetzliche Pflichten von strafbarem Verhalten abzuhalten oder dieses aufzudecken[232]. Es handelt sich um eine Form der *regulierten Selbstregulierung*.[233]

Versteht man jedes strafbarkeitsvermeidende oder -aufdeckende Verhalten als Criminal Compliance[234], können selbst solche wirtschaftsrechtlichen Pflichten noch mit dem Begriff umschrieben werden, die allein auf die Mithilfe bei der Durchsetzung von Sicherheitsinteressen gegenüber Dritten ausgerichtet sind. Da insofern aber der für den Begriff wichtige Aspekt der regulierten Selbstregulierung in den Hintergrund tritt, überrascht es nicht, dass die Mitwirkungspflichten bei der Vorrats- oder Bestandsdatenspeicherung nicht unter dem Schlagwort der Criminal Compliance diskutiert werden, sondern meist nur unter dem verfassungsrechtlichen Topos der *Indienstnahme Privater*.[235]

Anders verhält es sich bei solchen Normkomplexen, die eine aktive Mithilfe bei der Erlangung sicherheitsrechtlich relevanter Informationen über Dritte vorsehen, bei denen die jeweiligen Produkte der Unternehmen in einem engen Zusammenhang mit den verfolgten Delikten stehen. Hier sind etwa das Anti-Geldwäscherecht und das Netzwerkdurchsetzungsgesetz (NetzDG)[236] zu nennen. Diese Regelungsmaterien zeichnen sich dadurch aus, dass bestimmte strafbare Verhaltensweisen Dritter ohne die Angebote der jeweils verpflichteten Privaten kaum ausgeübt werden könnten.

---

231 *Schünemann*, GA 2013, 191 (196); aA *Kölbel*, ZStW 2014, 499, der die Criminal Compliance als Vertrauensvorschuss deutet.

232 Vgl. *Rotsch* in Rotsch (Hrsg.), Criminal Compliance, 2015, § 1 Rn. 42 ff., 50; *ders.* in Rotsch (Hrsg.), Compliance Zukunft, 2013, S. 3 (9 f.); *Bock,* Criminal Compliance, 2011, S. 23 ff.

233 *Kölbel*, ZStW 2014, 499 (507 ff.); *Sieber*, FS Tiedemann, 2008, S. 449 (460 f.); allg. zum Konzept *Ayres/Braithwaite,* Regulation, 1995, S. 101 ff.

234 Vgl. *Hilgendorf* in Rotsch (Hrsg.), Compliance Zukunft, 2013, S. 19 (21).

235 Etwa *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 306 ff.; *F. Braun*, K&R 2009, 386; *Schoch* in Schoch/Schneider, VerwR, VwVfG § 1 Rn. 175; allg. BVerfGE 30, 292 (311); *Ibler* in Dürig/Herzog/Scholz GG, Art. 86 Rn. 120; *Manssen* in v. Mangoldt/Klein/Starck GG, Art. 12 Rn. 202.

236 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) vom 01. September 2017 (BGBl. I S. 3352), zuletzt geändert durch Gesetz vom 21. Juli 2022 (BGBl. I S. 1182); dazu *Adelberg,* Netzwerke, 2020, S. 128 mwN.; *Wimmers/Heymann*, AfP 2017, 93 (S. 97 f.).

Bei diesen Normkomplexen wird vonseiten der Gesetzgebung gern argumentiert, dass es auch hier letztlich um Selbstschutz der Unternehmen geht.[237] Diese würden sonst regelmäßig in den Verdacht einer Beihilfestrafbarkeit gelangen[238] oder aufgrund der einschlägigen Delikte wirtschaftliche Nachteile erleiden. Im Erwägungsgrund Nr. 2 der 4. GeldwäscheRL[239] wird beispielsweise ausdrücklich darauf hingewiesen, dass die Verpflichteten durch ihre Mithilfe bei der Geldwäschebekämpfung *die Solidität, Integrität und Stabilität der Kreditinstitute und Finanzinstitute sowie das Vertrauen in das Finanzsystem* – also letztlich sich – behüten.

(2) Auswirkungen der Einbeziehung Privater auf die Grundrechtsprüfung

Für die grundrechtliche Bewertung spielt die begriffliche Abgrenzung der *Indienstnahme Privater* von der *Criminal Compliance* kaum eine Rolle. Sie sind aus wissenschaftlicher Perspektive allenfalls als „Schlüsselbegriffe"[240] interessant, da sich die jeweiligen Diskurse in Abhängigkeit von den Oberbegriffen durchaus unterscheiden.

Dass eine grundrechtsbeeinträchtigende, informationelle Maßnahme zur Sicherheitsgewährleistung nicht unmittelbar durch einen staatlichen Akteur ausgeübt wird, sondern aufgrund einer Verpflichtung durch einen Privaten, kann sich auf die Intensität der Maßnahme zwar mildernd auswirken, etwa wenn bei einer verpflichtenden Speicherung durch die Indienstnahme weitere Hürden geschaffen und Dezentralität gewährleistet werden.[241] Der Eingriff wird durch die Ausgliederung an Private aber nicht prinzipiell

237 BT-Drs. 14/8739, S. 11 „Einsparungen durch bessere Sicherheitslage"; vgl. auch *Findeisen*, wistra 1997, 121 (125); *ders.* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (113 ff.); *Bergles/Eul*, BKR 2002, 556 (562 f.).

238 Zur Geldwäschestrafbarkeit von Banken etc. *Boerger* in Momsen/Grützner (Hrsg.), Hdb. Wirtschafts- & SteuerstrafR, 2. Auflage 2020, § 38 Rn. 160 ff.

239 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. 2015, L 141/73.

240 Vgl. *Voßkuhle* in Grimm (Hrsg.), Selbstregulierung, 2001, S. 197 (198).

241 BVerfGE 125, 260 (320 ff.) – Vorratsdatenspeicherung.

intensiviert.[242] Eine verpflichtende Indienstnahme ist dem Staat weiterhin als eigener Eingriff zuzurechnen und ändert daher nicht grundsätzlich den Charakter der Maßnahme[243].

Im Urteil zur Kontostammdatenauskunft hatte das BVerfG sogar noch angenommen, dass den betroffenen Kontoinhabern praktische Nachteile dadurch entstehen könnten, dass die Institute von den Abfragen erfahren würden, da diese auf die Ermittlungsmaßnahmen proaktiv mit Kontoschließungen reagieren könnten.[244] Aus diesem Umstand leitete es ab, dass sich vollständig heimliche, weil technisch automatisierte Zugriffe von Sicherheitsbehörden bei Privatunternehmen weniger intensiv auf die Rechte der Betroffenen auswirkten, da schon mit dem Bekanntwerden von Ermittlungen bei Dritten eine Reputationsgefährdung einherginge.

Diese Auffassung hat das BVerfG allerdings in jüngeren Urteilen nicht mehr wiederholt. Sie ist auch nicht mit dem hier vorgestellten Verständnis der Heimlichkeit in Einklang zu bringen. Datenerhebungen bei Dritten, die auch dem Dritten verborgen bleiben, weisen eine maximal ausgeprägte Heimlichkeit auf, da faktisch keine Möglichkeit der Kenntnisnahme besteht. Zwar ist sicher richtig, dass die Kenntnis des Dritten über die Ermittlungen zu faktischen Nachteilen führen könnte, etwa durch die vorzeitige Kündigung von Vertragsverhältnissen. Diesen Gefahren kann aber auf entsprechender Ebene begegnet werden. So können beispielsweise Bankkunden die Ablehnung eines Antrags auf Eröffnung eines Basiskontos nach §§, 49, 50 ZKG rechtlich prüfen lassen. Wird eine Basiskontoeröffnung wegen einer Geldwäscheverdachtsmeldung abgelehnt, muss die Ablehnung nachträglich aufgehoben werden, wenn sich der Verdacht nicht erhärtet.[245]

Die *absolute* Heimlichkeit einer Maßnahme – in dem Sinne, dass kein Dritter von ihr erfährt – wirkt sich also nicht positiv, sondern eher negativ auf den Betroffenen aus, da ohne sie zumindest die Möglichkeit des Dritten bestünde, den Betroffenen über die Maßnahme zu informieren. Eine solche

242 aA. *Szuba,* Vorratsdatenspeicherung, 2011, S. 194 ff.; *Grafe,* Verkehrsdaten, 2008, S. 18 f.; *Herzog*, WM 1996, 1753 (1762).

243 Idem (310); *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff. mwN.; aA. *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 30.

244 BVerfGE 118, 168 (194 f.) – Kontostammdaten.

245 OLG Frankfurt, BKR 2021, 380 (382); zur Kündigung von Girokonten wegen Geldwäscheverdachts vgl. OLG Jena, Urt. v. 29.09.2020 – 5 U 165/19.

Informierung kann in Abwesenheit von Sanktionsvorschriften sogar eine vertragliche Pflicht darstellen.[246]

Es ist also zu begrüßen, dass das BVerfG nicht mehr versucht hat, die Kenntnisnahmemöglichkeit Dritter intensitäts*steigernd* zu berücksichtigen. Seiner nunmehr neutralen Haltung in dieser Frage ist beizupflichten.[247]

c. Schlussbemerkung: Massenüberwachung als Problem objektiven Grundrechtsschutzes und Rechtsstaatlichkeit

Die Maßnahmen der Massenüberwachung fallen dadurch auf, dass sie natürlicherweise die verschiedenen vom BVerfG identifizierten intensitätssteigernden Merkmale in sich vereinen. Dies wirft angesichts bestehender dogmatischer Ungereimtheiten die Frage auf, ob die intensitätssteigernden Überwachungsmerkmale nicht letztlich vom Ende her gedacht wurden.

Das BVerfG erblickt offenbar in den Massenüberwachungsmaßnahmen eine intrinsische Gefährlichkeit für die informationelle Selbstbestimmung der Gesellschaft. Es besteht der Verdacht, dass es Massenüberwachungen nicht für besonders intensiv hält, weil sie heimlich sind und eine hohe Streubreite aufweisen. Vielmehr scheint das BVerfG die Heimlichkeit und die Streubreite als intensivierende Merkmale einzustufen, weil sie für Massenüberwachungsmaßnahmen typisch sind.

Nach dieser Überlegung stellen Massenüberwachungsmaßnahmen primär ein rechtsstaatliches Problem dar, das im System der traditionellen Grundrechtsdogmatik über die Schöpfung von Intensitätsmerkmalen individuell rekonstruiert wurde.

aa. Totalüberwachung und Überwachungsgesamtrechnung

Noch auf grundrechtlicher Ebene bedürfte es einer solchen individuellen Rekonstruktion gar nicht, wenn man die Massenhaftigkeit bestimmter Überwachungsmaßnahmen nicht aus einer individuellen Grundrechtsper-

246 Für eine Informationspflicht aus dem Bankvertrag *Reichling*, JR 2011, 12 (16) mwN zum Streitstand; aA. *Krepold/Zahrte* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 8 Rn. 261.

247 BVerfGE 125, 260 (311 f.) – Vorratsdatenspeicherung; zust. *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 154; ebenso EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169.

spektive betrachtet, sondern die Grundrechte als objektiven Gesellschaftsschutz versteht.[248]

Diesen Gedanken legen die Aussagen des BVerfG zum Verbot der (gesellschaftlichen)[249] Totalüberwachung aus dem Urteil zur Vorratsdatenspeicherung nahe. Danach dürfe die Einführung der Speicherung von Verkehrsdaten, die das Gericht grundsätzlich für zulässig erachtete, „*nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. (…). Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.*"[250]

Dieses *obiter Dictum* wurde von Teilen der Rechtswissenschaft[251] und der Politik[252] zum Anlass genommen, eine „Überwachungsgesamtrechnung" zu fordern, nach der für die Legalität einzelner Überwachungsgesetze nicht nur deren individuelle Verhältnismäßigkeit ausschlaggebend sei. Stets müsse man sich obendrein fragen, ob sämtliche Überwachungsgesetze in einer Gesamtschau dazu führen könnten, dass ein von der Gesellschaft nicht mehr zu akzeptierendes Überwachungsniveau erreicht wird.

Im Koalitionsvertrag der „Ampel-Koalition" 2021 wurde die Durchführung einer solchen Überwachungsgesamtrechnung beschlossen.[253] Derzeit

248 *Breckwoldt,* Grundrechtskombinationen, 2014, S. 196 ff.; *Klement*, AöR 2009, 35 (45 ff.); *Brade*, DÖV 2019, 853 (856 f.); s.a. *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 177 Fn 58; *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f. Fn 158.

249 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 236 ff.; *Löffelmann,* Überwachungsgesamtrechnung, 2022, S. 14; zur Abgrenzung von gesellschaftlicher Totalüberwachung („Überwachungsgesamtrechnung", Begriff geprägt von *Roßnagel*, NJW 2010, 1238 (1242)) und Additiver Grundrechtseingriff siehe *Starnecker,* Videoüberwachung zur Risikovorsorge, 2016, S. 365 ff.; zu letzterem s. nur *Hornung* in Albers/Weinzierl (Hrsg.), Sicherheitspolitik, 2010, S. 65 (65 ff.); *Winkler*, JA 2014, 881.

250 BVerfGE 125, 260 (323 f.) – Vorratsdatenspeicherung.

251 Zuerst *Roßnagel*, NJW 2010, 1238; früher Umsetzungsversuch in Österreich durch *Tschohl et al.,* HEAT – Handbuch zur Evaluation der-Anti-Terror-Gesetze, 2016, https://epicenter.works/sites/default/files/heat_v1.2.pdf, zuletzt aufgerufen am 12.01.2025; krit. *Bieker/Bremert/Hagendorff* in Roßnagel/Friedewald/Hansen (Hrsg.), Fortentwicklung des Datenschutzes, 2018, S. 139; *Bieker/Bremert* FIfF-Kommunikation 2019(4), 34; *J. Pohle* FIfF-Kommunikation 2019(4), 37.

252 BT-Drs. 19/23695.

253 *SPD/Bündnis 90/Die Grünen/FDP,* Koalitionsvertrag "Mehr Fortschritt wagen", 2021, S. 85 f., https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

werden Vorschläge zusammengetragen, ob und wie eine solche *Rechnung* operationalisiert werden könnte.[254]

Die Debatte verdeutlicht, dass die Betrachtung massenhafter Überwachungsmaßnahmen nicht allein von individuell-grundrechtlichen Aspekten, sondern einer objektiven, politischen Skepsis gegenüber sicherheitsrechtlicher Dauerüberwachung der Gesamtbevölkerung geprägt ist.[255] Diese Skepsis wiederum besteht gewissermaßen *a priori*. Ihre praktischen Gründe ermittelt weniger die Grundrechtstheorie als die Sozialwissenschaft im Rahmen der *surveillance studies* (s. o.).[256]

Das BVerfG hat sich zu diesem Blickwinkel bzw. dieser objektiv-politischen Grundüberzeugung allerdings nicht ausdrücklich bekannt.[257] Es versucht stattdessen, aus der massenhaften Betroffenheit ein individuell intensivierendes Merkmal abzuleiten, indem es auf die Anlasslosigkeit und – aus der Gesetzesexistenz resultierende –Einschüchterungseffekte rekurriert. Massenhafte Überwachungsmaßnahmen sollen deshalb auch für den Einzelnen schwer wirken.

Auf die Kritik[258] an seiner Erklärung ist das Gericht bislang nicht eingegangen. Stattdessen behandelt es insbesondere die Gewichtung der Streubreite als sicherheitsrechtliches Axiom und geht somit letztlich selbstreferentiell[259] vor: Massenhafte Überwachungsmaßnahmen beeinträchtigen Grundrechte massiv, da sie breit streuen. Die Streubreite wiederum stellt eine Intensivierung dar, weil sie zu Einschüchterungseffekten führt und bewirkt, dass es immer auch zu anlasslosen Überwachungen kommt.

---

254 *Löffelmann,* Überwachungsgesamtrechnung, 2022; *Poscher/Kilchling/Landerer*, GSZ 2021, 225; *dies.*, (Friedrich-Naumann-Stiftung für die Freiheit), Überwachungsbarometer, 2022; *Gerson* KriPoZ 2022, 404; *Gemmin*, DÖV 2022, 789; krit. *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915.

255 *Kostov*, GSZ 2022, 267 (270).

256 Etwa *Adensamer,* Hdb. Überwachung, 2020, S. 24 ff.; *Kreissl/Norris/ Krlic Marija ua.* in Wright/Kreissl (Hrsg.), Surveillance, 2015, S. 150 (154 ff.); *Čas/Bellanova/Burgess ua.* in Friedewald/Burgess/Čas ua. (Hrsg.), Surveillance, 2017, S. 1; *Lemieux,* Surveillance, 2019; allg. *Lyon,* The electronic Eye, 1994; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18.

257 Vgl. aber BVerfGE 115, 320 (357) – Rasterfahndung.

258 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 142 ff; S. 176 ff.; *Nettesheim* in Nettesheim/Diggelmann/Lege ua. (Hrsg.), VVDStRL 70, 2011, S. 7 (28); *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 98 ff.; *ders.* in Möllers/van Ooyen (Hrsg.), BVerfG Öfftl. Sicherheit I, 2. Aufl. 2012, S. 65 (87 f.); *Trute*, Die Verwaltung 2009, 85 (98 ff.).

259 Dazu allg. krit. *Rusteberg*, KritV 2017, 24 (26 f.).

Auf dieser Begründungsebene treten aber Probleme auf. Die Einschüchterungseffekte sind eine mittelbare Folge der Gesetzesexistenz und keine unmittelbare Konsequenz der Ausübung der entsprechenden Maßnahme.[260] Überdies sind sie empirisch kaum zu belegen.[261]

Auch die Anlasslosigkeit ist nur schwer als Argument für eine Erhöhung der Eingriffsintensität in Stellung zu bringen. Die in den Überwachungsgesetzen festgelegten Schutzgüter und spezifische Eingriffsschwellen gewährleisten die Effektivität des Eingriffs, indem sie ihn auf bestimmte relevante Szenarien begrenzen. Faktisch sind die unmittelbaren Nachteile einer Überwachung aber stets dieselben. Die Tiefe, mit dem das Recht „*selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*"[262] gebrochen wird, ist von der konkreten Begründung erst einmal unabhängig. Dieser Aspekt betrifft allein die Rechtfertigungsseite. Da auch auf Gesetzesebene der Eingriff grundsätzlich nach den Nachteilen der tatsächlichen Durchführung bestimmt wird, lässt sich die Anlasslosigkeit als Grundlage der intensivierenden Wirkung mit der Datenherrschaftstheorie des BVerfG also kaum in Einklang bringen.[263]

Politisch bzw. gesellschaftlich lässt sich die kritische Betrachtung der Massenüberwachung durch das BVerfG sicher befürworten. Aus einer dogmatischen Perspektive wäre es aber wünschenswert, dass das BVerfG die Schwierigkeiten einer individuell-rekonstruierten Erklärung der intensiven Grundrechtsbelastung anerkennt. Mehrere Autoren haben festgestellt, dass die gesellschaftliche bzw. sicherheitspolitische Brisanz mit der objektivrechtlichen Dimension der Grundrechte eingefangen werden kann.[264] Es bedarf weder der Verfassungsidentität noch einer Erheblichkeit des Eingriffs aus der individuellen Perspektive, um die hohen Anforderungen an die Rechtfertigung massenhafter Überwachungsmaßnahmen zu begründen. Ausreichend wäre es, die Zahl der durch eine Maßnahme

260 Vgl. *Klement* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. III, 2. Aufl. 2022, § 80 Rn. 59.

261 *Rath* in *Kritische Justiz* (Hrsg.), 60 Jahre GG, 2009, S. 65 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 f.; *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915 (918).

262 Jüngst wieder BVerfGE 156, 11 (39) – Antiterrordatei II.

263 *Tanneberger,* Sicherheitsverfassung, 2014, S. 243 f.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 272 f.; vgl. auch *Bull* in Möllers/van Ooyen (Hrsg.), BVerfG Öfftl. Sicherheit I, 2. Aufl. 2012, S. 65 (87 Fn 117); *ders.* in van Ooyen/Möllers (Hrsg.), Hdb. BVerfG, 2015, S. 627 (642 f.); *Möstl*, GSZ 2019, 101.

264 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f.; *Breckwoldt,* Grundrechtskombinationen, 2014, S. 195 ff.; *Klement*, AöR 2009, 35 (45 ff.); *Brade*, DÖV 2019, 853.

betroffenen Grundrechtsträger im Rahmen einer objektiv dimensionierten Grundrechtsprüfung als intensivierendes Merkmal anzuerkennen. Dieses Vorgehen entspricht der Funktion der Verfassungsbeschwerde als objektive Kontrolle[265] von gesellschaftspolitisch brisanten, weil breitenwirksamen, Grundrechtbeeinträchtigungen.[266]

Gerade weil sich individuelle Beeinträchtigungen in vielen Fällen nur schlecht mit Kollektivinteressen abwägen lassen,[267] sollte das BVerfG von der tradierten Individualperspektive – jedenfalls in Fällen wie der sicherheitsrechtlichen Massenüberwachung – Abstand nehmen, um den gesellschaftlichen Implikationen solcher Maßnahmen Ausdruck zu verleihen.

Es ist also richtig, dass Massenüberwachungsmaßnahmen grundsätzlich eine intensive Grundrechtsbeeinträchtigung darstellen. Aber nicht, weil sie den Einzelnen schwer treffen, sondern weil sie eine Vielzahl von Personen und somit die „*Freiheitlichkeit der Gesellschaft insgesamt*"[268] beeinträchtigen.

bb. Vertrauensbruch als Abkehr von traditioneller Sicherheitsgewährleistung

Die Rechtsprechung des BVerfG tritt staatlicher Massenüberwachung im Ergebnis zurecht kritisch gegenüber. Damit steht das Gericht auch nicht allein. Die Rechtsprechung spiegelt letztlich eine in Politik, Gesellschaft und Wissenschaft weit verbreitete Skepsis wider.

Nun wurde gerade festgestellt, dass sich diese Aversion schon auf grundrechtlicher Ebene im Rahmen einer objektiven Betrachtung damit erklären lässt, dass die Eingriffe eine Vielzahl von Grundrechtsträgern betreffen. Die entsprechenden Vorschläge beschreiben diese horizontale Kumulation allerdings gewissermaßen als Automatismus, weshalb die Übertragung des Konzepts auf Eingriffsgesetze außerhalb des Rechts elektronischer Da-

265 *Gusy* in van Ooyen/Möllers (Hrsg.), Hdb. BVerfG, 2015, S. 333 (344 ff.); *Schlaich/Korioth,* BVerfG, 12. Aufl. 2021, Rn. 205; *E. Klein*, DÖV 1982, 797 (803 ff.).

266 Vgl. zu den Pandemiemaßnahmen *Murswiek*, NVwZ-Extra 5/2021 (6); zust. *Schoch*, NVwZ 2022, 1 (6 f.).

267 *Lepsius* in Jestaedt/Lepsius (Hrsg.), Verhältnismäßigkeit, 2021, S. 1 (34); *ders.* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (34 f.); *Gusy* in Weber-Dürler/Kokott/Vesting (Hrsg.), VVDStRL 63, 2004, S. 153 (176 f.); *Rusteberg* in *Junge Wissenschaft Öffentlichen Recht e.V.* (Hrsg.), Kollektivität, 2012, S. 13 (19 ff.).

268 BVerfGE 150, 244 (284) – Autom. Kennzeichenkontrolle II.

tenverarbeitung (zur Sicherheitsgewährleistung) noch skeptisch betrachtet wird.[269]

Daneben existieren allerdings auch zwei – eng verwandte – rechtsstaatliche Ansätze, mit denen die grundrechtliche Sensitivität erklärt werden könnte. Aus dem Umstand, dass breit streuende Überwachungsmaßnahmen zwingenderweise auch solche Personen betreffen, ergibt sich einerseits ein allgemeiner Vertrauensbruch des Staates gegenüber dem Bürger und weiter eine Umgehung des traditionellen Reaktionismus des Sicherheitsrechts.

(1) Rechtstreue des Bürgers und Prävention

Massenüberwachungsmaßnahmen begründen sich letztlich mit der Allgegenwärtigkeit kaum individualisierbarer Bedrohungen und der deshalb ständig notwendigen Prävention.[270] Sie sind daher eng verknüpft mit dem allgemein sicherheitsrechtlichen Phänomen der Vorfeldverlagerung, die gerade zur Terrorismusbekämpfung auch im materiellen Strafrecht beobachtet werden kann.[271]

Die strafrechtliche Entwicklung hat zur Abstrahierung bestimmter Rechtsgutverletzung. Geführt. Bei den sog. „Präventionsstraftaten" wird beispielsweise schon in einer Mitgliedschaft, etwa § 129a Abs. 1 S. 1 Alt. 2 StGB, die Begründung einer Gefährdungssituation gesehen und pönalisiert.[272] Der Gesetzgeber spekuliert insofern, dass durch die Mitgliedschaft das Risiko einer tatsächlichen Rechtsgutverletzung signifikant erhöht wird.

Solche Spekulationen liegen auch den Massenüberwachungsmaßnahmen zugrunde. Bei den strategisch überwachten Lebenssachverhalten wird

269 *Breckwoldt,* Grundrechtskombinationen, 2014, S. 200 f.; vgl. zu Pandemiemaßnahmen allerdings *Murswiek*, NVwZ-Extra 5/2021 (6); zust. *Schoch*, NVwZ 2022, 1 (6 f.).

270 *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999 ; *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *Wolff*, DÖV 2009, 597 (604).; allg. zur Tendenz präventiven (Sicherheits-)Rechts statt vieler *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 391 ff.; *Denninger* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 85 (88 ff.) und die übrigen Beiträge dort; übersichtlich *Volkmann*, NVwZ 2022, 1408 (1410 f.).

271 Dazu nur *Hawickhorst,* Terrorismusbekämpfung, 2011, S. 18 ff.; *Sieber*, NStZ 2009, 353 (356 ff.); *Weißer*, JZ 2008, 388 (390 ff.); *Jakobs*, ZStW 2006, 839.

272 BT-Drs. 10/6635, S. 4; OLG München, NJW 2007, 2786 (2787); ausf. *Hawickhorst,* Terrorismusbekämpfung, 2011, S. 98 ff.

aufgrund allgemeiner Annahmen davon ausgegangen, dass konkrete Verdachtslagen aus der Überwachung bestimmter Bereiche extrahiert werden können.[273] Bei Maßnahmen der Vorratsdatenspeicherung wird allgemein aufgrund der Daten-Art angenommen, dass zumindest die Möglichkeit einer zukünftigen Relevanz für sicherheitsrechtliche Übermittlungen entsteht.[274]

Mit dieser spekulativen Betrachtung unmittelbar nicht sicherheitsrelevanter Verhaltensweisen bringt der Staat Misstrauen gegenüber den Grundrechtsträgern zum Ausdruck. Dieses gilt es grundsätzlich zu rechtfertigen, wenn sich der Staat nicht dem Vorwurf der Willkür aussetzen will.

Im materiellen Strafrecht lässt sich diese Rechtfertigung noch ganz gut darstellen. So sprechen gute Gründe für die Annahme, dass eine Mitgliedschaft in einer terroristischen Vereinigung eine nicht mehr zu duldende Rechtsgutgefährdung darstellt. Durch die Anknüpfung an bestimmte Tatsachen wird dem Delikt die Willkürhaftigkeit genommen und somit aus verfassungsrechtlicher Perspektive entschärft.[275] Problematisch sind spekulative Annahmen des Gesetzgebers aber, wenn sie einem Generalverdacht[276] gleichkommen. Dann nämlich wird zum Ausdruck gebracht, dass der Staat den Grundrechtsträgern nicht grundsätzlich zutraut, dass diese sich nicht ausschließlich rechtmäßig verhalten.[277] Bestimmte Freiheiten werden somit unter Rechtfertigungslast gesetzt.[278] Die Frage ist dann, ob es ein solches Grundvertrauen ähnlich der Unschuldsvermutung überhaupt geben muss[279] und dieses universellen Überwachungsmaßnahmen entgegen-

273 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 53 ff.; zur PNR-Analyse *Arzt*, DÖV 2017, 1023 (1025); *Ders.* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap G Rn. 1330.

274 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 140; *Bull* in van Ooyen/Möllers (Hrsg.), Hdb. BVerfG, 2015, S. 627 (643).

275 OLG München, NJW 2007, 2786 (2787 f.) mwN.; krit. *Hawickhorst,* Terrorismusbekämpfung, 2011, S. 262 ff.

276 Vgl. Zur Vorratsdatenspeicherung *Orantek* NJ 2010, 193 (195).

277 *Breyer*, StV 2007, 214 (217).; *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 493 ff.; *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (31 f.); vgl. auch *B. Hirsch* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 164 (166 ff.), der die Vorratsdatenspeicherung in die Nähe des „Feindstrafrechts rückt.

278 *Masing*, JZ 2011, 753 (756 f.).

279 Für eine solche Annahme *Weßlau,* Vorfeldermittlungen, 1989, S. 300 ff.; *Dencker*, FS Dünnebier, 1982, S. 447 (459 f.) *Lisken*, NVwZ 1998, 22 (24); s.a. BayVGH ZD 2019, 515 (521).

steht[280], oder ob dem Staat aufgrund der Existenz bestimmter Kriminalitätsformen nicht doch ein niedrigschwelliger Generalverdacht zugestanden werden muss, der bestimmte anlasslose Datenverarbeitungen unter Umständen zulässig macht.

(2) Reaktivität der Sicherheitsgewährleitung als staatsrechtlicher Grundsatz?

Mit dem Verlust des Vertrauens in die Rechtstreue der Grundrechtsträger geht also die Abkehr vom Prinzip der Reaktivität des Sicherheitsrechts einher. Der Staat will nicht länger abwarten, dass für jede einzelne Person, die Ziel einer Datenverarbeitung werden soll, sicherheitsrechtlich relevante Tatsachen bekannt oder vermutet werden.

Traditionell sind in der Bundesrepublik die operativen Sicherheitsrechtsbereiche, das Polizeirecht und das Strafverfolgungsrecht zwar funktional getrennt. Das Polizeirecht dient als Gefahrenabwehr der Verhinderung konkreter Gefahren für die öffentliche Sicherheit, während das Strafverfahrensrecht der Durchsetzung des Strafrechts gilt. Beiden Rechtsbereichen gemein ist aber, dass sie grundsätzlich reaktiv ausgestaltet sind.[281]

Als Mindestanforderung gilt stets, dass grundrechtsbeeinträchtigende Maßnahmen erst dann vorgenommen werden können, wenn bestimmte Informationen die Erforderlichkeit ihres Handelns nahelegen. Das ergibt sich aus der rechtsstaatlichen Unschuldsvermutung, die auch für das Strafprozessrecht gelten soll.[282]

Für die Strafverfolgungsbehörden kommt dieser Grundsatz in § 152 Abs. 2 StPO zum Ausdruck, der für jede Ermittlungen mindestens einen Anfangsverdacht voraussetzt.[283] Ermittlungen, die dazu dienen sollen, erst einen Anfangsverdacht zu schaffen, sind den Behörden prinzipiell untersagt.[284]

280 So *Puschke/Singelnstein*, NJW 2008, 113 (118); *Szuba,* Vorratsdatenspeicherung, 2011, S. 196 ff. mit Bezug zum Rechstaatsprinzip (dazu unten).

281 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 51 ff., 122 ff.; *Gärditz* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. II, 2. Aufl. 2022, § 22 Rn. 60 ff.

282 *Schünemann*, FS 25 Jahre DAV, 2009, S. 827 (829 ff.).

283 BVerfG, NStZ-RR 2004, 143 (143)

284 Sog. „Vorfeldermittlungen" dazu *Rogall*, ZStW 1991, 907 (945 ff.); *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4b; *S. Peters* in MüKo StPO, § 152 Rn. 62;s.a.

Analog verhält es sich im Polizeirecht, das ein Tätigwerden mit operativem Eingriffscharakter stets vom Vorliegen einer konkreten Gefahr abhängig macht. Zwar sind Maßnahmen zur Gefahrenerforschung[285] grundsätzlich nicht unzulässig, diese dienen aber wie die staatsanwaltschaftlichen „Vorermittlungen" allein der Prüfung, ob bestimmte Erkenntnisse tatsächlich einen Eingriffsanlass konstituieren. Erforschungsmaßnahmen „ins Blaue hinein", die der proaktiven Besorgung solcher Erkenntnisse dienen sollen, verbieten sich.[286]

Von diesem Grundsatz der Reaktivität wird bei den anlasslosen Überwachungsmaßnahmen jedenfalls durch einzelne Datenverarbeitungsvorgänge abgerückt.[287] Sie dienen der Verdachtsgewinnung bzw. der Informationsvorsorge. Der Staat reagiert auf den Umstand, dass seine Sicherheitsbehörden angesichts der Universalität moderner Bedrohungen bei der Wahrung ihrer Aufgaben stets einen Schritt hintendran sind.[288]

Es stellt sich hier die allgemein staatsrechtliche Frage, ob dem Prinzip der reaktiven Sicherheitsgewährleitung überhaupt Verfassungsrang zukommt, etwa als Ausfluss der Menschenwürde[289] oder des Rechtsstaatsprinzips bzw. der Unschuldsvermutung[290], oder ob es sich schlicht um eine gesetzgeberische Entscheidung handelt.[291]

Das BVerfG hat im Urteil zur BKAG – jedenfalls für den Bereich der Gefahrenabwehr, festgestellt –, dass der Gesetzgeber nicht bei jeder sicherheitsrechtlichen Aufgabenwahrnehmung Eingriffstatbestände vorsehen

---

Zöller, Informationssysteme, 2002, S. 127 ff., der allerdings nicht zwischen „Vorermittlungen" und „Vorfeldermittlungen" unterscheidet.

285 Dazu nur *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. Dn Rn. 103 ff.; *Schenke*, JuS 2018, 505 (508 ff.).

286 Jüngst BVerfG, NJW 2023, 1196 (1212, Rn. 158) – Autom. Datenanalyse.; BVerfGE 115, 320 (361) – rasterfahndung.

287 *Puschke/Singelnstein*, NJW 2008, 113 (118); *Lisken*, ZRP 1994, 264 (267 f.).

288 *Albers,* Determination, 2001, 111 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 35 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (S. 253 ff.); *ders.*, Die Verwaltung 2008, 345 (345 ff.).

289 *Hund*, NJW 1992, 2118 (2119).

290 *Puschke/Singelnstein*, NJW 2008, 113 (118); *Szuba,* Vorratsdatenspeicherung, 2011, S. 196 ff. in diese Richtung auch *Lisken*, ZRP 1990, 15 (17 ff.); *ders.*, ZRP 1994, 264 (267 f.); übersichtlich *K. Weber,* Polizeirecht, 2011, S. 79 ff.

291 *Möstl* in Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer, 2008, S. 239 (242 ff.); *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.).; iE. auch BVerfGE 125, 260 (316 ff.) – Vorratsdatenspeicherung; E 150, 244 (282) – Autom. Kennzeichenkontrolle II.

muss, *„die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen."*[292]

Dabei ging es zwar konkret nicht um die Zulässigkeit anlassloser Massenüberwachungen, sondern um die Zulässigkeit individueller Maßnahmen bei „drohender Gefahr". Es ist aber bemerkenswert, dass sich das Gericht hier mit der tradierten Vorstellung reaktiver Sicherheitsgewährleistung grundsätzlich auseinandersetzt.

Ein Anknüpfungspunkt für einen *Grundsatz der Reaktivität im Sicherheitsrecht* außerhalb der Grundrechte müsste tatsächlich erst gefunden oder konstruiert werden. Insofern ist es verständlich, dass das BVerfG sich bei der Festlegung verfassungsrechtlicher Grenzen für sicherheitsrechtliche Überwachungsmaßnahmen vordergründig allein auf die grundrechtliche Verhältnismäßigkeitsprüfung verlässt und rechtsstaatliche Fragen als Intensitätskriterien verkleidet.

Vorzugswürdig scheint es aber, das Phänomen der Massenüberwachung als besonderes Verfassungsproblem zu begreifen. Man könnte dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG durchaus ein Prinzip entnehmen, wonach die Sicherheitsgewährleistung reaktiv zu erfolgen hat. Primär das Rechtsstaatsprinzip stünde der strukturell proaktiven[293] Massenüberwachung dann entgegen. Der Versuch des BVerfG, aus der Verfassungsidentität ein Verbot gesellschaftlicher Totalüberwachung abzuleiten, ging in diese Richtung, blieb bislang aber einmalig und wurde nie tatsächlich zur Anwendung gebracht.

3. Zusammenfassung

Staatliche bzw. sicherheitsrechtliche Überwachungsmaßnahmen haben also eine prominente Rolle in der Rechtsprechung des BVerfG eingenommen. Etliche Urteile zu überarbeiteten Sicherheitsgesetzen setzten sich überwiegend mit den jeweiligen Datenverarbeitungs- und -Übermittlungsrechten auseinander.[294]

Datenverarbeitende Handlungen der Sicherheitsbehörden greifen in Recht das Recht auf informationelle Selbstbestimmung, das Telekommuni-

292 BVerfGE 141, 220 (272) – BKA-Gesetz.

293 Vgl. *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 68 f.; Albers, Determination, 2001, S. 112 ff.

294 Insbesondere BVerfGE 141, 220 – BKA-Gesetz; NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz; ähnlich schon E 110, 33 – Außenwirtschaftsgesetz.

kationsgeheimnis und das Recht auf Vertraulichkeit und Integrität informationstechnischer Geräte ein. Bei der Verhältnismäßigkeitsprüfung durch des BVerfG hat sich aber eine Methode etabliert, die die Unterschiede der einzelnen Grundrechte verwischt.

a. Vorfeldüberwachung und Verhältnismäßigkeit

Die Überwachungsmaßnahmen haben dem BVerfG die Grenzen des Grundsatzes der Verhältnismäßigkeit aufgezeigt. Schon lange wird die Anwendung des Verhältnismäßigkeitsgrundsatzes bei Gesetzen kritisiert, da dieser mit seiner Kosten-Nutzen-Relation genuin auf den Einzelfall zugeschnitten ist.[295] Insbesondere Eingriffsgesetze regeln aber nicht den Einzelfall, sondern abstrakte Situationen und müssen entsprechend flexibel sein. Daher muss die konkrete Gestaltung des Gesetzes daraufhin geprüft werden, wie effektiv bzw. wie erfolgsversprechend die jeweilige Maßnahme zur Förderung des Gesetzeszweckes führt.[296]

Die Informationsgewinnung im Sicherheitsrecht betrifft den immer wichtiger gewordenen[297] Vorfeldbereich.[298] Sie findet also statt, bevor eine konkrete Gefahr erkennbar wird oder nur vermutet werden kann, bzw. vor dem Auftreten eines Anfangsverdachts. Das Ausmaß der Gefährdung eines Rechtsguts ist hier nicht bestimmbar, da die Zahl der möglichen Kausalverläufe immer größer wird, je weiter man sich von der tatsächlichen Rechtsgutverletzung wegbewegt.[299] Damit geht einher, dass der denklogi-

295 *Schlink,* Abwägung, 1976, S. 134 ff.; *ders.*, FS 50 Jahre BVerfG, Bd. II, 2001, S. 445 (461 f.); *Jestaedt* in Jestaedt/Lepsius (Hrsg.), Verhältnismäßigkeit, 2021, S. 293 (293 ff.).

296 *Hillgruber* in Isensee/Kirchhof (Hrsg.), Hdb StR Bd. IX, 3. Aufl. 2011, § 210 Rn. 76; *Stern,* StaatsR Bd. III/2, 1994, S. 836; speziell zum Sicherheitsrecht *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242 ff.; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82 f., 14 ff.; aus der Rspr etwa BVerfGE 155, 166 (197 f.); E 141, 220 (268 ff.) – BKA-Gesetz.

297 *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999 ; *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *Wolff*, DÖV 2009, 597 (604).

298 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Möstl* in Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer, 2008, S. 239 (240 ff.); *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.).

299 Vgl. BVerfGE 113, 348 (378 ff.) – TKÜ; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242; *Thiel,* Entgrenzung, 2012, S. 91 ff. mit Vergleich zum Umwelt-

sche Nutzen einer Überwachung mit der Verlagerung in den Vorfeldbereich zum Maximum strebt,[300] während der grundrechtliche Nachteil, die Preisgabe der Datenherrschaft[301], immer gleichbleibt. Überwachungsmaßnahmen im Vorfeld sind demnach *stets verhältnismäßig,* wenn sie möglichst früh ansetzen, und führen so die klassische Rationalitätskontrolle der Verhältnismäßigkeitsprüfung *ad absurdum*.[302]

Das BVerfG nutzt den Verhältnismäßigkeitsgrundsatz weniger zur Rationalitätskontrolle und mehr als Mittel zur Rechtsfortbildung.[303] Es verleiht ihm Ausdruck, indem es per Auslegung bestimmte materielle und formelle Zulässigkeitsvoraussetzungen sowie Kompensationsanforderungen für sicherheitsrechtliche Überwachungsmaßnahmen herausarbeitet.[304] Dieser Anforderungskomplex wird als *Sicherheitsverfassungsrecht* bezeichnet.[305]

---

recht; s.a. *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. D Rn. 255 ff.; *ders.,* Kriminalpräventionsrecht, 2015, S. 194 ff.

300 *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 f.); *Volkmann*, JZ 2006, 918 (919); allgemeiner. *Grimm* in Hassemer/Starzacher (Hrsg.), Organisierte Kriminalität, 1993, S. 28 (33 ff.); *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (S. 39 ff.).

301 BVerfGE 65, 1 (43) – Volkszählung; E 156, 11 (39) – Antiterrordatei II; krit. dazu etwa *Albers,* Informationelle Selbstbestimmung, 2005; *dies.* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11; *Poscher* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 167; *ders.* in Miller (Hrsg.), Privacy and Power, 2017, S. 129; *Britz* in Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.).

302 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82 mit Verweis auf *Enders* in Enders/Wiederin/Pitschas ua. (Hrsg.), VVDStRL 64 (2004), 2005, S. 7 (45 f.); ähnlich *Hassemer* in *30. Strafverteidigertag* (Hrsg.), Sicherheit Freiheit, 2007, S. 9 (27 f.).

303 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82.

304 BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84.; krit. *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., 373); *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (66 ff.); *Wolff*, ZG 2016, 361 (366 f.).

305 Vgl. *Tanneberger,* Sicherheitsverfassung, 2014; *Dietrich/Gärditz* (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245.

Das Verhältnismäßigkeitsprinzip kommt dabei in einer Je-desto-Formel[306] zum Ausdruck. Je intensiver die Überwachungsmaßnahme, desto strenger müssen die Zulässigkeitsvoraussetzungen sein und desto mehr Kompensations- und Kontrollmechanismen müssen etabliert werden. Dabei hält das BVerfG einen ganzen Katalog[307] an Merkmalen bereit, nach dem sich die Intensität der jeweiligen Überwachungsmaßnahmen bestimmen lässt. Ausgehend von diesen Merkmalen werden dann ebenfalls streng schematisch spezifische Anforderungen, gar Formulierungen hergeleitet, die das entsprechende Gesetz vorsehen muss.[308]

b. Grundrechtsintensität der Massenüberwachung

Maßnahmen der Massenüberwachung werden nach dieser Judikatur besonders kritisch gesehen, da sie ihrer Natur nach mehrere bedeutsame Intensitätsmerkmale in sich vereinen.[309] Ihre Anlasslosigkeit geht natürlicherweise mit einer extraordinären Streubreite einher.

Um die intensivierende Wirkung einer hohen Streubreite erklären zu können, sollte aber der Blickwinkel geändert werden. Statt aus einer individuellen Grundrechtsbetrachtung, erklärt sich die intensive Grundrechtsbeeinträchtigung aus einer objektiven. Schon die Menge der betroffenen Grundrechtsträger – jedenfalls im Rahmen der Bewertung von Überwachungsgesetzen – stellt per se einen intensivierenden Umstand dar, ohne dass sich dies erst durch die Wirkung auf den Einzelnen erklärt.[310]

---

306 *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.; *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 116; früh schon *Vahle,* Aufklärung, 1983, S. 94 ff., 130.

307 *Löffelmann*, GSZ 2019, 16 (19); *Poscher/Kilchling/Landerer*, GSZ 2021, 225 (230 ff.);*F. Braun/F. Albrecht* VR 2017, 151 (152); *Hornung/Schnabel*, DVBl 2010, 824 (826).

308 instruktiv BVerfGE 141, 220 – BKA-Gesetz; NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz; zu den „Eingriffsschwellen" *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff.).

309 Vgl. BVerfGE 100, 313 (376 ff.) – Strategische Fernmeldeaufklärung; E 115, 320 (347 ff.) – Rasterfahndung; E 120, 378 (401 ff.) – Autom. Kennzeichenkontrolle I; E 125, 260 (318 ff.) – Vorratsdatenspeicherung; E 152, 216 (283 ff.) – Autom. Kennzeichenkontrolle II; E 154, 152 (241 ff.) – Ausland-Ausland-Fernmeldeaufklärung

310 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f.; *Klement*, AöR 2009, 35 (45 ff.); *Breckwoldt,* Grundrechtskombinationen, 2014, S. 196 ff.; *Brade*, DÖV 2019, 853 (856 f.); Übertra-

Für eine solche horizontale Kumulation lassen sich allgemeine Verfassungsgrundsätze ins Feld führen, die – so lässt sich spekulieren – bei der Meinungsbildung des BVerfG eine Rolle spielten. Anlasslose Massenüberwachungen brechen mit der Idee, dass der Staat seinen Bürgen generell Vertrauen entgegenbringt.[311] In deren Grundrechte wird aufgrund neuartiger, universeller Bedrohungslagen eingegriffen, obwohl von Beginn an feststeht, dass das Gros dieser Beeinträchtigungen nichts zum sicherheitsrechtlichen Ziel beitragen kann. Faktisch werden die Grundrechtsträger bei anlasslosen Datenverarbeitungen also unter Generalverdacht gestellt. [312] Damit einher geht eine Abkehr von der Idee, dass das Sicherheitsrecht grundsätzlich reaktiv ausgestaltet sein sollte. Eine solche Reaktivität schreibt die Verfassung zwar nicht vor, sie drängt sich aber als rechtsstaatlicher Grundgedanke durchaus auf.[313]

gung auf Maßnahmen außerhalb der Informationseingriffe *Murswiek*, NVwZ-Extra 5/2021 (6); zust. *Schoch*, NVwZ 2022, 1 (6 f.).

311 *Weßlau,* Vorfeldermittlungen, 1989, S. 300 ff.; *Dencker*, FS Dünnebier, 1982, S. 447 (459 f.) *Lisken*, NVwZ 1998, 22 (24); s.a. BayVGH, ZD 2019, 515 (521).

312 *Orantek* NJ 2010, 193 (195); *Breyer*, StV 2007, 214 (217).; *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 493 ff.; *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (31 f.); *Masing*, JZ 2011, 753 (756 f.).

313 *Puschke/Singelnstein*, NJW 2008, 113 (118); *Lisken*, ZRP 1990, 15 (17 ff.); *ders.*, ZRP 1994, 264 (267 f.); *Hund*, NJW 1992, 2118 (2119); zur „Dammbruchtheorie" *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 181 ff.