19. Nutzen und Risiken der Kontrolle von Kommunikation

Wolfgang Schulz

19.1 Einführung

Das Spannungsfeld der Zielsetzungen der Regulierung im Bereich Kommunikation und Kontrolle wird schlaglichtartig deutlich, wenn man zwei geltende Normen gegenüberstellt, die beide eine durchaus prominente Rolle im Kommunikationsrecht besitzen.

Dies ist zunächst § 113a des Telekommunikationsgesetzes (TKG), der besagt:

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten [...] sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern.

Diese unter dem Rubrum »Vorratsdatenspeicherung« heftig diskutierte Regelung liest sich auffallend anders als der § 13 Telemediengesetz (TMG), der normiert:

(6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Nun stehen diese Regelungen nicht in einem wirklichen Widerspruch, da die Verpflichteten im einen Fall Telekommunikationsdiensteanbieter und im anderen Telemedienanbieter sind, also einmal Anbieter der Transport- und einmal der Inhalte-Ebene betrifft. Nichtsdestotrotz wird deutlich, dass ein Spannungsverhältnis besteht. Auf der einen Seite das Interesse daran, etwa zum Schutz von Rechtsgütern wie der äußeren und inneren Sicherheit Informationen über Kommunikation zu erhalten, auf der ande-

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

ren Seite das Interesse, gerade in diesem Bereich anonym, d.h. auch ohne Kontrollrisiko, kommunizieren zu können.

Der folgende Beitrag will dieses Spannungsverhältnis aus einer vor allem verfassungsrechtlichen Perspektive beleuchten.

19.2 Kommunikation in der Wissensgesellschaft

Über die Sinnhaftigkeit von Labeln wie »Informationsgesellschaft« oder »Wissensgesellschaft« wird trefflich gestritten.[1] Worauf sie sicherlich aufmerksam machen, ist der Umstand, dass Kommunikationstechnologien und darauf basierende Kommunikationsdienste zunehmend alle Lebensbereiche durchdringen.

Auf der Ebene der technischen Infrastruktur ist etwa zu beobachten, dass seit 2006 in der Bundesrepublik die Penetration mit Mobilfunkanschlüssen mehr als 100 Prozent beträgt, d.h. rechnerisch kommt auf jeden Einwohner mehr als ein Mobilfunkvertrag.[2] Der Ausbau der Netze für Mobilkommunikation sowie der technische Fortschritt bei den Mobiltelefonen, insbesondere bei der Darstellung audiovisueller Daten sowie durchsatzstärkeren Datenanbindungen, eröffnen weitere Verbreitungsmöglichkeiten für digitalisierte Inhalte, die ortsunabhängig genutzt werden können.[3]

Letzteres verweist bereits auf ein Phänomen, das in der Fachwelt als »Konvergenz« thematisiert wird, nämlich den Umstand, dass die Digitalisierung der Übertragungswege dazu führt, dass vormals mit bestimmten Kommunikationsformen verknüpfte technische Plattformen nun offen für ganz unterschiedliche Kommunikationsdienste sind. Diese unbestrittene Ebene der technischen Konvergenz[4] schlägt nicht unbedingt auf den Ebenen der Angebote und der Nutzung durch, auch wenn sich zunehmend Verwischungen zwischen ehemals getrennten Formaten ergeben und eine gewisse Austauschbarkeit und auch Funktionsverschiebungen bei den Nutzern zu beobachten sind, etwa von klassischen Medien hin zu Online-Angeboten.[5]

Die Durchdringung aller Lebensbereiche mit Kommunikationsdiensten wird dadurch erleichtert, dass auch im Bereich der breitbandigen kabelbasierten Internetanschlüsse starke Zuwachsraten zu verzeichnen

1 | Vgl. Hans-Dieter Kübler: Mythos Wissensgesellschaft, Wiesbaden: VS Verlag 2009, S. 82ff.

2 | Vgl. Bundesnetzagentur (Hg.): Jahresbericht 2007, S. 81.

3 | Vgl. Hans-Bredow-Institut (Hg.): Wissenschaftliches Gutachten zum Kommunikations- und Medienbericht der Bundesregierung 2008, S. 164.

4 | Vgl. zum Konvergenzbegriff: Wolfgang Hoffmann-Riem/Wolfgang Schulz/Thorsten Held: Konvergenz und Regulierung, Baden-Baden: Nomos 2000.

5 | Vgl. Hans-Bredow-Institut (Hg.): Wissenschaftliches Gutachten zum Medien- und Kommunikationsbericht der Bundesregierung 2008, S. 235ff.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

sind. Ende 2008 ist in über 23 Millionen Haushalten der Zugang zu breitbandigem Internet in der Bundesrepublik möglich.[6] Damit liegt die Bundesrepublik im EU-Vergleich zwar nur im oberen Mittelfeld,[7] dennoch steigt auch in Deutschland die Online-Nutzung weiterhin an, auch wenn gelegentlich davon ausgegangen wird, dass nur eine Sättigung deutlich unter der 100 %-Marke erreicht werden kann.[8] Es waren durchschnittlich 42,84 Millionen Personen ab 14 Jahren zwischen Juli und September 2008 online. Davon nutzten 97,5 % das Internet mindestens einmal innerhalb von drei Monaten, 96,9 % nutzen es täglich.[9]

Ein wichtiger Aspekt ist, dass sich das Internet-Protokoll (IP-Protokoll) als Standard etabliert hat. Experten gehen überwiegend davon aus, dass sich die Kommunikationsinfrastruktur auf dem Weg zum »All-IP« befindet.[10] Dies macht es nicht nur schwierig zu bestimmen, was eigentlich »das Internet« ist, wenn man davon ausgeht, dass dieses lediglich durch den Protokollstandard definiert wird, über den ganz unterschiedliche Dienste von der Telefonie bis zu traditionellem Fernsehen übertragen werden können. Man sieht auch beispielsweise einer ganz normalen Breitbandfernsehkabelanlage nicht mehr an, ob sie letztlich genauso wie Web-TV auf dem IT-Standard basiert.

Der Trend zum All-IP umschließt auch die Vision, dass die Kommunikation technischer Geräte untereinander weiterhin verstärkt über Netze auf IP-Basis abgewickelt wird und so ein »Internet der Dinge« entsteht, bis hin zu dem mittlerweile schon sprichwörtlichen Kühlschrank, der selbst neuen Riesling bestellt, wenn die letzte Flasche entnommen wird.

Es liegt auf der Hand, dass diese Entwicklung die Kontrolle potenziell erleichtern kann, da grundsätzlich alles auf demselben Protokollstandard basiert. Es macht auch deutlich, dass damit Daten von ganz unterschiedlicher Sensibilität betroffen sein können, denn auf den Netzen läuft möglicherweise rein technischer Datenverkehr neben individueller Mediennutzung, Gesundheitsdaten neben Werbung, Kommunikation zwischen Journalisten und Informanten neben Software-Downloads. Es sind faktisch alle Bereiche des Lebens umfasst, Bildung, Beruf, Politik, Freizeit, höchstpersönliche Lebensbereiche und so weiter.

Ein für die vorliegende Fragestellung interessanter Umstand besteht darin, dass »das Internet« potenziell global, weltöffentlich ist, de facto aber entweder allein durch die Nutzung oder aber auch durch technische

6 | Vgl. Bundesnetzagentur (Hg.): Jahresbericht 2008, S. 69.

7 | Vgl. KOM (2008) 158, S. 9.

8 | Vgl. Birgit van Eimeren/Beate Frees: »Ergebnisse der ARD/ZDF-Onlinestudie 2008 -Internetverbreitung: Größter Zuwachs bei Silver-Surfern«, in: Media Perspektiven 7 (2008), S. 330-344, hier. S. 331.

9 | Bundesnetzagentur (Hg.): Jahresbericht 2008, S. 84.

10 | Vgl. zur verständlichen Erklärung der Technik: Anatol Badach: Voice over IP, München: Hanser 2007.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

Schutzmechanismen die Kommunikation deutlich kleinräumiger stattfindet.

Für alle vorgenannten Kommunikationsformen gilt, dass mit der steigenden sozialen Bedeutung der Kommunikationsnetze auch das Kontrollinteresse zunimmt, zum einen, weil die Kommunikationsformen selbst Risiken auslösen oder vergrößern – etwa wenn Kriminelle oder Terroristen sich des Netzes als Kommunikationsplattform bedienen oder Copyright-Piraterie durch die Netze deutlich vereinfacht wird –, allerdings auch, weil die Ubiquität der Netze Kontrolle einfach und effektiv macht. Interessant ist dabei, dass mit staatlichem Kontrollinteresse auch das private zunimmt; bei letzterem sind es vor allem die Inhaber von Rechten an urheberrechtlich geschützten Werken, die eine Kontrolle einfordern.[11]

19.3 Formen der Kontrolle

Wenn über Kontrolle von Kommunikation gesprochen wird, dann sind unterschiedliche Gegenstände der Kontrolle denkbar, die durchaus unterschiedlichen rechtlichen Regelungen unterliegen können. So ist zu unterscheiden, ob der Inhalt von Kommunikation kontrolliert wird, die Identität der Kommunizierenden in Rede steht, der Ort ermittelt werden soll, von dem aus kommuniziert wird, oder es um andere Umstände der Kommunikation geht. Besonders sensibel sind Datenschützer, wenn unterschiedliche dieser Aspekte zusammengeführt und Kommunikationsprofile erstellt werden.[12]

Es können dabei ganz unterschiedliche Ansatzpunkte für die Kontrolle gewählt werden, etwa Auskünfte der unterschiedlichen am Kommunikationsprozess beteiligten Akteure, von denen es bei IP-Netzen diverse gibt, etwa Betreiber des genutzten Telekommunikationsnetzes, den Access-Provider, der die entsprechenden Nutzer ins Internet vermittelt, Content-Provider, die selbst Inhalte zur Verfügung stellen, und andere Anbieter von Telemedien, die etwa als Aggregatoren oder Anbieter von Suchmaschinen eine vermittelnde Funktion erfüllen.[13] Schließlich kann aber auch eine Kommunikationskontrolle unmittelbar bei Einzelnutzern erfolgen,

11 | Dirk Seichter: »Die Umsetzung der Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums«, in: Wettbewerb in Recht und Praxis (2006), S. 391-400.

12 | Vgl. zu diesem Problem Gerald Spindler/Judith Nink: Kommentierung zu § 15 TMG, in: Gerald Spindler/Fabian Schuster (Hg.), Recht der elektronischen Medien, München: Beck 2008, Rn. 7.

13 | Alexander Tettenborn/Gunnar Bender/Natalie Lübben/Jörg Karenfort: »Rechtsrahmen für den elektronischen Geschäftsverkehr«, in: Betriebs-Berater Beilage (2001), Nr. 10, S. 1-40.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

wie die Diskussion[14] mit anschließender Bundesverfassungsgerichtsentscheidung[15] über die so genannten »Bundes-Trojaner« gezeigt hat, also die Kommunikationsüberwachung über auf heimische PCs eingespielte Software-Programme.

Die rechtlichen Voraussetzungen sind vielfältig, auch differenziert nach dem Grund der Kontrolle und den ermächtigten Behörden. Der folgende Überblick ist daher notwendigerweise kursorisch und unvollständig.

Die gesetzlichen Grundlagen zur Überwachung telekommunikativ übermittelter Kommunikation umfasst Bundes- und Ländergesetze und ist auf den Gebieten des Telekommunikations-, Strafverfahrens- sowie Polizeirechts und dem Recht der Nachrichtendienste anzutreffen. Damit das Verhältnis dieser Normbereiche nicht einfach den ungeschriebenen Kollisionsregeln folgen muss, enthält § 110 Abs. 1 Satz 6 TKG eine besondere legislative Kollisionsregel, wonach die strafverfahrensrechtlichen, nachrichtendienstlichen und landesrechtlichen Regelungen zur polizeilich-präventiven Telekommunikationsüberwachung – von den telekommunikationsrechtlichen Vorschriften – unberührt bleiben.[16]

19.4 StPO

Im achten Abschnitt ist die Überwachung des Fernmeldeverkehrs geregelt. Die §§ 99, 100a und 100g StPO enthalten spezielle Ermächtigungsgrundlagen für Eingriffe in Art. 10 GG, diese sperren jedoch nicht den Rückgriff auf die allgemeinen Vorschriften.

19.4.1 §§ 94, 98 StPO

Die Eingriffsbefugnisse gem. §§ 94ff. StPO sind zwar ursprünglich auf die Beschlagnahme körperlicher Gegenstände zugeschnitten; der Wortsinn von § 94 StPO gestattet es jedoch, als »Gegenstand« des Zugriffs auch nichtkörperliche Gegenstände zu verstehen.[17] § 94 StPO erfasst grund-

14 | Zur Diskussion vgl. Burkhard Hirsch: »Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme«, in: Neue Juristische Wochenschrift (2008), S. 1922-1925; Bertold Huber: »Trojaner mit Schlapphut – Heimliche ›Online-Durchsuchung‹ nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz«, in: Neue Zeitschrift für Verwaltungsrecht (2007), S. 880-884.

15 | BVerfGE 120, 274.

16 | Kurt Graulich: »Telekommunikationsgesetz und Vorratsdatenspeicherung«, in: Neue Zeitschrift für Verwaltungsrecht (2008), S. 485-492, hier S. 487.

17 | Vgl. BVerfGE 113, 29 (50).

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

sätzlich alle Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können.[18]

Die Maßnahme muss in angemessenem Verhältnis zu der Schwere der Straftat und der Stärke des Tatverdachts stehen.

19.4.2 § 100a StPO

Die eigentlichen Eingriffsvoraussetzungen für die Anordnung einer Überwachung der Telekommunikation sind nun in § 100a Abs. 1 StPO in den Ziff. 1 bis 3 enthalten. Durch die Formulierung »ohne Wissen des Betroffenen« am Anfang sollte der Aspekt der Heimlichkeit der Maßnahme und somit die Eingriffsintensität besonders hervorgehoben werden.[19] Der Erlass einer Anordnung nach § 100a StPO ist nur bei Vorliegen des durch bestimmte Tatsachen begründeten Verdachts einer Katalogtat nach Abs. 2 zulässig. Zusätzlich muss die Tat nicht nur abstrakt, sondern auch im Einzelfall schwer wiegen. Auf diese Weise sollen jene Sachverhalte ausgeschieden werden, die zwar dem Anlasstatenkatalog grundsätzlich unterfallen, jedoch mangels hinreichender Schwere im konkreten Einzelfall den mit einer Telekommunikationsüberwachung verbundenen Eingriff in das Fernmeldegeheimnis nicht zu rechtfertigen vermögen.[20] Schließlich darf eine Maßnahme nach § 100a StPO nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre (Abs. 1 Nr. 3). Die Maßnahme ist in erster Line gegen Beschuldigte, unter den Voraussetzungen des Abs. 3, aber auch gegen Nichtbeschuldigte anwendbar.

Wenn gewonnene Erkenntnisse den Kernbereich privater Lebensgestaltung betreffen, ist nach Abs. 4 ein Erhebungs- bzw. Verwertungsverbot normiert.

19.4.3 § 100g StPO

Die Verkehrsdatenerhebung ist – eingeschränkt – bei Straftaten erlaubt, die mittels Telekommunikation begangen wurden, und zwar auch, wenn diese Straftaten nicht von erheblicher Bedeutung sind (Abs. 1 Satz 1 Nr. 2), nicht jedoch bei Ordnungswidrigkeiten (§ 46 Abs. 3 Satz 1 OWiG). Bei mittels Telekommunikation begangenen Straftaten ist diese Maßnahme

18 | BVerfGE, in: Neue Juristische Wochenschrift (2009), S. 2431-2439, hier S. 2434.

19 | Wolfgang Bär: »Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen«, in: Multimedia und Recht (2008), S. 215-222, hier S. 216.

20 | Jürgen Peter Graf: Kommentierung zu § 100a StPO, in: Jürgen Peter Graf/Klaus Folk (Hg.), Beck'scher Online-Kommentar zur StPO, München: Beck, Stand 15.06.2009, Rn. 38.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

nach Abs. 1 Satz 2 nur unter engeren Voraussetzungen möglich. Die Taten müssen vollendet sein, es gilt die strenge Subsidiaritätsklausel (§ 100c) und die Erhebung der Daten muss in einem angemessenen Verhältnis zur Bedeutung der Sache stehen.[21]

Es gibt insbesondere zwei Gruppen von Straftaten: Delikte, bei denen die Telekommunikation notwendiges Tatmittel zur Begehung ist, und Straftaten, bei denen der Täter die Anonymität der Telekommunikation nutzt. Das gilt namentlich auch für Straftaten unter Nutzung des Internets.[22]

19.5 TKG

19.5.1 § 113 TKG

§ 113 TKG ist als Befugnisnorm ausgestaltet.[23] Denn in § 113 TKG ist die Rechtsfolge in Form der Auskunftspflicht und deren tatbestandlichen Voraussetzungen festgelegt. Das Auskunftsverfahren ist durch die direkte Anfrage der berechtigten Stellen bei dem Verpflichteten Telekommunikationsunternehmen und die direkte Auskunft gegenüber den berechtigten Stellen gekennzeichnet. Soweit die Unternehmen nach § 113 Abs. 1 Satz 1 TKG zur Auskunftserteilung über erhobene Daten verpflichtet sind, ist damit auch die Auskunftserteilung datenschutzrechtlich gerechtfertigt. Von der Auskunftspflicht ausgenommen sind explizit solche Daten, die dem Fernmeldegeheimnis unterliegen.[24] Die Norm dient sowohl der Strafverfolgung als auch der Gefahrenabwehr.

19.6 BKAG

19.6.11 § 20k BKAG

Bei den Online-Durchsuchungen,[25] in § 20k BKAG als »verdeckte Eingriffe in informationstechnische Systeme« bezeichnet, handelt es sich um Maßnahmen, die regelmäßig gleichzeitig präventive wie auch repressive

21 | Armin Nack: Kommentierung zu § 100g StPO, in: Rolf Hannich (Hg.), Karlsruher Kommentar zur Strafprozessordnung, München: Beck 2008, Rn. 7.

22 | Vgl. ebd., Rn. 8.

23 | Zu 113a und 113b TKG vgl. Graulich, NVwZ 2008, S. 485-492.

24 | Jens Eckhardt: Kommentierung zu § 113 TKG, in: Gerald Spindler/Fabian Schuster (Hg.), Recht der elektronischen Medien, München: Beck 2008, Rn. 6.

25 | §§ 102, 103 StPO bieten keine Ermächtigungsgrundlage für Online-Durchsuchung, siehe Kai Cornelius: »Besonderheiten des Strafrechts und Strafprozessrechts (Teil 8)«, in: Andreas Leupold/Silke Glossner (Hg.), Münchener Anwaltshandbuch IT-Recht, München: Beck 2008, Rn. 183 und dort Fn. 27.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

Zwecke erfüllen können bzw. sollen.[26] Nach dem Tatbestand des § 20k Abs. 1 sind heimliche Eingriffe in informationstechnische Systeme zulässig, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr für höchstrangige Rechtsgüter, namentlich Leib und Leben von Personen sowie überragend wichtige Güter der Allgemeinheit vorliegt.

19.6.2 § 20l BKAG

Neben der tatbestandlichen Schwelle einer dringenden Gefahr ist eine Telekommunikationsüberwachung auch zulässig bei tatsächlichen Anhaltspunkten für die Vorbereitung einer terroristischen Straftat (vgl. § 20l Abs. 2 Nr. 2 BKAG). § 20l Abs. 2 BKAG regelt die Quellen-Telekommunikationsüberwachung. Diese ist mit der unbemerkten Infiltration eines von der Zielperson genutzten informationstechnischen Systems verbunden und weist insoweit technische Ähnlichkeiten mit einer Online-Durchsuchung auf. Die Regelung in § 20l Abs. 6 entspricht insoweit nicht den verfassungsgerichtlichen Maßgaben zum Kernbereichsschutz, als ein Überwachungsverbot lediglich bei tatsächlichen Anhaltspunkten für die alleinige Betroffenheit der Intimsphäre der Betroffenen bestimmt wird.[27]

19.7 G 10

Einen besonders weitreichenden Eingriff in Art. 10 Abs. 1 GG enthält das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz, G 10). In der Literatur wurde das G 10 überwiegend als verfassungswidrig klassifiziert.[28] Das Bundesverfassungsgericht hat das G 10 im Wege einer verfassungskonformen Auslegung als mit dem GG vereinbar erklärt.[29]

19.8 Privilegierung für Journalisten

Ein immer wieder diskutiertes Thema sind besonders schützenswerte Kommunikationsbeziehungen wie die von Journalisten zu ihren Infor-

26 | Fredrik Roggan: »Das neue BKA-Gesetz. Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur«, in: Neue Juristische Wochenschrift (2009), S. 257-262, hier S. 259.

27 | Vgl. ebd., S. 262.

28 | Martin Pagenkopf: Kommentierung zu Art. 10 GG, in: Michael Sachs (Hg.), Grundgesetz-Kommentar, München: Beck 2009, Rn. 50, m.w.N.

29 | BVerfGE 30, 1.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

manten.[30] Das Bundesverfassungsgericht geht allerdings nicht von einer verfassungsrechtlich gebotenen generellen Privilegierung der Beziehung aus, obwohl etwa § 53 Abs. 1 Satz 2 StPO zur Verweigerung des Zeugnisses darüber berechtigt. Es schließt mangels Regelungslücke die analoge Anwendung des § 53 Abs. 1 Satz 2 StPO auf Ermittlungsmaßnahmen betreffend den journalistischen Kommunikationsverkehr aus, d.h. § 100a StPO darf auch gegen Journalisten angewandt werden. Im Rahmen der Verhältnismäßigkeitsprüfung sind aber die Besonderheiten des Einzelfalls zu berücksichtigen.[31]

19.9 Verfassungsrechtliche Vorgaben

Staatliche Kontrolle von Kommunikation kann sich im Schutzbereich unterschiedlicher Grundrechte auswirken, je nachdem, um welche Kontrollform und welchen Ansatzpunkt der Kontrolle es sich handelt. Die einschlägigen Normen und damit verbundenen Strukturierungen und Begrenzungen von Kommunikationskontrolle sollen im Folgenden – wiederum sehr kursorisch – umrissen werden.

Einschlägig ist natürlich zunächst das Brief- und Fernmeldegeheimnis nach Art. 10 GG.[32] Es erfasst zuvörderst den Kommunikationsinhalt; die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis von Inhalten eines über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Informations- und Gedankenaustausches zu verschaffen.[33] Es ist jede unkörperliche Übermittlung individueller Kommunikation erfasst, unabhängig von Netzen und Protokollstandards. Es muss allerdings ein verbergender Kommunikationsweg vorliegen; der Umstand, dass internetvermittelte Kommunikation etwa in Form von E-Mails in Fachkreisen mit einer von jedem lesbaren Postkarte verglichen wird, ändert nichts daran, dass sie vom Schutz erfasst werden.[34]

Beschränkungen sind gemäß Art. 10 Abs. 2 Satz 1 GG auf der Grundlage eines Gesetzes möglich. Der oben angeführte § 100a StPO und auch § 100b Abs. 1 StPO sind entsprechende Gesetze. Auch das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10, s.o.) wird

30 | Dieter Kugelmann: »Die Vertraulichkeit journalistischer Kommunikation und das BVerfG«, in: Neue Juristische Wochenschrift (2003), S. 1777-1780.

31 | BVerfGE, in: Neue Juristische Wochenschrift (2003), S. 1787-1795, hier S. 1794.

32 | Vgl. zu den einzelnen Schutzgegenständen Pagenkopf, Kommentierung zu Art. 10 GG, Rn. 12ff.

33 | BVerfGE 100, 313 (358).

34 | Vgl. Wolfgang Löwer: Kommentierung zu Art. 10 GG, in: Ingo von Münch/Philip Kunig (Hg.), Grundgesetz-Kommentar, München: Beck 2009, Rn. 14.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

trotz zahlreicher Kritik in der Wissenschaft[35] in verfassungskonformer Auslegung vom Bundesverfassungsgericht für verfassungskonform gehalten.[36]

Das Bundesverfassungsgericht hat sich kürzlich mit der Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers auseinandergesetzt. Die Maßnahme, die hier auf §§ 94, 98 StPO, die eine verfassungsmäßige Grundlage für den Eingriff in Art. 10 GG bilden, beruhte, muss dem Gericht zufolge vor allem in angemessenem Verhältnis zu der Schwere der Straftat und der Schwere des Tatverdachts stehen. Hierbei ist nicht nur die Bedeutung des potenziellen Beweismittels für das Strafverfahren, sondern auch der Grad des auf die verfahrenserheblichen Gegenstände oder Daten bezogenen Auffindeverdachts zu bewerten. Auf die E-Mails darf nur zugegriffen werden, wenn ein konkret zu beschreibender Tatvorwurf vorliegt, also mehr als nur vage Anhaltspunkte oder bloße Vermutungen.[37]

Beim Zugriff auf die bei dem Provider gespeicherten E-Mails ist auch die Bedeutung der E-Mails für das Strafverfahren sowie der Grad des Auffindeverdachts zu bewerten. Im Einzelfall können die Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung der zu beschlagnahmenden E-Mails sowie die Vagheit des Auffindeverdachts der Maßnahme entgegenstehen.[38]

Im konkreten Fall hat das Bundesverfassungsgericht den Eingriff in Art. 10 GG als verhältnismäßig erachtet.

Neben dem Fernmeldegeheimnis beinhaltet der Schutz der Persönlichkeit nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG durch unterschiedliche Gewährleistungsgehalte Grenzen für die Kontrolle von Kommunikation.

Ein solcher Gehalt ist zunächst das Recht auf informationelle Selbstbestimmung, die verfassungsrechtliche Verankerung des Datenschutzes. Das Bundesverfassungsgericht hatte dies im so genannten Volkszählungsurteil herausgearbeitet.[39] Es gewährt grundsätzlich die Autonomie des Betroffenen über seine personenbezogenen Daten. Beschränkungen sind auch hier möglich, sie müssen allerdings den vom Bundesverfassungsgericht für die informationelle Selbstbestimmung herausgearbeite-

35 | Vgl. etwa Christoph Gusy: »Der Schutz vor Überwachungsmaßnahmen nach dem Gesetz zur Beschränkung des Art. 10 GG«, in: Neue Juristische Wochenschrift (1981), S. 1581-1586; Peter Häberle: »Die Abhörentscheidung des Bundesverfassungsgerichts vom 15.12.1970«, in: Juristenzeitung (1971), S. 145-156; Bernhard Schlink: »Das Abhörurteil des Bundesverfassungsgerichts«, in: Der Staat 12 (1973), S. 85-108.

36 | BVerfGE 30, 1.

37 | BVerfGE, in: Neue Juristische Wochenschrift (2009), S. 2431-2439, hier S. 2435f.

38 | Ebd., S. 2436.

39 | BVerfGE 65, 1 (46ff.).

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

ten Grundsätzen der Verhältnismäßigkeit genügen. Dazu gehört, dass das Bundesverfassungsgericht eine anlasslose Erfassung wie etwa bei der Rasterfahndung nur unter der Voraussetzung als gerechtfertigt ansieht, dass eine konkrete Gefahr für hochrangige Rechtsgüter gegeben ist.[40] Das Bundesverfassungsgericht ist für seine Orientierung am Gefahrenbegriff kritisiert worden, weil sie neuartige, etwa terroristische, Bedrohungslagen nicht hinreichend erfassen könnten.[41] Allerdings hat das Gericht seinen Gefahrenbegriff durchaus den Veränderungen angepasst.[42] Es bleibt allerdings mit Blick auf die Risiken gerade der Kontrolle personenbezogener Informationen bei seiner Grundhaltung.

Konsequent auf der genannten Linie und auch konsequent mit Blick auf die dogmatische Haltung des Bundesverfassungsgerichts in den letzten Jahren, die Gewährleistungsgehalte der Grundrechte klarer herauszuarbeiten und auf neue Gefährdungslagen gegebenenfalls mit neuen Gewährleistungsgehalten zu reagieren, ist die »Erfindung« des umgangssprachlich so genannten »IT-Grundrechts«, richtigerweise die Herausarbeitung eines Gewährleistungsgehaltes mit dem Inhalt, dass die Sicherheit und Integrität informationstechnischer Systeme besonders durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützt ist.[43] Die Entscheidung ist im vorliegenden Kontext vor allem interessant, weil sie anerkennt, dass sich die Persönlichkeit von Menschen durch die oben beschriebene zunehmende kommunikationstechnische Vernetzung quasi ins Technische hinein verlängert und dort in besonderer Weise geschützt sein muss, da der Betreffende in seiner Lebensgestaltung auf die Sicherheit und Integrität der Systeme vertraut und vertrauen darf.[44]

Wenn es um die Kontrolle von Kommunikation geht, können auch die Freiheiten aus Art. 5 Abs. 1 Satz 1 und 2 GG, also die Meinungsfreiheit, die Informationsfreiheit und die Massenmedienfreiheiten betroffen sein.[45] Die Abgrenzung zu den Freiheiten nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG ist in derartigen Fällen nicht einfach, etwa wenn es um die Frage geht, wann das Überwachen des Medienkonsums das Recht auf

40 | Vgl. BVerfGE 115, 320 (344ff.).

41 | Hans-Detlef Horn: »Vorbeugende Rasterfahndung und informationelle Selbstbestimmung«, in: Die öffentliche Verwaltung (2003), S. 746-755.

42 | Vgl. Wolfgang Hoffmann-Riem: »Freiheit und Sicherheit im Angesicht terroristischer Anschläge«, in: Zeitschrift für Rechtspolitik (2002), S. 497-501.

43 | Vgl. BVerfGE 120, 274; kritisch zu der Entscheidung und ihrer dogmatischen Konstruktion siehe Pagenkopf: Kommentierung zu Art. 10 GG, Rn. 6; Wolfgang Hoffmann-Riem: »Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme«, in: Juristenzeitung (2008), S. 1009-1022.

44 | Vgl. BVerfGE 120, 274.

45 | Überblick vgl. Wolfgang Schulz: »Meinungs- und Informationsfreiheit«, in: Marian Paschke/Wolfgang Berlit/Claus Mayer (Hg.), Hamburger Kommentar zum gesamten Medienrecht, Baden-Baden: Nomos 2008, S. 130ff.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

informationelle Selbstbestimmung und wann es die Kommunikationsfreiheiten berührt.[46]

Was bei der Lektüre der Entscheidungen des Bundesverfassungsgerichts zu Art. 5 Abs. 1 GG sehr deutlich wird, ist die hohe Bedeutung, die das Bundesverfassungsgericht freier individueller und öffentlicher Meinungsbildung beimisst, und dies aus zwei Gründen: Zum einen geht das Gericht davon aus, dass die demokratische Selbstverständigung einer Gesellschaft auf freie Kommunikationsprozesse angewiesen ist. Zum anderen – dies scheint insbesondere bei Entscheidungen zur Informationsfreiheit auf – ist auch die Persönlichkeitsentwicklung in starker Weise vom kommunikativen Austausch abhängig; mit den Worten des Bundesverfassungsgerichts ist es ein elementares Bedürfnis des Menschen, sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten.[47]

Interessant für den vorliegenden Kontext ist insbesondere, dass das Bundesverfassungsgericht bei Eingriffen in die Kommunikationsfreiheit eine Verstärkung von objektiver Komponente und subjektiver Komponente des Grundrechts postuliert. Es geht davon aus, dass Eingriffe, die ein konkretes Kommunikat betreffen, überschießende Wirkungen für die öffentliche Kommunikation entfalten können, etwa wenn sie andere in ihrer Unbefangenheit zu kommunizieren beeinträchtigen.[48] In der amerikanischen Literatur wird dies auch unter dem Rubrum »Chilling Effect« diskutiert, also eine einschüchternde Wirkung, die von staatlichen Kommunikationskontrollmaßnahmen ausgehen kann. Aus diesem Grunde ist auch die Pflicht, ent-anonymisiert zu kommunizieren, eine Berührung des Schutzbereiches von Art. 5 Abs. 1 Satz 1, 1. Alt. GG.[49] Dies ungeachtet des Umstands, dass anonymer Kommunikation möglicherweise ein Glaubwürdigkeitsmangel anhaftet und sie auch dazu führt, dass soziale Kontrollen nicht greifen und dementsprechend das Risiko für die Rechtsgüter Dritter steigen kann. Letzteres ist bei Abwägungsentscheidungen zu berücksichtigen.

Was darüber hinaus an Maßnahmen der Kommunikationsüberwachung berufsmäßige Anbieter von Telekommunikationsdiensten oder von Telemedien in ihrer Berufsfreiheit nach Art. 12 Abs. 1 GG beeinträchtigen kann und – etwa wenn der Gewerbebetrieb in seiner Substanz betroffen ist – inwiefern auch die Eigentumsfreiheit nach Art. 14 Abs. 1 GG staatlichen Maßnahmen Grenzen setzt, kann hier nicht weiter erörtert werden, ist aber insbesondere bei der Frage relevant, inwieweit die Kosten

46 | Aktuell vgl. BGH, Multimedia und Recht (2009), S. 608-614.

47 | BVerfGE 27, 71 (81).

48 | Vgl. BVerfGE, in: Neue Juristische Wochenschrift (2006), S. 207-211.

49 | Vgl. Miriam Ballhausen/Jan Dirk Roggenkamp: »Personenbezogene Bewertungsplattformen«, in: Kommunikation & Recht (2008), S. 403-410, hier S. 406.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

für Überwachungsmaßnahmen den Unternehmen selber auferlegt werden können.[50]

19.10 Abwägungstopoi der Kommunikationskontrolle

Die verfassungsrechtlichen Grundsätze der Abwägung hat das Bundesverfassungsgericht in der Entscheidung zur vorbeugenden Telekommunikationsüberwachung sehr deutlich markiert:

»Je gewichtiger das gefährdete Rechtsgut ist und je weit reichender es durch die jeweiligen Handlungen beeinträchtigt würde oder beeinträchtigt worden ist, desto geringere Anforderungen dürfen an den Grad der Wahrscheinlichkeit gestellt werden, mit der auf eine drohende oder erfolgte Verletzung geschlossen werden kann, und desto weniger fundierend dürfen gegebenenfalls die Tatsachen sein, die auf die Gefährdung oder Verletzung des Rechtsguts schließen lassen.«[51]

Auf der Seite der Sicherheit, die durch Kommunikationskontrollmaßnahmen erhöht werden kann, ist daher genau zu differenzieren, welche Struktur die Gefahr hat, um deren Abwehr es geht, insbesondere ob es sich um abstrakte oder konkrete Gefährdungen handelt. Überwachungsmaßnahmen im Vorfeld von Gefährdungen sind nicht ausgeschlossen, aber im Hinblick auf Intensität und Wahrscheinlichkeit der Gefahren, die möglicherweise drohen, hohe Anforderungen zu stellen.

Differenzierungen sind insbesondere möglich und geboten im Hinblick auf die Rechtsgüter, um die es geht. Hier ergibt sich aus der Rechtsprechung des Bundesverfassungsgerichts, dass Leib, Leben und Freiheit von Personen sowie Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates berühren, bei einer entsprechenden Abwägung die weitest reichenden Eingriffe legitimieren.

Auf der anderen Seite haben die kurzen Ausführungen zur Kommunikationskontrolle gezeigt, dass Kommunikation gerade in der Wissensgesellschaft von elementarer Bedeutung für viele Lebensbereiche ist, so dass sich auch hier die Notwendigkeit von Differenzierungen ergibt. Es sind besonders schützenswerte Kommunikationssphären zu definieren; das Bundesverfassungsgericht hat in letzten Entscheidungen die Sphäre der »privaten Lebensgestaltung« als die definiert, die die eines gesteiger-

50 | Zu dieser Diskussion vgl. Christian von Hammerstein: »Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle«, in: Multimedia und Recht (2004), S. 222-227; Ernst Georg Berger: »Wer anschaffen will, muss auch zahlen«, in: Computer und Recht (2008), S. 557-560.

51 | BVerfGE 113, 348 (386).

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

ten Schutzes bedarf; inklusive ihrer Verlängerung in kommunikationstechnische Systeme.[52]

Schließlich ist zu bedenken, dass es bestimmte Kommunikatoren gibt, die eines besonderen Schutzes bedürfen, dazu gehören etwa Journalisten in Erfüllung ihrer öffentlichen Aufgabe. Die einfachgesetzlichen Grundlagen reagieren hier zum Teil mit gesteigerten Anforderungen; das System ist in dieser Hinsicht allerdings noch nicht konsistent.

Aus den Überlegungen des Bundesverfassungsgerichts zur einschüchternden Wirkung von Kommunikationskontrollmaßnahmen ist zu lernen, dass Rückwirkungen auf die freie individuelle und öffentliche Kommunikation besonderer verfassungsrechtlicher Betrachtung bedürfen. Im Hinblick auf die unterschiedlichen über IP-Netze verbreiteten Dienste bedarf es in Zukunft einer noch viel differenzierteren Betrachtung, welche Formen von Überwachungsmaßnahmen welche Effekte im Hinblick auf die Nutzung dieser Dienstangebote haben.

19.11 Schlussfolgerungen

Zunächst ist festzuhalten, dass Maßnahmen der Kommunikationskontrolle sich grundsätzlich im Schutzbereich von einem oder mehreren Grundrechten auswirken und insoweit die verfassungsrechtliche Begründungslast auf der Seite derer liegt, die durch Kommunikationskontrolle zur Verbesserung der Sicherheit beitragen wollen.

Das Bundesverfassungsgericht verlangt hier zu Recht eine Konkretisierung, nicht nur, um dem verfassungsrechtlichen Bestimmtheitsgebot aus Art. 20 Abs. 3 GG zu genügen, sondern auch, um dem Gericht die Grundlage für eine differenzierte Verhältnismäßigkeitsprüfung zur Verfügung zu stellen. Dazu gehört eine Konkretisierung der Gefährdungen und auch der Eignung der Maßnahmen.

Zu fordern ist aus einer verfassungsrechtlichen Perspektive auch, dass in diesem sensiblen Bereich klare Rechtsgrundlagen existieren, etwa die Gerichte nicht gezwungen sind, über gewundene Auslegungen das Abhören von E-Mails und die Überwachung von IP-Telefonie durchzusetzen.

Schließlich muss der Grundsatz gelten, dass Eingriffe bei Unbeteiligten zu minimieren sind. Wo besonders schützenswerte Kommunikationsbeziehungen existieren, ist ein konsistentes System gesteigerter Anforderungen zu entwickeln, etwa wenn es um Journalisten in Erfüllung ihrer öffentlichen Aufgabe geht. Dass letzteres angesichts von Entgrenzung des Journalismus und Funktionsverschiebungen im Bereich der Massenmedien zunehmend schwer fällt, kann von dieser Pflicht nicht entbinden.

52 | Vgl. BVerfGE 109, 279; 120, 274; BVerfGE, in: Neue Juristische Wochenschrift (2007), S. 2753-2757.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

Defizite werden mit Recht konstatiert, wenn es um die Frage von Transparenz und Evaluation von Maßnahmen geht.[53] Es ist nicht auszuschließen, dass auch Experten der Gefahrenabwehr der Vorstellung verfallen, neue technische Maßnahmen würden Probleme quasi von selbst lösen. Jedenfalls existieren sehr unterschiedliche Vorstellungen zur praktischen Bedeutung von technischen Maßnahmen wie etwa dem Ausspähen von Personal Computern durch Trojaner.[54]

Schließlich sind bei allen Maßnahmen strukturelle Folgen für die öffentliche Kommunikation im Auge zu behalten. Das Ausspielen von Freiheit gegen Sicherheit und umgekehrt ist wenig weiterführend. Eindeutig ist aber, dass ein Staat, der die Freiheit öffentlicher Kommunikation etwa durch Kontrollmechanismen untergräbt, die Basis seiner eigenen Akzeptanz gefährdet.

53 | Vgl. Hoffmann-Riem, in: ZRP 2002, S. 497-501.

54 | Vgl. zur Diskussion um die Effektivität Burkhard Hirsch: »Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme«, in: Neue Juristische Online Zeitschrift (2008), S. 1907-1915, hier: S. 1911.

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.14361/transcript.9783839414354.303 - am 14.02.2026, 16:01:49. https://www.inlibra.com/de/agb - Open Access -