

Missbrauch staatlicher Datenmacht: Verfassungsrechtliche Perspektive

Thomas Wischmeyer

I. Einführung¹

Verfassung und Verfassungsrecht streben ein möglichst funktionsfähiges Gemeinwesen an und konstituieren dieses durch organisationsrechtliche Vorgaben. Staatliche Stellen müssen daher alle nötigen Informationen zu ihrer Verfügung haben, um die ihnen durch Verfassung und Gesetz zugewiesenen Aufgaben erfüllen zu können. Der Zugriff auf qualitativ und quantitativ hinreichende Daten, auch und gerade solche personenbezogener Natur, ist somit Bedingung der Möglichkeit des recht- und zweckmäßigen Staatshandelns.² Von der Corona-Pandemie bis zum E-Government sehen wir, welche Probleme entstehen, wenn staatliche Stellen zu wenig Daten haben.³ „Small data“ gefährdet die Effektivität und mittelbar auch die Legitimität staatlichen Handelns. Jedenfalls im Grundsatz gilt das auch im Bereich des Sicherheitsrechts, auf das ich mich im Folgenden konzentriere. Denn es ist Ziel und Aufgabe des demokratischen Verfassungsstaates, die Sicherheit seiner Bürger:innen zu gewährleisten.⁴ Und dies verlangt personenbezogene Daten in großer Menge.

- 1 Dem Beitrag liegt ein Kommentar auf dem Symposium zu den Vorträgen von *Moritz Vormbaum* und *Matthias C. Kettemann* zugrunde. Die Vortragsform wurde für die Veröffentlichung beibehalten und nur um ausgewählte Nachweise ergänzt.
- 2 Diesem Themenfeld widmet sich intensiv das Informationsverwaltungsrecht; aus der überbordenden Literatur hierzu s. nur im Überblick *Augsberg*, Informationsverwaltungsrecht, 2014; *Vesting*, Die Bedeutung von Information und Kommunikation für das Handeln der Verwaltung, in Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, 3. Aufl. 2022, § 20; *Wischmeyer*, Informationsbeziehungen in der Verwaltung, in a.a.O., § 24.
- 3 Hierzu im Überblick *Britz/Eifert*, Digitale Transformation der Verwaltung, in Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, 3. Aufl. 2022, § 26.
- 4 Vgl. aus der uferlosen Literatur nur die grundlegenden Beiträge von *Isensee*, Das Grundrecht auf Sicherheit, 1983; *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S.14 ff.; *Stoll*, Sicherheit als Aufgabe, 2003, S.15 ff.; *Brugger*, Gewährleistung von Freiheit und Sicherheit, in VVDStRL 63 (2004), S. 102 ff.; *Gusy*, Gewährleistung von Freiheit und Sicherheit, in VVDStRL 63 (2004), S.151,

Erst in einem zweiten Schritt zieht das Verfassungsrecht dem staatlichen Datenhunger Grenzen. Diese ergeben sich vor allem – nicht nur – aus den Grund- und Menschenrechten. Aus diesen Garantien folgt ein individueller Anspruch der Bürger:innen, die Erhebung und Verarbeitung personenbezogener Daten unter bestimmten – eben: missbräuchlichen – Umständen zu unterlassen.

Aufgabe meines Kommentars ist es nicht, die Gehalte des Rechts auf informationelle Selbstbestimmung und verwandter einschlägiger Grundrechte darzulegen. Hierzu existiert ausreichend Literatur.⁵ Stattdessen will ich hervorheben, dass „verfassungsrechtliche Perspektive“ im digitalen Raum, der ein weitgehend entterritorialisierter Raum ist,⁶ im Plural verstanden werden muss. Diese Pluralität soll im Folgenden zumindest in Ansätzen entfaltet werden. Dazu werde ich in drei kurzen Vignetten darstellen, wie das BVerfG, der EuGH und der United States Supreme Court die Funktion von Verfassungsrecht interpretieren, wenn es um die Einhegung staatlicher Datenmacht geht, und wie unterschiedlich weit der jeweilige Schutzanspruch reicht.⁷ Dabei zeigt sich, dass in dieser für die Gegenwartsgesellschaft zentralen Frage weder ein europäischer oder gar transatlantischer Wertekonsens noch ein einheitliches verfassungsrechtliches Konstruktionsmodell existieren (II.). Noch deutlicher zeigen sich die Differenzen bei der durch das Tagungsthema aufgeworfenen Frage, inwieweit das Verfassungsrecht über Unterlassungsgebote hinaus den Staat positiv zur – womöglich sogar strafrechtlichen – Sanktionierung von (staatlichem)

174 ff.; *Isensee*, Staatsaufgaben, in: *Isensee/Kirchhof* (Hrsg.), *HStR*, Bd. IV, 3. Aufl. 2006, § 73 Rn. 26; *Götz*, Innere Sicherheit, in *Isensee/Kirchhof* (Hrsg.), *HStR*, Bd. IV, 3. Aufl. 2006, § 85; *Thiel*, Die „Entgrenzung“ der Gefahrenabwehr, 2011; *Leuschner*, Sicherheit als Grundsatz, 2018, S. 13 ff.; *Barczak*, *Der nervöse Staat*, 2. Aufl. 2021, S. 353 ff.

5 Vgl. nur aus jüngerer Zeit *Pieper*, Der grundrechtliche Schutz des Kommunikationsraums, 2019; *Schneider*, Fernmeldegeheimnis und Fernmeldeaufklärung, 2020; *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019; *Eichenhofer*, e-Privacy, 2021; *Albers*, Umgang mit personenbezogenen Informationen und Daten, in *Voßkuhle/Eifert/Möllers* (Hrsg.), *Grundlagen des Verwaltungsrechts*, Bd. I, 3. Aufl. 2022, § 22.

6 Zum Stand der Debatte aus Sicht des deutschsprachigen Öffentlichen Rechts s. *Bast*, Völker- und unionsrechtliche Anstöße zur Entterritorialisierung des Rechts, in *VVDStRL* 76 (2017), S. 277 ff.; *Schmalenbach*, Völker- und unionsrechtliche Anstöße zur Entterritorialisierung des Rechts, in *VVDStRL* 76 (2017), S. 245 ff.; *Kahl*, Entterritorialisierung im Wirtschaftsrecht und im Kommunikationsrecht, in *VVDStRL* 76 (2017), S. 343 ff.; *Cornils*, Entterritorialisierung im Wirtschaftsrecht und im Kommunikationsrecht, in *VVDStRL* 76 (2017), S. 390 ff.

7 Aus Zeitgründen bleibt der Ansatz des EGMR, der manche Parallelen mit dem Zugriff des BVerfG aufweist, hier ausgeklammert.

Datenmissbrauch verpflichtet. Das ist, wie ich zeigen will, keineswegs die primäre und, jedenfalls global betrachtet, sogar eine sehr unwahrscheinliche Funktion von Verfassung (III.).

II. Schutz der Privatheit: Verfassungsgerichtliche Schutzkonzeptionen im Vergleich

1. Bundesverfassungsgericht: Privatheitsschutz als Rationalisierungsgebot

Das Grundgesetz enthält bekanntlich verschiedene Grundrechtsgarantien, die in der Lehre oft zum Konzept des verfassungsrechtlichen Privatheitsschutzes verdichtet werden.⁸ Privat ist dabei nicht nur das Intime, dem Blick bewusst Entzogene, sondern etwa auch die interpersonelle Kommunikation über Technologieplattformen und soziale Medien.⁹ Das BVerfG kalibriert den Umfang des grundrechtlichen Schutzes nach Art und Ausmaß der betroffenen Privatheitsinteressen. Dabei orientiert das Gericht seine Arbeit weniger an den einzelnen grundrechtlichen Schutzgehalten als am allgemeinen Verhältnismäßigkeitsgrundsatz.¹⁰ So nutzt das Gericht insbesondere die Angemessenheitsprüfung, um detaillierte Vorgaben für gesetzgeberische Eingriffe zu entwickeln.¹¹ Echte (materielle) Stopp-Regeln sind dabei allerdings sehr selten. Vielmehr verpflichtet das Gericht den Gesetzgeber in erster Linie darauf, normenklare und bestimmte Ermächtigungsgrundlagen zu schaffen sowie organisatorische und prozedurale Sicherungsmechanismen zu implementieren. Auch die oft als „Grenze“ hoheitlicher Datenerhebung interpretierten Einschränkungen in Gestalt der Beschränkung von Erhebungs- bzw. Verwendungszwecken¹², des Kern-

8 Vgl. nur *Rüpke*, Der verfassungsrechtliche Schutz der Privatheit, 1976; *Horn*, Schutz der Privatsphäre, in *Isensee/Kirchhof* (Hrsg.), Handbuch des Staatsrechts, Bd. VII, 3. Aufl. 2009, § 149; *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, S. 90 ff.; *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, 2014, S. 84 ff.; *Gusy/Eichenhofer/Schulte*, e-privacy, JöR 64 (2016), S. 385 ff.; *Eichenhofer* (Fn. 5), S. 9 ff.

9 Zur Reichweite des Grundrechtsschutzes s. *Wismeyer*, in *Dreier/Brosius-Gersdorf*, GG, 4. Aufl. 2023, Art. 10 Rn. 60 ff. Vgl. auch ausführlich *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018.

10 Vgl. beispielhaft zur Übertragung der für das Grundrecht auf informationelle Selbstbestimmung entwickelten Schranken-Schranken auf Art. 10 GG BVerfGE 100, 313, 359; st. Rspr.

11 S. zuletzt insbesondere BVerfGE 141, 220; 154, 152; 156, 11.

12 Vgl. BVerfGE 129, 208, 243 f., Rn. 203 ff.; 141, 220, 270, Rn. 106 ff.; 155, 119, 190, Rn. 154.

bereichsschutzes¹³ sowie der Erhöhung der Eingriffsschwellen¹⁴ wirken in der Praxis primär als Verfahrensgebote für die Rechtsanwender. Die den Privatheitsschutz garantierenden Grundrechte sind, so wie sie das BVerfG versteht, also in erster Linie Instrumente zur Rationalisierung der Datenverarbeitung, nicht zur Minimierung oder gar Verhinderung.

Dieser Zugriff erlaubt dem Gericht eine engmaschige Kontrolle des staatlichen Handelns und gewährt Sicherheitsgesetzgeber und -behörden dennoch hinreichende Handlungsspielräume. Ein solcher Zugriff erscheint auf den ersten Blick gleichermaßen grundrechtsschonend wie praxissensibel. Allerdings hat dies seinen Preis. Zum einen macht sich das Gericht methodisch angreifbar, wenn sich seine Maßstäbe immer weiter vom Verfassungstext entfernen. Wo in der Verfassung steht das Doppeltürmodell?¹⁵ Zum anderen gleichen sich verfassungsrechtliche Maßstäbe und einfachgesetzliche Ermächtigungsgrundlagen mit der Zeit immer stärker an.¹⁶ Das führt zu einem zunehmend dysfunktionalen Verhältnis von Gericht und Sicherheitsgesetzgeber, in dem sich letzterer darauf beschränkt, die verfassungsgerichtlichen Ausführungen „eins-zu-eins“ nachzuzeichnen.¹⁷ Die Eigenrationalität der Verfassung *und* die Eigenlogik des demokratisch erzeugten Gesetzesrechts werden so kompromittiert. Hierzu ließe sich noch viel ergänzen. Ich will an dieser Stelle aber, wie angekündigt, den Blick vom deutschen Recht auf das Unionsrecht lenken.

13 Dazu zuletzt BVerfG, Beschl. v. 9.12.2022, 1 BvR 1345/21, Rn. 101 ff.

14 Vgl. BVerfGE 141, 220, 271, Rn. 109 ff.; 155, 119, 187 ff., Rn. 148 ff.; BVerfG, 1 BvR 1619/17 v. 26.4.2022, Rn. 162 ff., 181 ff.

15 Vgl. BVerfGE 130, 151, 184, Rn. 123; 150, 244, 278, Rn. 80; 150, 309, 335, Rn. 68; 155, 119, 167, Rn. 93 ff.; 179, Rn. 130; 209, Rn. 201.

16 Dies gilt insb. für BVerfGE 141, 220; 154, 152; 156, 11.

17 Vgl. *Groß*, in Friauf/Höfling, GG, Art. 10 (2016), Rn. 71; *Bäcker*, Sicherheitsverfassungsrecht, in Herdegen/Masing/Poscher/Gärditz, HVerfR, § 28 Rn. 184 ff. Besonders aktiv ist die Europäische Union im Bereich der Cybersicherheit, vgl. dazu *Dewar/Cavelty*, Die Cybersicherheitspolitik der Europäischen Union, in Schüneman/Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, 2. Aufl. 2019, S. 281 ff.; *Calliess/Baumgarten*, Cybersecurity in the EU, German Law Journal 21 (2020), S. 1149 ff.; *Bendiek/Pander Maat*, The EU's Cybersecurity Policy, in Siboni/Ezioni (Hrsg.), Cybersecurity and Legal-Regulatory Aspects, 2021, S. 23 ff.; *Wischmeyer*, Cybersecurity in the European multi-level governance system, in Dietrich/Pilniok (Hrsg.), European Security Union Law and Policies, 2024, § 16.

2. EuGH: Privatheitsschutz als Stopp-Regel

Die Dynamik der Sicherheitspolitik verlagert sich derzeit rasant auf die Europäische Union.¹⁸ Sie trifft hier auf einen EuGH, der seinen Anspruch, ein genuines Verfassungsgericht zu sein, gerade auch mit seinen Entscheidungen zum Schutz vor privatem und staatlichem Datenmissbrauch legitimiert.¹⁹ Wie genau die Anwendungsbereiche der Grundrechtskataloge der Charta und des Grundgesetzes voneinander abzugrenzen sind, soll hier dahinstehen.²⁰ Stattdessen ist zu betrachten, wie sich EuGH und BVerfG in ihrem Umgang mit den die Privatheit schützenden Grundrechten unterscheiden. Offensichtlich kann im Rahmen dieses Kommentars kein nuancierter Vergleich, sondern nur eine auch mit Schematisierungen arbeitende Gegenüberstellung geleistet werden.

Als Anschauungsmaterial soll die Rechtsprechung zur Vorratsdatenspeicherung dienen. Während das BVerfG in den einschlägigen Entscheidungen, ganz im obigen Sinne, dem Gesetzgeber das Instrument keineswegs grundsätzlich aus der Hand geschlagen hat,²¹ sondern seinen Einsatz an (rationale) Voraussetzungen gebunden hat, zeigt der EuGH, jedenfalls seit 2014, einen deutlich rigoristischeren Zug. Zwar ist der Gerichtshof mittlerweile von seinem zunächst rein kassatorischen Vorgehen abgerückt²² und hat analog zum BVerfG begonnen, Maßstäbe zu entwickeln, denen

18 Programmatisch *Europäische Kommission*, EU-Strategie für eine Sicherheitsunion 2020–2025, COM (2020) 605. Vgl. im Überblick *Gärditz*, in *Stern/Sodan/Möstl*, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 22 Rn. 81 ff.

19 Vgl. etwa EuGH, C-293/12 u. a. v. 8.4.2014 – Digital Rights Ireland; EuGH, Gutachten I/15 v. 26.7.2017 – PNR-Abkommen EU-Kanada; EuGH, C-207/16 v. 2.10.2018 – Ministerio Fiscal; EuGH, C-311/18 v. 16.7.2020, – Schrems II. S. dazu auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 205 ff. und passim.

20 Zum Verhältnis der Grundrechtsebenen s. aus Sicht des deutschen Verfassungsrechts BVerfG 152, 152, 179 ff., Rn. 63 ff.; 152, 216, 233 ff., Rn. 42 ff.; 158, I, 30 ff., Rn. 56 ff.

21 Grundlegend, wenn auch mit Blick auf die unionsgrundrechtliche Seite teilweise überholt: BVerfGE 121, I, 19 ff., Rn. 146 ff.; 125, 260, 307 ff., Rn. 183 ff. Zur Neufassung der Speicherpflicht im TKG und der korrespondierenden Abrufermächtigung in § 100g II StPO sind aktuell diverse Verfassungsbeschwerden (1 BvR 141/16 u.a.) anhängig; den Normen wird allerdings überwiegend attestiert, den vom BVerfG definierten Maßstäben zu genügen. Das BVerfG hat diesbezüglich mehrfach den Antrag auf Erlass einer einstweiligen Anordnung abgelehnt, vgl. BVerfG (K), 1 BvQ 42/15 u.a. v. 8.6.2016; 1 BvR 3156/15 v. 26.3.2017. Zu landesrechtlichen Kompetenzen in diesem Bereich s. jetzt auch BVerfG, 1 BvR 1619/17 v. 26.4.2022, Rn. 335.

22 So zunächst EuGH, C-293/12 u.a. v. 8.4.2014 – *Digital Rights Ireland*.

mitgliedstaatliche Normen zur Datenspeicherung genügen müssen.²³ Massivem politischem Druck mächtiger Mitgliedstaaten zum Trotz hält der Gerichtshof jedoch am grundsätzlichen Verbot der Maßnahme fest und fasst die Ausnahmen so eng, dass das Instrument für die Ermittler weitgehend nutzlos ist.²⁴

Aus verfassungsrechtlicher Sicht beeindruckt dieses Beharren auf dem Primat des Rechts: Nicht alles wird prozeduralisiert und rationalisiert, Verfassungsrecht wirkt als echte Stopp-Regel. Allerdings sind die politischen Verwerfungen, die ein solcher Zugriff mit sich bringt, beachtlich und stellen die gerade für die Europäische Union prekäre Frage nach der Befolgungsbereitschaft.²⁵ Hinzu kommt, dass der EuGH mangels entsprechender Vorlagefragen seinen rigoristischen Ansatz bisher nur selektiv für ein Ermittlungsinstrument, eben die Vorratsdatenspeicherung, erproben konnte, während das BVerfG in Verfassungsbeschwerden mit der ganzen Bandbreite behördlicher Ermittlungsmaßnahmen konfrontiert ist und schon aus diesem Grund einen anderen Zugriff wählen dürfte. Dem EuGH steht die Probe, inwieweit ein Höchstgericht einen sehr restriktiven Zugriff tatsächlich flächendeckend durchhalten kann, noch bevor.²⁶ Schon bald dürften wir hier mehr wissen.²⁷

23 S. zusammenfassend EuGH, C-511/18 u.a. v. 6.10.2020 – *La Quadrature du Net*; EuGH, C-140/20 v. 5.4.2022 – *G.D.*; EuGH, C-793/19 und C-794/19 v. 20.9.2022 – *SpaceNet und Telekom*; EuGH, C-339/20 und C-397/20 v. 20.9.2022 – *VD und SR*.

24 Vgl. die scharfe Kritik in Conseil d'État, ECLI:FR:CEASS:2021:393099 v. 21.4.2021, Rn. 53. S. auch *Cameron*, *European Union Law Restraints on Intelligence Activities*, *International Journal of Intelligence and Counterintelligence* 2020, 453. S. auch die Überlegungen der *Kommission*, *Non-paper on the way forward on data retention* der Europäischen Kommission, WK 7294/2021 INIT v. 10.6.2021.

25 Zu berücksichtigen ist auch, dass die Vorratsdatenspeicherung zwar eine hohe symbolische Bedeutung hat, ihre praktische Relevanz aus Expertensicht jedoch vergleichsweise gering ist. Hier die Machtprobe zu wagen, ist für ein Höchstgericht daher doch weniger „gefährlich“ als in anderen Konstellationen.

26 Dass der EuGH seine Entscheidungen zugleich zur Selbstermächtigung nutzt, indem er – trotz unionsrechtlich eher zweifelhafter Anknüpfungspunkte – den Anwendungsbereich seiner Rechtsprechung sehr weit ausdehnt, mit Blick auf Art. 4 Abs. 2 S. 3 EUV womöglich sogar überdehnt, ist ein weiterer Aspekt, der in diesem Kontext Beachtung verlangt.

27 Zu beobachten ist insbesondere das Vorlageverfahren zur Verwertbarkeit der Erkenntnisse im Komplex EncroChat, das aktuell unter dem Aktenzeichen C-670/22 beim EuGH anhängig ist. Zur Vorlagefrage s. LG Berlin, B. v. 19.10.2022 – (525 KLS) 279 Js 30/22 (8/22).

3. United States Supreme Court: Privatheitsschutz als Schutz von Mindestpositionen

Die Jurisdiktionsgewalt des EuGH reicht weit, ist aber gleichwohl nicht grenzenlos. In einer vernetzten Welt wird regelmäßig über die Unionsgrenzen hinweg kommuniziert und insbesondere die Inanspruchnahme von Cloud Services führt dazu, dass Daten im außereuropäischen Ausland verarbeitet werden.²⁸ Das ermöglicht den dortigen Behörden den Zugriff und verleiht den Verfassungsgarantien jener Staaten, durch die Kommunikationsdaten geleitet werden, Relevanz für die hier untersuchte Frage.

Ein Großteil des Internetverkehrs wird bekanntlich über US-Anbieter abgewickelt und steht damit dem Zugriff der dortigen Behörden offen. Aus diesem Grund kommt dem US-Verfassungsrecht entscheidende Bedeutung für den globalen Schutz der Telekommunikation zu. Der US Supreme Court versteht die Schutzfunktion der Verfassung, konkret: des Vierten Verfassungszusatzes, nun wiederum in ganz eigener Form. Anders als das BVerfG setzt der Supreme Court nicht auf eine begleitende Rationalitätskontrolle des Sicherheitsgesetzgebers und dynamisiert seine Maßstäbe nur minimal. Anders als der EuGH setzt sich der Supreme Court auch nicht punktuell an die Spitze des normativen Fortschritts. Stattdessen konzentriert er sich darauf – so würden jedenfalls die Verteidiger seiner Rechtsprechung argumentieren –, eine im Text und in der Tradition der Verfassung klar dokumentierte Mindestposition zu schützen: Die Verfassung schützt Inländer (sog. US-Personen) im Inland vor der gezielten Überwachung von *Kommunikationsinhalten*.²⁹

Das scheint der klassischen Funktion der Grundrechtskontrolle recht nahe zu kommen und vermeidet genau jene verfassungstheoretischen Schwierigkeiten, die der rationalisierende Ansatz des BVerfG und die progressive Herangehensweise des EuGH mit Blick auf die Legitimität der Verfassungsgerichtsbarkeit als einer *countermajoritarian institution* mit sich bringt. Das Problem eines solchen eng auf den Text und die Entstehungssituation gezogenen Zugriffs auf die Verfassung ist jedoch offensichtlich.³⁰ Die Recht-

28 Grundlegend *Daskal*, The Un-Territoriality of Data, Yale Law Journal 125 (2015), S. 326 ff.

29 Grundlegend *Katz v. United States*, 389 U.S. 347 (1967); *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). Ausführlich *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014.

30 Zum Folgenden ausführlich *Wischmeyer*, Überwachung ohne Grenzen, 2017.

sprechung beruht auf von der Wirklichkeit längst überholten sozialen und technologischen Annahmen. Die Differenz zwischen statischem Normprogramm und dynamischem Realbereich produziert über die Zeit Inkohärenzen und unterminiert damit den Schutzanspruch der Verfassung.³¹ Auch jene Mindestgarantien, die eigentlich gesichert werden sollen, werden so mit der Zeit unterlaufen. Dennoch: Aus Sicht des Supreme Court sind die im Zuge des sogenannten NSA-Skandals aufgedeckten staatlichen Ermittlungspraktiken eben gerade kein „Datenmissbrauch“ und keine systematische Datenschutzverletzung; vielmehr sind sie, zumindest in weiten Teilen, durchaus mit den vor über zweihundert Jahren getroffenen Grundentscheidungen des Verfassungsgebers kompatibel.

III. Grundrechtlich radizierte Sanktionspflichten für Datenmissbrauch?

Während das BVerfG den grundrechtlichen Privatheitsschutz als Instrument zur Rationalisierung der Sicherheitspolitik nutzt, möchte der EuGH mit seiner Hilfe den Primat des Rechts (und seine eigene Vorrangstellung) sichern. Der United States Supreme Court setzt schließlich die Rolle der Verfassung mit der Gewährleistung von Mindestschutzpositionen gleich. Der vergleichende Blick zeigt, dass die Vorstellung, Verfassungen bzw. Verfassungsgerichte könnten und wollten dem staatlichen Missbrauch von Daten effektiv entgegenwirken, einer nuancierten Behandlung bedarf. Schon was den Anspruch betrifft, staatliche Datensammlungen in der Sicherheitsverwaltung zu beschränken, treffen wir in Deutschland, in Europa und in den USA sehr unterschiedliche Modelle an, mit je unterschiedlicher Schutzreichweite und – wie angedeutet – je eigenen Schwächen.

Dass die Grundrechte präventiv gegen staatlichen Datenmissbrauch in Stellung gebracht werden können, indem sie zur Unterlassung und Begrenzung staatlicher Datenverarbeitung zwingen können – das lässt sich allerdings noch als eine Art internationaler Minimalkonsens festhalten. Von einem solchen Konsens kann dann aber nicht mehr die Rede sein, wenn es um eine verfassungsrechtlich radizierte Pflicht zur Sanktionierung von Verstößen geht. Hierzu finden sich bei den in Augenschein genommenen Verfassungsordnungen nur beim BVerfG entsprechende Hinweise. So hat das BVerfG in der Vorratsdatenspeicherungsentscheidung ausgeführt:

31 Selbstverständlich ist die Dynamik der technischen Entwicklung auch für die deutsche Verfassungsgerichtsbarkeit eine erhebliche Herausforderung.

„Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts, auch soweit er in Art. 10 Abs. 1 GG eine spezielle Ausprägung gefunden hat, angesichts der immateriellen Natur dieses Rechts verkümmern würde [...], widerspräche dies der Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen [...] und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen.“³²

Entsprechend hat das Gericht dann auch in seiner Entscheidung zum BKAG aus dem Verhältnismäßigkeitsgebot abgeleitet, dass die Rechtsordnung „wirksame Sanktionen bei Rechtsverletzungen“ vorsehen muss.³³

Diese Aussagen des BVerfG dürfen jedoch nicht überinterpretiert werden. So handelt es sich bei der Forderung nach wirksamen Sanktionen erstens nur um ein einzelnes Element in der gesamten Verhältnismäßigkeitsarchitektur. Zweitens versteht das Gericht „Sanktion“ denkbar weit und fasst auch die zivilrechtliche Haftung oder strafprozessuale Beweisverwertungsverbote darunter. Drittens betont es den Gestaltungsspielraum des Gesetzgebers an dieser Stelle ganz besonders. Von einer Pflicht zur Pönalisierung, wie sie aus dem Kontext der Abtreibung bekannt ist, kann also keine Rede sein.

IV. Ausblick

Ich fasse zusammen: Wenn die Erwartung war, aus „der“ Verfassung ließen sich klare Direktiven für die Sanktionierung staatlichen Datenmissbrauchs ableiten, dann musste diese enttäuscht werden. Vielmehr verlangt das Verfassungsrecht in erster Linie einen gut informierten Staat. Auch die Grundrechte ziehen staatlichen Datensammlungen nur eingeschränkt Grenzen. Und Pflichten zur Sanktionierung von Datenmissbrauch lassen sich zwar im deutschen Recht dogmatisch konstruieren; der vergleichende Blick zeigt jedoch, wie wenig anschlussfähig ein solches (Verfassungs-)Verständnis international ist. Und auch hierzulande können die Sanktionspflichten vom Gesetzgeber auf ganz unterschiedliche Art und Weise umgesetzt werden.

32 BVerfGE 125, 260, 339 f., Rn. 252 f.

33 BVerfGE 141, 220, 284, Rn. 139.

Aber das ist ja vielleicht ohnehin die grundlegendste Einsicht des Verfassungsrechts: Auf den Gesetzgeber kommt es an.