GAZEAS NEPOMUCK | THEODOR-HEUSS-RING 34 | 50668 KÖLN

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

vorab per Telefax: 07 21 91 01-382 (ohne Anlagen)

Dr. Nikolaos Gazeas LL.M.
Rechtsanwalt

Dr. Lutz Nepomuck
Rechtsanwalt
Fachanwalt für Strafrecht

Dr. Andrej Umansky LL.M.
Rechtsanwalt

Köln, 14. Juli 2021

242/21 NG
NG/es

Verfassungsbeschwerde

1. des Herrn Christian Lindner, MdB, Platz der Republik 1, 11011 Berlin,
2. des Herrn Wolfgang Kubicki, MdB, Platz der Republik 1, 11011 Berlin,
3. des Herrn Dr. Hermann Otto Solms, MdB, Platz der Republik 1, 11011 Berlin,
4. des Herrn Dr. Marco Buschmann, MdB, Platz der Republik 1, 11011 Berlin,
5. der Frau Bettina Stark-Watzinger, MdB, Platz der Republik 1, 11011 Berlin,
6. des Herrn Dr. Florian Toncar, MdB, Platz der Republik 1, 11011 Berlin,
7. der Frau Katja Suding, MdB, Platz der Republik 1, 11011 Berlin,
8. des Herrn Michael Theurer, MdB, Platz der Republik 1, 11011 Berlin,
9. des Herrn Stephan Thomae, MdB, Platz der Republik 1, 11011 Berlin,
10. des Herrn Christian Dürr, MdB, Platz der Republik 1, 11011 Berlin,
11. des Herrn Frank Sitta, MdB, Platz der Republik 1, 11011 Berlin,
12. des Herrn Grigorios Aggelidis, MdB, Platz der Republik 1, 11011 Berlin,

13. der Frau Christine Aschenberg-Dugnus, MdB Platz der Republik 1, 11011 Berlin,
14. der Frau Nicole Bauer, MdB, Platz der Republik 1, 11011 Berlin,
15. des Herrn Jens Brandenburg, MdB, Platz der Republik 1, 11011 Berlin,
16. des Herrn Mario Brandenburg, MdB, Platz der Republik 1, 11011 Berlin,
17. der Frau Sandra Bubendorfer-Licht, MdB, Platz der Republik 1, 11011 Berlin,
18. des Herrn Karlheinz Busen, MdB, Platz der Republik 1, 11011 Berlin,
19. des Herrn Carl-Julius Cronenberg, MdB, Platz der Republik 1, 11011 Berlin,
20. des Herrn Bijan Djir-Sarai, MdB, Platz der Republik 1, 11011 Berlin,
21. des Herrn Marcus Faber, MdB, Platz der Republik 1, 11011 Berlin,
22. des Herrn Daniel Föst, MdB, Platz der Republik 1, 11011 Berlin,
23. des Herrn Dr. Christopher Gohl, MdB, Platz der Republik 1, 11011 Berlin,
24. des Herrn Thomas Hacker, MdB, Platz der Republik 1, 11011 Berlin,
25. des Herrn Reginald Hanke, MdB, Platz der Republik 1, 11011 Berlin,
26. des Herrn Peter Heidt, MdB, Platz der Republik 1, 11011 Berlin,
27. der Frau Katrin Helling-Plahr, MdB, Platz der Republik 1, 11011 Berlin,
28. des Herrn Torsten Herbst, MdB, Platz der Republik 1, 11011 Berlin,
29. der Frau Katja Hessel, MdB, Platz der Republik 1, 11011 Berlin,
30. des Herrn Gero Hocker, MdB, Platz der Republik 1, 11011 Berlin,
31. des Herrn Manuel Höferlin, MdB, Platz der Republik 1, 11011 Berlin,
32. des Herrn Christoph Hoffmann, MdB, Platz der Republik 1, 11011 Berlin,
33. des Herrn Reinhard Houben, MdB, Platz der Republik 1, 11011 Berlin,
34. der Frau Ulla Ihnen, MdB, Platz der Republik 1, 11011 Berlin,
35. des Herrn Olaf in der Beeck, MdB, Platz der Republik 1, 11011 Berlin,
36. der Frau Gyde Jensen, MdB, Platz der Republik 1, 11011 Berlin,
37. des Herrn Karsten Klein, MdB, Platz der Republik 1, 11011 Berlin,
38. der Frau Daniela Kluckert, MdB, Platz der Republik 1, 11011 Berlin,
39. des Herrn Dr. Lukas Köhler, MdB, Platz der Republik 1, 11011 Berlin,
40. der Frau Carina Konrad, MdB, Platz der Republik 1, 11011 Berlin,
41. des Herrn Konstantin Kuhle, MdB, Platz der Republik 1, 11011 Berlin,
42. des Herrn Alexander Kulitz, MdB, Platz der Republik 1, 11011 Berlin,
43. des Herrn Ulrich Werner Maria Lechte, MdB, Platz der Republik 1, 11011 Berlin,
44. des Herrn Michael Georg Link, MdB, Platz der Republik 1, 11011 Berlin,
45. des Herrn Oliver Luksic, MdB, Platz der Republik 1, 11011 Berlin,
46. des Herrn Till Mansmann, MdB, Platz der Republik 1, 11011 Berlin,
47. des Herrn Dr. Jürgen Martens, MdB, Platz der Republik 1, 11011 Berlin,
48. des Herrn Christoph Meyer, MdB, Platz der Republik 1, 11011 Berlin,
49. des Herrn Alexander Müller, MdB, Platz der Republik 1, 11011 Berlin,
50. des Herrn Roman Müller-Böhm, MdB, Platz der Republik 1, 11011 Berlin,
51. des Herrn Frank Müller-Rosentritt, MdB, Platz der Republik 1, 11011 Berlin,
52. des Herrn Prof. Martin Neumann, MdB, Platz der Republik 1, 11011 Berlin,

53. des Herrn Matthias Nölke, MdB, Platz der Republik 1, 11011 Berlin,
54. des Herrn Dr. Thomas Sattelberger, MdB, Platz der Republik 1, 11011 Berlin,
55. des Herrn Christian Sauter, MdB, Platz der Republik 1, 11011 Berlin,
56. des Herrn Frank Schäffler, MdB, Platz der Republik 1, 11011 Berlin,
57. der Frau Dr. Marie-Agnes Strack-Zimmermann, MdB, Platz der Republik 1, 11011 Berlin,
58. des Herrn Benjamin Strasser, MdB, Platz der Republik 1, 11011 Berlin,
59. der Frau Linda Teuteberg, MdB, Platz der Republik 1, 11011 Berlin,
60. des Herrn Prof. Dr. Andrew Ullmann, MdB, Platz der Republik 1, 11011 Berlin,
61. des Herrn Gerald Ullrich, MdB, Platz der Republik 1, 11011 Berlin,
62. des Herrn Johannes Vogel, MdB, Platz der Republik 1, 11011 Berlin,
63. der Frau Sandra Weeser, MdB, Platz der Republik 1, 11011 Berlin,
64. der Frau Katharina Willkomm, MdB, Platz der Republik 1, 11011 Berlin

– Beschwerdeführerinnen und Beschwerdeführer –

Die ladungsfähigen Privatanschriften der Beschwerdeführer, da sie auch als Bürgerinnen und Bürger diese Verfassungsbeschwerde erheben, sind als Anlage GN zusammengestellt mit der Bitte, sie vertraulich zu behandeln.

– Bevollmächtigter: Rechtsanwalt Dr. Nikolaos Gazeas LL.M.,
GAZEAS NEPOMUCK Rechtsanwälte PartG mbB
Theodor-Heuss-Ring 34
50668 Köln –

wegen: Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl. 2021 I, S. 2274).

Ich zeige an, dass mir die Beschwerdeführerinnen und Beschwerdeführer (im Folgenden: Beschwerdeführer) besondere Vollmacht für das Verfahren erteilt und mich mit der Wahrnehmung ihrer Interessen beauftragt haben. Die Vollmachten sind als Anlagen im Original beigefügt. Die Originale der Vollmachten der Beschwerdeführer zu 38) 54) und 59) werde ich kurzfristig nachreichen.

Namens und im Auftrag der Beschwerdeführer erhebe ich

V e r f a s s u n g s b e s c h w e r d e

gegen das Gesetz zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl. 2021 I, S. 2274) sowie das Artikel 10-Gesetz i.d.F. des Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl. 2021 I, S. 2274).

Die Verfassungsbeschwerde richtet sich gegen die gesetzlichen Neuregelungen zur sog. Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz (im Folgenden: G 10) sowie gegen damit zusammenhängende Verfahrensregelungen und Datenübermittlungsermächtigungen im G 10.

Angegriffen werden wegen Verfassungswidrigkeit folgende Normen:

- § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 i.V.m. § 11 Abs. 1a Satz 1,
- § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 i.V.m. § 11 Abs. 1a Satz 2,
- § 3 Abs. 2 Satz 2 i.V.m. § 11 Abs. 1a Satz 2,
- § 3a,
- § 4 Abs. 4,
- § 11 Abs. 1b Satz 1,
- § 12 Abs. 1 Satz 2, Satz 5,
- § 12 Abs. 1 Satz 2, Satz 5 i.V.m. § 12 Abs. 2 Satz 1,
- § 13 und
- § 15a

des G 10 i.d.F. des Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl. 2021 I, S. 2274).

Ich rüge die Verletzung der

- Art. 1 Abs. 1 GG
- Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG
- Art. 10 Abs. 1 GG
- Art. 12 Abs. 1 GG
- Art. 19 Abs. 4 GG
- Art. 38 Abs. 1 Satz 2 i.V.m. Art. 47 GG.

Ich beantrage,

1. **die § 11 Abs. 1a Satz 1 und 2, § 3a , § 4 Abs. 4, § 11 Abs. 1b Satz 1, § 12 Abs. 1 Satz 2, Satz 5, § 13 und § 15a des G 10 i.d.F. des Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl. 2021 I, S. 2274) für nichtig, hilfsweise für unvereinbar mit dem Grundgesetz zu erklären,**

2. **einen angemessenen Gegenstandswert festzusetzen.**

Der besseren Übersichtlichkeit wegen sei eine Gliederung der Verfassungsbeschwerde vorangestellt:

Begründung

A. Sachverhalt

I. Gegenstand der angegriffenen Regelungen

Die Verfassungsbeschwerde richtet sich im Kern gegen die gesetzliche Ermächtigung zur sog. Quellen-Telekommunikationsüberwachung im G 10 (§ 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 1 G 10, im Folgenden: *Quellen-TKÜ* genannt) sowie gegen die Ermächtigung zur Durchführung einer inhaltlich auf bestimmte Kommunikationsinhalte beschränkten Online-Durchsuchung (im Folgenden: *beschränkte Online-Durchsuchung*) (§ 3 Abs. 1 i.Vm. § 11 Abs. 1a Satz 2 G 10). In der öffentlichen Diskussion wird diese beschränkte Online-Durchsuchung (vornehmlich von ihren Befürwortern) – irreführend – als „Quellen-TKÜ plus" oder „erweiterte Quellen-TKÜ" bezeichnet. Angegriffen wird auch das Fehlen von verfassungsrechtlich gebotenen gesetzlichen Regelungen zum Umgang mit IT-Sicherheitslücken, mithin eine Verletzung von objektivrechtlichen Schutzpflichten aus dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

Angegriffen wird konkret die Eingriffsbefugnis zur Quellen-TKÜ in § 3 Abs. 1 i.V.m. § 11 Abs. 1a i.V.m. § 1 Abs. 1 Nr. 1 G 10 und die Eingriffsbefugnis zur beschränkten Online-Durchsuchung in derselben Norm (konkret § 11 Abs. 1a Satz 2 G 10), die durch Art. 5 des Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 eingefügt worden sind.

Angegriffen werden auch Regelungen des G 10-Gesetzes, die mit der Quellen-TKÜ und der beschränkten Online-Durchsuchung im Zusammenhang stehen und insbesondere die Voraussetzungen ihrer Anordnung regeln. Dies sind verschiedene Verfahrensregelungen bzw. verfahrensrechtliche Schutzvorkehrungen sowie Übermittlungsbefugnisse im G 10. Die Einführung der Quellen-TKÜ und der beschränkten Online-Durchsuchung in § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 gibt den nunmehr möglichen Individual-Überwachungsmaßnahmen (sog. „Beschränkungen in Einzelfällen") ein völlig neues Gesicht. Dies hat in der Folge auch Auswirkungen auf Verfahrensregelungen, verfahrensrechtliche Schutzvorkehrungen sowie auf die Übermittlungsvorschriften, die daher ebenso mit dieser Verfassungsbeschwerde angegriffen werden.

Angegriffen werden neben den Eingriffsbefugnissen insoweit namentlich, soweit sie sich auf diese Eingriffsbefugnisse beziehen:

- die Vorschrift zum Schutz des Kernbereichs privater Lebensgestaltung (§ 3a G 10), die Regelungen dahingehend vorsieht, wann Beschränkungen

in Einzelfällen unzulässig sind und wie mit Überwachungsmaßnahmen im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung umzugehen ist;

- die Vorschrift über Mitteilung an Betroffene, die sog. Benachrichtigungspflicht (§ 12 G 10), die Vorgaben dazu enthält wann dem Betroffenen Beschränkungsmaßnahmen nach § 3 G 10 nach ihrer Einstellung mitzuteilen sind und vor allem wann nicht;
- die Übermittlungsregelung in § 4 Abs. 4 G 10, die unter den dort genannten Voraussetzungen zur Übermittlung der aus einer Überwachungsmaßnahme gewonnenen Daten ermächtigt;
- die Regelung zur Beschränkung des Rechtsweges (§ 13 G 10), die bei Anordnungen von Beschränkungsmaßnahmen u.a. nach § 3 G 10 und deren Vollzug den Rechtsweg vor Mitteilung an den Betroffenen einschränkt.
- Die Regelung in § 15a G 10 ermöglicht im Falle der Annahme von Gefahr im Verzug die autarke Anordnung von Überwachungsmaßnahmen nach § 3 Abs. 1 G 10 durch den Nachrichtendienst selbst. Die Anordnung wird in diesen Fällen in verschiedenen Konstellationen ohne Einhaltung des üblichen Anordnungsweges, wie er in § 10 G 10 vorgesehen ist, gestattet.

Die Beschwerdeführer greifen als Mitglieder des Deutschen Bundestages sowie als Bürgerinnen und Bürger auch im Wege der Rüge einer objektiv-rechtlichen Schutzpflichtverletzung des Rechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

II. Die Beschwerdeführer

Die Beschwerdeführer sind Mitglieder des 19. Deutschen Bundestages und dort in verschiedenen Funktionen tätig. Sie erheben die Beschwerde daher zum einen als Abgeordnete des Deutschen Bundestages, weil die angegriffenen Regelungen die Vertraulichkeit der Kommunikation von ihnen als Abgeordneten mit Dritten verletzen. Zum anderen rügen sie aber auch die Verletzung ihrer Grundrechte, weil die angegriffenen Regelungen sie nicht nur als Abgeordnete, sondern auch als Bürgerinnen und Bürger, teilweise auch im Rahmen ihrer Berufsausübung berühren. In diesem Zusammenhang machen sie auch die Verletzung einer staatlichen Schutzpflicht zur Sicherung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“) geltend.

B. Zulässigkeit der Verfassungsbeschwerde

I. Beschwerdefähigkeit

Gemäß Art. 93 Abs. 1 Nr. 4a GG kann die Verfassungsbeschwerde von jedermann eingelegt werden. Jedermann ist jeder, der Träger von Grundrechten sein kann.

1. Statthaftigkeit der Verfassungsbeschwerde im Lichte der Abgeordnetenstellung der Beschwerdeführer

Abgeordnete können sich grundsätzlich nicht auf die Grundrechte berufen, soweit sie allein in ihrer Funktion als Abgeordneter betroffen sind. Gerade im Hinblick auf den Schutz ihrer Privatsphäre hat das Gericht dies aber bisher ausdrücklich nicht ausgeschlossen.[1] Vor Eingriffen in die Vertraulichkeit der Kommunikation mit ihnen als Abgeordnete, wie sie die Beschwerdeführer hier geltend machen, schützt sie aber in jedem Falle Art. 38 Abs. 1 Satz 2 i.V.m. Art. 47 Satz 2 GG, soweit sie im Rahmen ihrer Abgeordnetentätigkeit handeln. Auch wenn es sich dabei um kein Grundrecht oder grundrechtsgleiches Recht handelt, ist nach der Rechtsprechung des angerufenen Gerichts gegen solche Eingriffe die Verfassungsbeschwerde statthaft.[2] Es will so eine schlechtere Behandlung von Abgeordneten im Vergleich zu anderen Grundrechtsträgern verhindern.[3] Zudem stellt, so das angerufene Gericht, ein Organstreitverfahren keine ebenso effektive Alternative zur Durchsetzung der Rechte der Abgeordneten dar,[4] weil die angegriffenen Regelungen im Organstreitverfahren nicht aufgehoben werden können.[5]

Die angegriffenen Regelungen greifen in die Gewährleistung des freien Mandats nach Art. 38 Abs. 1 Satz 2 GG ein. Dieses umfasst auch eine „die freie, von staatlicher Beeinflussung unberührte Kommunikationsbeziehung des Abgeordneten mit den Wählerinnen und Wählern“.[6] Danach ist bereits die Sammlung öffentlich verfügbarer Informationen ein Eingriff in das freie Mandat.[7] Dies muss erst recht gelten, wenn Inhalte der Kommunikation zwischen einem Abgeordneten und Wählerinnen und Wählern oder anderen Kommunikationspartnern heimlich erhoben werden. Verstärkt wird diese Vertrauensbeziehung durch Art. 47 GG, der dem Abgeordneten für Informationen ein Zeugnisverweigerungsrecht zubilligt, die ihm als

---

1 BVerfGE 118, 277, 320; 99, 19, 29.
2 BVerfGE 108, 251, 266 ff.
3 BVerfGE 108, 251, 267.
4 BVerfGE 108, 251, 268.
5 BVerfGE 24, 300, 351 f.
6 BVerfGE 134, 141, 178.
7 BVerfGE 134, 141, 178.

Abgeordneter anvertraut worden sind, und überlassene Schriftstücke insoweit einem Beschlagnahmeverbot unterwirft.[8] Diese Vertraulichkeit zwischen einem Abgeordneten und einer Person, die sich ihm anvertraut, wird durch eine tatsächliche oder auch nur vermutete heimliche Überwachung dieser Kommunikation erheblich beeinträchtigt. Letztlich kann es danach keinen Unterschied machen, ob staatliche Stellen Unterlagen, die einem Abgeordneten überlassen und ausgedruckt worden sind, im Rahmen einer Durchsuchung als Schriftstücke beschlagnahmen oder ob sie diese Informationen während oder nach der Kommunikation mittels heimlichen Zugriffs auf ein informationstechnisches System erlangen.[9]

2. Beschwerdeführer als Grundrechtsträger

Soweit die angegriffenen Regelungen oder auf ihrer Grundlage ergriffene Maßnahmen die Beschwerdeführer nicht nur in ihrer Funktion als Abgeordnete betreffen, können sie sich auf ihre Grundrechte berufen und sind damit als natürliche Personen, die in der Bundesrepublik Deutschland leben, auch in dieser Hinsicht nach § 90 Abs. 1 BVerfGG beschwerdefähig.

II. Beschwerdegegenstand

Die Verfassungsbeschwerde kann gem. Art. 93 Abs. 1 Nr. 4 lit. a GG gegen Akte der öffentlichen Gewalt eingelegt werden. Die mit dieser Verfassungsbeschwerde angegriffenen Regelungen sind als Parlamentsgesetz, das vom Deutschen Bundestag verabschiedet worden ist, ein Akt der öffentlichen Gewalt. Ein statthafter Beschwerdegegenstand liegt damit vor.

Die Verfassungsbeschwerde ist hinsichtlich aller Beschwerdeführer auch insoweit zulässig, als sie sich bezüglich der Regelungen der Quellen-TKÜ (nur) auf die Verletzung einer Schutzpflicht berufen, die aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme i.S.d. Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG folgt.

Gem. §§ 92, 95 Abs. 1 BVerfGG können auch Unterlassungen der öffentlichen Gewalt mit der Verfassungsbeschwerde gerügt werden. Dies gilt auch für die Verletzung grundrechtlicher Schutzpflichten.[10]

---

8 BVerfGE 108, 251, 286 f.

9 Angedeutet in BVerfGE 129, 208, 265. Für die Ausdehnung des Art. 47 Satz 2 GG auf funktionale Äquivalente einer Beschlagnahme wie Überwachungsmaßnahmen *Schulze-Fielitz*, in: Dreier, GG, 3. Aufl. 2015, Art. 47 Rn. 14; *Trute*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 47 Rn. 15; *Klein*, in: Maunz/Dürig, GG, 93. EL Oktober 2020, Art. 47 Rn. 31 m.w.N.

10 BVerfGE 77, 170, 214.

III. Beschwerdebefugnis im Allgemeinen

Die Beschwerdeführer sind beschwerdebefugt im Sinne von § 90 Abs. 1 BVerfGG.

Sie sind durch die angegriffenen Vorschriften selbst, gegenwärtig und unmittelbar in ihren Rechten aus Art. 38 Abs. 1 Satz 2 i.V.m. Art. 47 Satz 2 GG sowie ihren Grundrechten aus Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 12 Abs. 1 sowie Art. 19 Abs. 4 GG betroffen. Es ist zumindest möglich, dass Überwachungsmaßnahmen nach dem G 10 (Beschränkungen im Einzelfall nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10) sowie eine unterbleibende Benachrichtigung darüber, eine Übermittlung der aus einer solchen Maßnahme gewonnen Erkenntnisse sowie der gerügte unzureichende Schutz des Kernbereichs privater Lebensgestaltung sowie des Schutzes der Beschwerdeführer als zeugnisverweigerungsberechtigte Personen auf Grundlage der angegriffenen Regelungen den verfassungsmäßigen Schutz der Beschwerdeführer als Abgeordnete oder ihre Grundrechte verletzen.

1. Unmittelbare Betroffenheit

Die Beschwerdeführer sind durch die angegriffenen Vorschriften unmittelbar betroffen.

a. Heimlichkeit der Maßnahme

Zwar bedürfen diese Vorschriften generell einer Umsetzung durch weitere Vollzugsakte. Eine unmittelbare Betroffenheit durch ein Gesetz ist jedoch auch dann zu bejahen, wenn der potenziell Betroffene den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhält. In solchen Fällen steht ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu.[11]

Bei der Überwachung der Telekommunikation nach dem G 10 im Wege von Beschränkungen in Einzelfällen (§ 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10) handelt es sich um eine Maßnahme, von der der Betroffene weder vor noch während ihrer Durchführung etwas erfährt, sodass fachgerichtlicher Rechtsschutz nicht in Anspruch genommen werden kann.

b. Keine nachträgliche Benachrichtigung gewährleistet

Hieran ändern auch die Pflicht zur Mitteilung von Beschränkungen nach § 12 Abs. 1 Satz 1 G 10 nichts, weil sie weite Ausnahmen vorsieht (aa.) und

---

11 BVerfGE 67, 157, 169 f.; 100, 313, 354; 109, 279, 306 f.; 113, 348, 362 f.

möglicherweise Drittbetroffene in der Praxis gar nicht erfasst (bb.). Auch die Möglichkeit zur Erhebung einer Beschwerde an die G 10-Kommission nach § 15 Abs. 5 S. 1 G 10 ändert hieran nichts (cc.).

aa. Ausnahmen von der Benachrichtigungspflicht nach § 12 G 10-Gesetz

Die Erhebung einer Verfassungsbeschwerde unmittelbar gegen das Gesetz ist nicht nur dann zulässig, wenn nach der gesetzlichen Regelung die Betroffenen zu keinem Zeitpunkt Kenntnis von einem heimlichen Vollzugsakt erhalten, sondern darüber hinaus auch dann, wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber auf Grund weit reichender Ausnahmetatbestände auch langfristig abgesehen werden kann.[12] Unter diesen Umständen ist ebenfalls nicht gewährleistet, dass der Betroffene effektiven fachgerichtlichen Rechtsschutz erlangen kann.[13]

So verhält es sich hier. Die Ausnahmen von der grundsätzlich bestehenden Benachrichtigungspflicht sind im Ergebnis derart weitgehend, dass von ihr letztlich nur sehr wenig übrigbleibt oder sie erst mit erheblicher Verzögerung greift.

Es ist nicht nur so, dass von der grundsätzlich bestehenden Benachrichtigungspflicht nach § 12 Abs. 1 Satz 1 G 10 durch sehr weitreichende Ausnahmetatbestände abgesehen werden *kann*. Vielmehr *muss* weitgehend sogar zwingend von einer Benachrichtigung abgesehen werden.

So unterbleibt nach § 12 Abs. 1 Satz 2 G 10 die Benachrichtigung – zwingend – „solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist“. Diese Voraussetzungen sind extrem weit. So ist es nicht erforderlich für eine Zurückstellung der Benachrichtigung positiv das Vorliegen einer Gefährdung des Zwecks der Beschränkung festzustellen, sondern nur, dass diese Gefährdung nicht auszuschließen ist. Die Voraussetzungen für ein Zurückstellung der Benachrichtigung liegen zudem gerade im Falle der Nachrichtendienste aufgrund ihrer Tätigkeit häufig vor.[14] Ihre Maßnahmen zur Informationserhebung, auch nach § 3 Abs. 1 G 10, greifen bereits weit im Vorfeld einer Gefahr und richten sich gegen Organisationen und Strukturen. Dies zeigt auch § 3 Abs. 1 Satz 2 G 10, der Beschränkungen gegen eine Person allein aufgrund ihrer Mitgliedschaft in einer dort genannten Organisation zulässt. Eine Mitteilung gegenüber einem Betroffenen könnte

12 BVerfGE 109, 279, 307; zuletzt BVerfGE 154, 152, 209; 150, 309, 324.
13 BVerfGE 109, 279, 307.
14 Zu möglichen Ausschlussgründen in der Praxis *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Nachrichtendienstrechts, 2017, Kap. VI § 4 Rn. 80 ff.

dann die weitere Beobachtung der Organisation erschweren, weil andere Mitglieder gewarnt werden würden.

Nicht auszuschließen ist zudem speziell im Hinblick auf Beschränkungen, welche die Infiltration informationstechnischer Systeme voraussetzen, das Argument der Gefährdung des Wohles des Bundes oder der Länder, weil durch die Mitteilung Methoden der staatlichen Überwachung offengelegt werden könnten. Folgen wären, so ließe sich argumentieren, wiederum Gegenmaßnahmen der Personen, die zukünftig damit rechnen, nachrichtendienstlich überwacht zu werden. Die Gründe für eine Zurückstellung der Mitteilung sind extrem auslegungsbedürftig und teilweise auch von ermittlungstaktischen Überlegungen der zuständigen Behörden sowie der G 10-Kommission abhängig. Ihnen kommt daher ein großer Auslegungs- und Beurteilungsspielraum zu,[15] was aus Sicht der Beschwerdeführer noch einmal die Unsicherheit erhöht, ob sie von einer Beschränkung nach § 3 Abs. 1 G 10 nachträglich erfahren würden.

Auch ein endgültiges Absehen von einer Benachrichtigung ist nach § 12 Abs. 1 Satz 4 und 5 G 10 vorgesehen.

bb. Pflicht zur Benachrichtigung von Nebenbetroffenen

Es ist zudem nicht eindeutig, ob die Pflicht zur Benachrichtigung auch Nebenbetroffene erfasst, z.B. Kommunikationspartner der Person, gegen die sich die Beschränkung nach § 3 Abs. 1 G 10 unmittelbar richtet. Gerade aus Sicht der Beschwerdeführer ist diese Konstellation von besonderer Relevanz, weil sie mit großer Wahrscheinlichkeit gerade als Kommunikationspartner und nicht als Zielperson betroffen sind. § 12 Abs. 1 G 10 enthält hierzu keine Regelung, was in der Literatur zurecht kritisiert wird.[16] Vergleichbare Regelungen über die Benachrichtigung von Personen, die heimlich überwacht worden sind, wie sie z.B. § 101 Abs. 4 bis 6 StPO enthalten, fehlen und können aufgrund der Wesentlichkeit der Entscheidung für die Möglichkeit, Rechtsschutz zu suchen, auch nicht im Wege der Auslegung erlangt werden.[17] Dies könnte als umfassende Pflicht zur Benachrichtigung verstanden werden. In der Praxis ist aber davon auszugehen, dass eine ganz überwiegende Zahl der sog. Nebenbetroffenen nicht

---

15 Vgl. zur „Beurteilungsermächtigung“ der G 10-Kommission BVerwG, Urteil vom 23. Januar 2008 – 6 A 1/079, Rn. 42 ff.

16 *Roggan*, in: NOMOS-G 10, 2018, § 12 Rn. 3; *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 12 Rn. 11 f.

17 So aber offenbar *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Nachrichtendienstrechts, 2017, Kap. VI § 4 Rn. 85.

benachrichtigt werden.[18] Denn in weitem Umfang werden noch nicht einmal konkrete Zielpersonen endgültig benachrichtigt.[19]

cc. Beschwerde an die G 10-Kommission

Die Beschwerdeführer können auch nicht Kenntnis darüber erlangen, ob sie von einer Beschränkung nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 geworden sind, indem sie eine Beschwerde an die G 10-Kommission nach § 15 Abs. 5 Satz 1 G 10 erheben. Liegen die Gründe für einen Ausschluss einer Mitteilung nach § 12 Abs. 1 G 10 vor, schlagen diese auch auf die Beschwerde durch.[20] Die Beschwerdeführer würden nur eine allgemein gehaltene Nachricht erhalten, dass die G 10-Kommission keinen Verstoß gegen Art. 10 Abs. 1 GG habe feststellen können.[21]

2. Eigene und gegenwärtige Betroffenheit

a. Zur eigenen und gegenwärtigen Betroffenheit im Allgemeinen

Die Beschwerdeführer sind durch die angegriffenen Vorschriften auch selbst und gegenwärtig betroffen. Erforderlich, aber auch ausreichend ist hierfür bei gesetzlichen Ermächtigungen zu verdeckten Überwachungsmaßnahmen die Darlegung, zukünftig mit einiger Wahrscheinlichkeit von einer solchen Maßnahme betroffen und dadurch in seinen Grundrechten berührt zu sein.[22] Der geforderte Grad der Wahrscheinlichkeit wird davon beeinflusst, welche Möglichkeit der Beschwerdeführer hat, seine Betroffenheit darzulegen.[23] So ist bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann.[24] Dies hat das Gericht bereits für die Telekommunikationsüberwachung zu präventiven Zwecken anerkannt:

> „Die Möglichkeit, Objekt einer Maßnahme der Telekommunikationsüberwachung aufgrund der angegriffenen Regelung zu werden, besteht praktisch für jedermann. Sie kann nicht nur den möglichen Straftäter selbst oder dessen Kontakt- und Begleitpersonen erfassen, sondern auch Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen in Verbindung stehen.“[25]

---

18 S. nur *Roggan*, in: NOMOS-G 10, 2018, § 12 Rn. 3.

19 S. nur *Roggan*, in: NOMOS-G 10, 2018, § 12 Rn. 14 m.w.N. zu den Zahlen aus Berichten des PKGr.

20 Vgl. zum ähnlich gelagerten Auskunftsanspruch BVerfGE 154, 152, 209 f.

21 *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 15 Rn. 40.

22 BVerfGE 67, 157, 169 f.; 100, 313, 354; 109, 279, 307 f.

23 BVerfGE 100, 313, 355 f.; 109, 279, 308.

24 BVerfGE 109, 279, 308.

25 BVerfGE 113, 348, 363.

Zudem liegt eine Betroffenheit jedenfalls für mögliche Eingriffsmaßnahmen außerhalb der Reichweite des Berufsgeheimnisses und dessen Schutz vor. So berechtigt etwa das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Satz 1 Nr. 4 StPO, auf das die Beschwerdeführer sich i.V.m. § 3b Abs. 1 und 2 G 10 für ein Erhebungs- und Verwertungsverbot stützen können, lediglich zur Verweigerung des Zeugnisses über Personen, die Abgeordneten in „ihrer Eigenschaft als" Mitglieder des Deutschen Bundestages kontaktieren „oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben, sowie über diese Tatsachen selbst."

Einer Betroffenheit der Beschwerdeführer steht auch nicht entgegen, dass die Beschränkungen sich nach § 3 Abs. 2 Satz 4 G 10 nicht auf „Abgeordnetenpost" beziehen dürfen. Telekommunikation ist hiervon nicht erfasst.[36]

3. Konkretere Darlegung nicht möglich

Eine noch konkretere Darlegung ihrer voraussichtlichen Betroffenheit ist den Beschwerdeführern nicht möglich. Zum einen haben sie – wie dargelegt – von konkreten Beschränkungen, die sie betreffen, keine positive Kenntnis. Zum anderen würden konkretere Informationen über ihre Kommunikationspartner und die Situation, die Anlass für eine Beschränkung nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 sein könnten, die Vertraulichkeit der Kommunikation mit ihnen als Abgeordnete gefährden. Würden die Beschwerdeführer etwa darlegen, wer sich an sie zu welchem Thema mit vertraulichen Informationen gewandt hat, würde dies nicht nur die verfassungsrechtlich gewährleistete Vertraulichkeit dieser Kommunikation empfindlich beeinträchtigen, sondern für die Kommunikationspartner auch das Risiko von Folgemaßnahmen[37] begründen. Zudem hätte dies für zukünftige Kommunikationspartner eine abschreckende Wirkung.

Sollte das Gericht dennoch weitere Informationen zur Betroffenheit der Beschwerdeführer benötigen, bitte ich um einen entsprechenden Hinweis.

IV. Beschwerdebefugnis hinsichtlich der Schutzpflichtverletzung

Die Beschwerdeführer sind auch hinsichtlich der gerügten Schutzpflichtverletzung aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme i.S.d.

---

36 *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 3 Rn. 40; *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Nachrichtendienstrechts, 2017, Kap. VI § 4 Rn. 50.

37 Vgl. zu diesem Kriterium BVerfGE 154, 152, 210.

Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG beschwerdebefugt; auch die Übrigen Zulässigkeitsvoraussetzungen sind insoweit gegeben.

Gem. §§ 92, 95 Abs. 1 BVerfGG können auch Unterlassungen der öffentlichen Gewalt mit der Verfassungsbeschwerde gerügt werden. Dies gilt auch für die Verletzung grundrechtlicher Schutzpflichten.[38]

1. Möglichkeit einer Grundrechtsverletzung

Der Gesetzgeber hat durch die Einführung der (bereits einfachen) Quellen-TKÜ für die Nachrichtendienste Anreize geschaffen, sich Sicherheitslücken in IT-Systemen zu verschaffen, die dem Hersteller des Systems (noch) unbekannt sind. Gleichzeitig bestehen keine gesetzlichen Regelungen, wie die Nachrichtendienste und andere Behörden, welche im Bund und in den Ländern die Befugnis zur Durchführung einer Quellen-TKÜ oder Online-Durchsuchung haben, mit der Kenntnis dieser besonders gefährlichen Kategorie von Sicherheitslücken umzugehen haben (sog. Schwachstellenmanagement). Hierdurch werden die Beschwerdeführer in einem aus dem IT-Grundrecht folgenden Anspruch gegenüber dem Staat verletzt, ein verfassungsrechtliches Mindestmaß an IT-Sicherheit zu schaffen und sich schützend vor die IT-Sicherheit in der Bundesrepublik zu stellen.

Es entspricht ständiger Rechtsprechung des angerufen Gerichts, dass die Grundrechte nicht lediglich subjektive Abwehrrechte des Einzelnen gegen die staatliche Gewalt enthalten, sondern diese zugleich objektivrechtliche Wertentscheidungen darstellen, aus der sich Richtlinien auch für die Gesetzgebung ergeben. Die Existenz und der Umfang solcher Schutzpflichten hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen ab.[39] Für das IT-Grundrecht ergibt sich diese Schutzpflicht vor dem Hintergrund der enormen Bedeutung informationstechnischer Systeme in allen Bereichen des heutigen (nicht nur Wirtschafts-)Lebens sowie aus den erheblichen und allgegenwärtigen Gefahren, die Cyberangriffe für nahezu alle verfassungsrechtlich geschützten Rechtsgüter – bis hin zum Rechtsgut Leben – mit sich bringen.

Die Beschwerdeführer verkennen dabei in ihrem Vortrag nicht, dass dem Gesetzgeber bei der Ausgestaltung der Schutzpflicht ein sehr weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum zukommt, der auch Raum lässt, konkurrierende öffentliche und private Interessen zu berücksichtigen. Dieser Spielraum ist jedoch dort überschritten, wo der Gesetzgeber gänzlich

38 BVerfGE 77, 170, 214.
39 BVerfGE 49, 89, 142.

ungeeignete oder völlig unzulängliche Vorkehrungen zum Schutz des Grundrechtes trifft[40] – oder gar keine.

So liegt es hier. Mit den Regelungen zur Quellen-TKÜ und Online-Durchsuchung schafft der Gesetzgeber bewusst einen Anreiz für die Nachrichtendienste und andere Sicherheitsbehörden, sich Kenntnis von Sicherheitslücken zu verschaffen, die den Herstellern der betreffenden IT-Geräte unbekannt sind.

Grundsätzlich muss für die Durchführung der Quellen-TKÜ eine Spähsoftware auf dem IT-System der Zielperson installiert werden. Unabhängig von der Art der Installation der konkreten Spähsoftware, muss diese regelmäßig Sicherheitslücken im IT-System der Zielperson ausnutzen. Dies liegt darin begründet, dass das zu überwachende IT-System gewöhnlich vom Hersteller mit Schutzmaßnahmen gegen Überwachung ausgestattet ist. Diese Schutzmechanismen bestehen dabei hauptsächlich, um Angriffe krimineller Dritter abzuhalten. Sie müssen jedoch auch von staatlicher Spähsoftware überwunden werden, da sog. Hintertüren für staatliche Überwachungsmaßnahmen (engl. *Backdoors*) nach Kenntnis der Beschwerdeführer nicht „von Werk aus" existieren.

Dabei besteht für Sicherheitsbehörden, die das Instrument der Quellen-TKÜ einsetzen wollen, ein besonderer Anreiz, auf Sicherheitslücken zurückzugreifen, die dem Hersteller der betreffenden Geräte unbekannt sind. Zum einem ist so sichergestellt, dass die Sicherheitslücke im System der Zielperson noch nicht (etwa durch ein Update des Herstellers in der Betriebssoftware) geschlossen ist und der Angriff somit in jedem Falle erfolgreich ist. Zum anderen besteht nicht das Risiko, dass die Sicherheitslücke im Laufe einer Überwachungsmaßnahme geschlossen wird und die heimliche Überwachung dann in dieser Weise nicht mehr weiter durchgeführt werden kann.

Diese Sicherheitslücken werden *Zero-Day*-Sicherheitslücken genannt, weil sie ausgenutzt werden, bevor der Hersteller des IT-Systems von ihnen Kenntnis erlangt. Es besteht also keine Zeit – nicht einen Tag (= *zero days*) – die Sicherheitslücke vor ihrer Ausnutzung zu schließen. Dass diese Sicherheitslücken nicht nur für Nachrichtendienste, sondern auch für sonstige Dritte besonders interessant für Cyber-Angriffe sind, liegt auf der Hand. Dies haben eine Vielzahl von Fällen auch in der jüngeren Vergangenheit – nicht nur im Ausland, sondern auch in der Bundesrepublik – gezeigt. Die spezifische Gefährlichkeit von *Zero-Day*-Sicherheitslücken ist dabei vergleichbar mit einer im Zeitpunkt des Ausbruchs unbekannten Krankheit, für die dementsprechend oftmals noch keine Behandlungsmethode und kein Impfstoff vorliegen wird.

---

40 BVerfGE 77, 170, 215.

Durch die Schaffung von Ermächtigungsgrundlagen zur Quellen-TKÜ und damit zum Einsatz des Staatstrojaners werden die Sicherheitsbehörden geradezu herausgefordert, sich ein Arsenal an (i.d.R. besonders gefährlichen) *Zero-Day*-Sicherheitslücken zu verschaffen, um überhaupt in der Lage zu sein, eine Quellen-TKÜ oder Online-Durchsuchung durchführen zu können. Dennoch hat der Gesetzgeber es unterlassen, sowohl in dem angegriffenen Gesetz als auch in irgendeinem anderen Gesetz Regelungen dazu zu treffen, wie mit der staatlichen Kenntnis dieser Sicherheitslücken im Lichte des Risikos für die Allgemeinheit umzugehen ist. Vielmehr existieren hierzu keinerlei gesetzliche Vorgaben des Gesetzgebers. Im absoluten Mindestmaß müsste der Gesetzgeber Regelungen sowie Abwägungskriterien zum Umgang mit der staatlichen Kenntnis von *Zero-Day*-Sicherheitslücken definieren. Dies ist nicht geschehen – auch nicht im Rahmen der Novellierung des IT-Sicherheitsgesetzes 2.0. Vielmehr ist die einzige bestehende gesetzliche Unterrichtungspflicht im Hinblick auf IT-Sicherheitslücken aus § 4 Abs. 3 BSIG auf Grund der Ausnahme in § 4 Abs. 4 Var. 1 BSIG („Regelungen zum Geheimschutz“) von vornherein nicht anwendbar. Somit bestehen in dieser Hinsicht nicht nur ungeeignete oder völlig unzulängliche, sondern gar keine Vorkehrungen zum Schutz des IT-Grundrechts.[41]

In diesem Unterlassen liegt die Verletzung der aus dem IT-Grundrecht folgenden Schutzpflicht für den Staat, sich schützend vor die IT-Sicherheit in der Bundesrepublik zu stellen.

Werden aus einem Grundrecht folgende Schutzpflichten verletzt, so liegt darin eine Verletzung des Grundrechts selbst, gegen die sich der Betroffene mit der Verfassungsbeschwerde zur Wehr setzen kann.[42]

2. Eigene, gegenwärtige und unmittelbare Beschwer

Das Unterlassen der Regelung eines geeigneten Schwachstellenmanagements betrifft die Beschwerdeführer selbst, gegenwärtig und unmittelbar.

a. Eigene Beschwer

Durch die Verletzung der aus dem IT-Grundrecht folgenden Schutzpflicht sind die Beschwerdeführer selbst betroffen.

---

41 S. zur hier vorliegenden Möglichkeit einer Grundrechtsverletzung ergänzend auch die Ausführungen unter C. III. weiter unten, die vorsorglich auch zum Gegenstand des Vortrags zur Zulässigkeit gemacht werden.

42 BVerfG, Beschluss vom 24. März 2021 – 1 BvR 2656/18, Rn. 145; BVerfGE 77, 170, 214; 77, 381, 402 f.; 79, 174, 201 f.; 125, 30, 78.

Dies ergibt sich bereits aus dem Umstand, dass alle Beschwerdeführer in nahezu allen Lebensbereichen IT-Systeme nutzen. Daher sind sie auf deren Integrität und Vertraulichkeit angewiesen. Der Umstand, dass hiernach der weit überwiegende Teil der Bundesbürger von der Schutzpflichtverletzung ebenso selbst betroffen ist wie die Beschwerdeführer, steht deren eigener Betroffenheit nicht entgegen. Dies ist vielmehr ein logisch zwingender Ausfluss aus der allgegenwärtigen Bedeutung informationstechnischer Systeme in allen Gesellschaftsbereichen. Es handelt sich demnach nicht um eine unzulässige Popularverfassungsbeschwerde. Wie das angerufene Gericht erst kürzlich festgestellt hat, wird eine über die bloße eigene Betroffenheit hinausgehende besondere Betroffenheit, die die Beschwerdeführer von der Allgemeinheit abheben würde, regelmäßig nicht verlangt.[43]

Ungeachtet dessen ergibt sich jedoch für die Beschwerdeführer eine gegenüber der „Normalnutzer" informationstechnischer Systeme herausgehobene individuelle Betroffenheit. Alle Beschwerdeführer sind als Mitglieder des Deutschen Bundestages herausgehobene Ziele für Cyberangriffe. Dabei sind sie – wie die Vergangenheit gezeigt hat – auch einer erhöhten Qualität und Quantität von Angriffen ausgesetzt, die stellenweise von ausländischen Geheimdiensten ausgeführt werden.[44] Dabei werden die Beschwerdeführer auch in der Ausübung ihres verfassungsrechtlich gem. Art. 38 Abs. 1 Satz 2 GG garantierten freien Mandats beeinträchtigt. Denn sie üben ihr Mandat in der konstanten Gefahr aus, dass über IT-Systeme vorgenommene Kommunikation oder auf diesen gespeicherten Daten abgehört bzw. ausgespäht wird.

Darüber hinaus besteht für alle Beschwerdeführer das Risiko, dass im Rahmen eines Cyberangriffs nicht für die Öffentlichkeit bestimmte Daten gestohlen werden, die für „Schmutzkampagnen" bis hin zu Erpressungsversuchen missbraucht werden können. Dass es sich hierbei um kein abstraktes Drohszenario handelt, zeigen die Erfahrungen anderer Länder, wobei die Cyberangriffe auf den Server der Demokratischen Partei (DNC) und den Rechner von Clinton-Kampagnenchef *John Podesta* 2016 in den USA und die *Macron*-Kampagne zwei Tage vor der Stichwahl der französischen Präsidentschaftswahl 2017 die bislang prominentesten Beispiele sein dürften. In beiden Fällen wurden danach vertrauliche Informationen veröffentlicht, im Falle der Macron-Kampagne sogar gemischt mit falschen Informationen. Ein erhöhtes Risiko besteht für weite Teile der Beschwerdeführer, die nicht nur als Mitglieder des Bundestages, sondern auch als herausgehobene Personen des öffentlichen Lebens besonders „attraktive" Ziele für Hackerangriffe sind. Dies

---

43 BVerfG, Beschluss vom 24. März 2021 – 1 BvR 2656/18, Rn. 110.

44 S. SPIEGEL online, Deutsche Ermittler fahnden nach Putins Tophacker, abrufbar unter https://www.spiegel.de/politik/deutschland/bundestag-angegriffen-deutsche-ermittler-fahnden-nach-putins-top-hacker-a-abdc9c2f-697d-461f-bfcd-b5a054a509bd, zuletzt abgerufen am 8. Juli 2021.

demonstrierte auch die Veröffentlichung teilweise sensibler personenbezogener Daten (*Doxing*) von Politikern um den Jahreswechsel 2018/2019.[45]

b. Gegenwärtige Beschwer

Die Beschwerdeführer sind von der Schutzpflichtverletzung auch gegenwärtig betroffen. Dies bereits, soweit die Beschwerdeführer nur als gewöhnliche Nutzer von IT-Systemen betroffen sind. Dabei ist die Besonderheit der hier gegenständlichen Zero-Day-Schwachstellen zu beachten, die per Definition erst bekannt werden, wenn es bereits zu spät ist.

Ausweislich des zuständigen Bundesamtes für Sicherheit in der Informationstechnik (BSI) besteht in Deutschland eine allgegenwärtige Bedrohungslage für die IT-Sicherheit:

> „Die Gefährdungslage der IT-Sicherheit bleibt in diesem Zeitraum angespannt. Dabei konnte eine Fortsetzung des Trends beobachtet werden, dass Angreifer Schadprogramme für cyber-kriminelle Massenangriffe auf Privatpersonen, Unternehmen und andere Institutionen nutzen. Auch Abflüsse von personenbezogenen Daten, in diesem Berichtszeitraum u. a. von Patientendaten, sowie kritische Schwachstellen in Software- und Hardwareprodukten konnten beobachtet werden.“[46]

Auch Bundesinnenminister Seehofer warnte die Bundestagsabgeordneten vor den besonderen Gefahren für die IT-Sicherheit im Zusammenhang mit der Bundestagswahl – allerdings ohne ein entsprechendes Konzept vorzulegen.[47]

Dabei beschränkt sich die gegenwärtige Gefährdung der Beschwerdeführer durch *Zero-Day*-Schwachstelle nicht etwa auf Nischensoftware. Vielmehr existiert sie ganz konkret für Softwareprodukte, die weltweit, auch in Deutschland, und auch von den Beschwerdeführern in ganz überwiegendem Maße verwendet werden. So nutzen alle Beschwerdeführer bereits im Rahmen ihrer Standard IT-Ausstattung des Deutschen Bundestages Rechner mit dem Betriebssystem Microsoft Windows sowie ganz überwiegend zumindest Mobilgeräte der Firma Apple mit dem Betriebssystem iOS. Medienberichte

---

45 ZEIT online vom 7. Januar 2019, „Eine Waffe namens Doxing“, abrufbar unter: https://www.zeit.de/digital/datenschutz/2019-01/privatsphaere-doxing-daten-sammeln-datensicherheit-politiker, zuletzt abgerufen am 8. Juli 2021.

46 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 8. Juli 2021.

47 FAZ von 14. Mai 2021, abrufbar unter https://www.faz.net/aktuell/politik/inland/seehofer-warnt-abgeordnete-vor-it-sicherheitsproblemen-im-wahljahr-17340130.html, zuletzt abgerufen am 8. Juli 2021.

haben zudem im März 2021 über Versuche der Hackergruppe „*Ghostwriter*“ berichtet, die dem russischen Geheimdienst zuzurechnen sein soll, die Rechner von Bundestagsabgeordneten zu infiltrieren.[48]

Als aktuelles Beispiel lassen sich etwa die sog. *BlueKeep*- bzw. *DejaBlue*-Schwachstellen im Windows Remote Desktop Protocol anführen. Durch diese Zero-Day-Schwachstelle[49] können viele Windows-Systeme bis hin zur aktuellen Betriebssystemversion (Windows 10) angegriffen werden. Hierdurch ist es den Angreifern möglich, beliebigen Code – also auch Schadprogramme – auf den angreifbaren Systemen auszuführen. Dabei ermöglicht die Schwachstelle auch eine automatisierte Weiterverbreitung.[50]

Ein weiteres ganz aktuelles Beispiel sind zwei *Zero-Day*-Schwachstellen in der Browsersoftware *Google Chrome,* die erst kürzlich im Juni 2021 bekannt wurden.[51] *Google Chrome* hat in Deutschland einen Marktanteil von 47,73 % und wird – schon aus technischen Gründen – von den Beschwerdeführern täglich genutzt.

Die Beschwerdeführer sind darüber hinaus aber auch insoweit gegenwärtig betroffen, als ihr Verhalten insbesondere im Rahmen der Ausübung ihres Abgeordnetenmandats bereits durch die Bedrohung einer angespannten IT-Sicherheitslage in Deutschland beeinflusst wird.

c. Unmittelbare Beschwer

Auch das Kriterium der unmittelbaren Betroffenheit steht der Zulässigkeit der Verfassungsbeschwerde nicht entgegen. Die geltend gemachten Risiken für die IT-Sicherheit der Beschwerdeführer finden ihre Ursache im Verhalten nichtstaatlicher Dritter. Dass damit ein nur mittelbarer Zusammenhang zu der geltend gemachten Schutzpflichtverletzung durch den Gesetzgeber besteht, kann der Zulässigkeit der Verfassungsbeschwerde jedoch mit Blick auf die Gewährleistung wirksamen Rechtsschutzes nicht entgegenstehen.[52] Zu berücksichtigen ist hier zudem, dass auch staatliches Handeln – die

---

48 ZEIT Online vom 26. März 2021, abrufbar unter https://www.zeit.de/politik/deutschland/2021-03/cyberangriff-russland-hacker-bundestag-ghostwriter-geheimdienst-gru-cyberwar, zuletzt abgerufen am 8. Juli 2021.

49 S. Virsec.com, Microsoft ‘Bluekeep’ Flaw Threatens Medical Devices, IoT, abrufbar unter: https://www.virsec.com/blog/microsoft-bluekeep-flaw-threatens-medical-devices-iot, zuletzt abgerufen am 9. Juli 2021.

50 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 8. Juli 2021.

51 Forbes, Google Confirms 7th ‚Zero Day’ Vulnerability, 19. Juni 2021, abrufbar unter https://www.forbes.com/sites/gordonkelly/2021/06/19/google-chrome-warning-zero-day-security-exploit-free-upgrade-chrome-users/?sh=42a9a1056296, zuletzt abgerufen am 9. Juli 2021.

52 Vgl. BVerfGE 77, 170, 214.

Geheimhaltung und Ausnutzung von Sicherheitslücken zu Zwecken der Quellen-TKÜ und Online-Durchsuchung – dieses Handeln Privater begünstigt.

Darüber hinaus sind die Beschwerdeführer insoweit unmittelbar betroffen, als sie gegen den denkbaren „Vollzugsakt", die staatliche Erlangung und Geheimhaltung von *Zero-Day*-Schwachstellen, mangels Kenntnis nicht vorgehen können.

V. Rechtschutzbedürfnis – Vorherige Erschöpfung des Rechtswegs und Subsidiarität

Einer vorherigen Erschöpfung des Rechtsweges bedurfte es nicht. Erstens ist gegen formelle Gesetze des Bundes ein Rechtsweg nicht gegeben. Zweitens ist ein Abwarten eines Aktes der Exekutive den Beschwerdeführern nicht zuzumuten. Drittens ist – wie dargelegt – nicht sicher, ob die Beschwerdeführer überhaupt von einem Grundrechtseingriff, der auf die angegriffenen Regelungen gestützt ist, Kenntnis erlangen und einfachgerichtlichen Rechtsschutz suchen können.

Viertens schließt § 13 G 10 den Rechtsweg gegen hier angegriffene Beschränkungsmaßnahmen vor der Mitteilung an die Betroffenen in weitem Umfang aus. Hieran ändert auch die Möglichkeit zur Erhebung einer Beschwerde bei der G 10-Kommission nichts. Das angerufene Gericht hat in einer Kammerentscheidung von 1993 zwar die Subsidiarität einer Verfassungsbeschwerde abgelehnt, weil der Beschwerdeführer nicht zuerst die G 10-Kommission angerufen hatte.[53] Der vorliegende Fall unterscheidet sich jedoch vom Sachverhalt der damaligen Entscheidung grundlegend, weil sich die Beschwerdeführer nicht gegen eine konkrete Entscheidung im Einzelfall richten, sondern gegen die Vereinbarkeit der gesetzlichen Eingriffsgrundlage mit dem Grundgesetz. Die G 10-Kommission hätte daher keine Möglichkeit, der Beschwerde abzuhelfen, wenn sie Zweifel an der Verfassungsmäßigkeit von § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 hätte. Sie könnte – anders als ein Fachgericht – noch nicht einmal nach Art. 100 Abs. 1 GG eine konkrete Normenkontrolle einleiten. In einem anschließenden fachgerichtlichen Verfahren hätten die Beschwerdeführer wiederum keine Möglichkeit, ihre Klagebefugnis zu belegen, und müssten eine Klage „ins Blaue hinein" erheben.[54] Dementsprechend hat das Gericht in seiner Entscheidung im Jahr 1999 zum G 10-Gesetz keine vorherige Anrufung der G 10-Kommission verlangt.[55] Auch das Bundesverwaltungsgericht differenziert die Zulässigkeitsanforderungen, die an

---

53 BVerfG, Beschluss vom 13. Juli 1993 – 1 BvR 1016/93.

54 *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 13 Rn. 9; vgl. auch BVerfGE 154, 152, 213 zur Tätigkeit des Bundesnachrichtendienstes und der Schwierigkeit, fachgerichtlichen Rechtsschutz geltend zu machen.

55 Vgl. BVerfGE 100, 313, 354 ff.

eine Klage gegen eine konkrete Beschränkung zu stellen sind und diejenigen, die das Bundesverfassungsgericht für ein Vorgehen gegen das zugrundeliegende Gesetz verlangt.[56]

Fünftens ist es auch nicht erforderlich, zunächst fachgerichtlichen Rechtsschutz zu suchen, weil Kern der Verfassungsbeschwerde eine rein verfassungsrechtliche Frage ist – die Vereinbarkeit der Befugnisse nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 mit den Grundrechten. Das Gericht hat in seiner Entscheidung zum BND-Gesetz diesen Grundsatz noch einmal klargestellt:

> „Nach dem Grundsatz der Subsidiarität sind auch vor der Erhebung von Rechtssatzverfassungsbeschwerden grundsätzlich alle Mittel zu ergreifen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Zu den insoweit zumutbaren Rechtsbehelfen kann gegebenenfalls die Erhebung einer Feststellungs- oder Unterlassungsklage gehören, die eine fachgerichtliche Klärung entscheidungserheblicher Tatsachen- oder Rechtsfragen des einfachen Rechts ermöglicht (vgl. grundlegend zuletzt BVerfGE 150, 309 (326 ff. Rn. 41 ff.) m.w.N.). Anders liegt dies jedoch, soweit es allein um die sich unmittelbar aus der Verfassung ergebenden Grenzen für die Auslegung der Normen geht. Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht (vgl. BVerfGE 123, 148 (172 f.); 143, 246 (322 Rn. 211); stRspr). Insoweit bleibt es dabei, dass Verfassungsbeschwerden unmittelbar gegen ein Gesetz weithin auch ohne vorherige Anrufung der Fachgerichte zulässig sind (vgl. BVerfGE 150, 309 (326 f. Rn. 44)).“[57]

Auch im Fall der vorliegenden Beschwerde würde daher die Anrufung der Fachgerichte zu keiner weiteren Klärung des Sachverhalts führen, sondern die Entscheidung der verfassungsrechtlichen Kernfragen nur verzögern.

VI. Frist

Die Verfassungsbeschwerde ist innerhalb der Jahresfrist des § 93 Abs. 3 BVerfGG erhoben. Die mit der Verfassungsbeschwerde angegriffenen Vorschriften in den § 11 Abs. 1a G 10, § 11 Abs. 1b, § 15a G 10 treten nach Art. 8 Abs. 1 des Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 am Tag nach der Verkündung des Gesetzes in Kraft. Die Verkündung im Bundesgesetzblatt erfolgte am 8. Juli

---

56 BVerwGE 149, 359, 372 f.

57 BVerfGE 152, 154, 185 f.

2021 (s. BGBl. 2021 I, S. 2274). Die angegriffenen Vorschriften sind mithin am 9. Juli 2021 in Kraft getreten.
Soweit sich die Verfassungsbeschwerde gegen weitere Vorschriften im G 10, namentlich gegen § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1, § 3 Abs. 2 Satz 2, § 3 Abs. 2 Satz 2, § 3a, § 4 Abs. 4, § 12 und § 13 G 10 richtet, die nicht durch das vorgenannte Gesetz in ihrem Wortlaut selbst geändert wurden, ist sie ebenfalls fristgemäß erhoben. Die Jahresfrist des § 93 Abs. 3 BVerfGG ist auch insoweit gewahrt. Zwar wurden diese Vorschriften nicht durch das Gesetz zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 geändert.

Bei einer Gesetzesänderung wird die Jahresfrist des § 93 Abs. 3 BVerfGG auch dann neu in Lauf gesetzt, wenn der Gesetzgeber das materielle Gewicht einer Regelung verändert, den Anwendungsbereich einer Norm eindeutiger als bisher bestimmt, ihn grundlegend umgestaltet oder erweitert und der Vorschrift damit einen neuen Inhalt oder eine andere Bedeutung gibt oder wenn durch die Gesetzesänderung durch die Einbettung einer äußerlich unverändert gebliebenen Norm in ein anderes gesetzliches Umfeld eine neue und zusätzliche Beschwer geschaffen wird.[58]

Dies ist vorliegend der Fall. Der Gesetzgeber schafft durch § 11 Abs. 1a G 10 die Grundlage für einen neuen Eingriff in die Grundrechte, der bisher nach § 3 Abs.1 i.V.m. § 11 G 10 nicht zulässig war. Dabei greift er auf die Voraussetzungen (§ 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10) und Begleitregelungen des G 10, namentlich auf Regelungen dahingehend, gegen wen sich die Anordnung richten darf (§ 3 Abs. 2 Satz 2 G 10), solche zum Schutz des Kernbereichs privater Lebensgestaltung (§ 3a G 10), zu Übermittlungen (§ 4 Abs. 4 G 10), zur Benachrichtigungspflicht (§ 12 G 10) sowie zur Einschränkung des Rechtswegs (§ 13 G 10) zurück, die schon für die bisher zulässigen Beschränkungen galten. Ebenso gut hätte er die Voraussetzungen und Begleitregelungen der Quellen-TKÜ und der beschränkten Online-Durchsuchung nach § 11 Abs. 1a G 10 als eigenständige Befugnisnorm neu erlassen können. Nur weil der Gesetzgeber regelungstechnisch einen anderen Weg gewählt hat, darf dies den verfassungsgerichtlichen Rechtsschutz nicht verkürzen. Die Einfügung der Befugnis zur Durchführung von sog. Quellen-TKÜ und beschränkten Online-Durchsuchungen in § 11a Abs. 1a G 10 verändert damit den Regelungskontext und erweitert so den Anwendungsbereich dieser bereits früher erlassenen Regelungen. Die angegriffenen weiteren Vorschriften im G 10 bewirken mithin im Vergleich mit dem früheren Rechtszustand neue und zusätzliche Belastungen.[59] Dementsprechend beginnt auch in Bezug auf diese Regelungen die

---

58 BVerfGE 11, 351, 359 f.; 74, 69, 73; 78, 350, 356; 100, 313, 356; 111, 382, 411; 120, 274, 298; 131, 316, 333.

59 Vgl. BVerfGE 141, 220, 262 f. (zu dem ähnlich gelagerten Fall der Übermittlungsbefugnis im BKA-Gesetz); ferner BVerfGE 100, 313, 356.

Beschwerdefrist neu, soweit sie sich auf Beschränkungen nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 1 und 2 G 10 beziehen.

VII. Sonstige allgemeine Zulässigkeitsvoraussetzungen

Die Verfassungsbeschwerde enthält einen ordnungsgemäßen Antrag gemäß §§ 23 Abs. 1, 93 BVerfGG. Sie ist schriftlich mit Begründung erhoben und genügt mithin den Anforderungen des § 23 Abs. 1 BVerfGG.

VIII. Ergebnis zur Zulässigkeit

Die Verfassungsbeschwerde ist mithin zulässig.

C. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist begründet.

I. Formelle Verfassungswidrigkeit – keine Gesetzgebungskompetenz des Bundes für Verfassungsschutzbehörden der Länder

Die § 3 i.V.m. § 11 Abs. 1a G 10 verstoßen gegen die Kompetenzordnung des Grundgesetzes und verletzten damit Art. 30, 70 GG, indem sie in Befugnisse der Verfassungsschutzbehörden der Länder (§ 1 Abs. 1 Nr. 1 G 10) Regelungen treffen.

1. Teilweise fehlende Gesetzgebungskompetenz für § 3 i.V.m. § 11 Abs. 1a G 10 in Bezug auf Verfassungsschutzbehörden der Länder

Nach Art. 70 Abs. 1 GG haben die Länder das Recht der Gesetzgebung, soweit das Grundgesetz nicht dem Bund Gesetzgebungsbefugnisse verleiht. Eine solche Verleihung der Gesetzgebungskompetenz durch das Grundgesetz zugunsten des Bundes ist vorliegend nicht gegeben.

Eine Grundrechtsverletzung liegt auch dann vor, wenn der den Eingriff begründende Rechtssatz nicht mit der bundesstaatlichen Ordnung der Gesetzgebungskompetenzen, wie sie im Grundgesetz vorgesehen ist, vereinbar ist.[60]

Vorliegend verletzt § 3 i.V.m. § 11 Abs. 1a G 10 die Kompetenzordnung des Grundgesetzes, soweit hierin eine Ermächtigung für Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden

60 S. etwa BVerfGE 98, 106, 117.

enthalten ist.[61] Für eine solche Ermächtigung fehlt dem Bund die Gesetzgebungskompetenz.[62]

Hierdurch werden die Beschwerdeführer in Art. 10 Abs. 1 GG sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt.

2. Keine Gesetzgebungskompetenz des Bundes durch Art. 74 Abs. 1 Nr. 1 GG

Das angerufene Gericht hat in seinem ersten G 10-Urteil in BVerfGE 30, 1 die Vorgängerregelung des gegenwärtigen § 3 G 10[63] kompetenzrechtlich gebilligt. Als maßgeblichen Kompetenztitel hat das angerufene Gericht seinerzeit Art. 74 Nr. 1 GG[64] angeführt, wonach der Bund das „gerichtliche Verfahren" regeln darf. In dem Urteil wird dazu ausgeführt:

> „Art. 1 § 2 G 10 dient der Abwehr verfassungsfeindlicher Bestrebungen im Vorfeld strafprozessualer Ermittlungen. Die zulässigen Beschränkungsmaßnahmen sind begrenzt auf die Fälle, in denen tatsächliche Anhaltspunkte für den Verdacht bestehen, daß bestimmte strafbare Handlungen geplant, begangen werden oder begangen worden sind. Die Beschränkungsmaßnahmen nach Art. 1 § 2 G 10 dienen also (wenigstens mittelbar) der Verhinderung, Aufklärung und Verfolgung von Straftaten."[65]

Aus heutiger Stand ist diese Auslegung der Verfassung nicht tragfähig. Würde dieses Verständnis von Art. 74 Abs. 1 Nr. 1 GG zutreffen, so könnte der Bund neben dem Verfassungsschutzrecht auch das allgemeine Polizeirecht, das weitgehend unbestritten in die alleinige Gesetzgebungskompetenz der Länder fällt, weitgehend an sich ziehen. Das allgemeine Polizeirecht hat in wesentlichem Maße die Verhinderung von Straftaten zum Gegenstand.

Im Hinblick auf die Zwecken des Gesetzes, die das angerufene Gericht in BVerfGE 30, 1, 29 seinerzeit ausgeführt hat, ist aus heutiger Sicht weiter entgegenzubringen, dass die Aufklärung von Straftaten kompetenzrechtlich unergiebig ist. Denn für die Verteilung der Gesetzgebungskompetenzen ist das Ziel einer Aufklärungsmaßnahme entscheidend. Tatsächlich unterfällt die Verfolgung von Straftaten dem Kompetenztitel in Art. 74 Abs. 1 Nr. 1 GG. Die Verfolgung von Straftaten ist jedoch nicht das Ziel von

---

61 Zur Erstreckung der Vorschrift auch auf die Landesverfassungsschutzbehörden siehe § 1 Abs. 1 Nr. 1 G 10.

62 Näher hierzu *Bäcker*, DÖV 2011, S. 840 ff.; *ders.*, DÖV 2012, S. 560 ff.

63 Art. 1 § 2 G 10 a.F.

64 Heute ist dies Art. 74 Abs. 1 GG.

65 BVerfGE 30, 1, 29.

Überwachungsmaßnahmen durch Verfassungsschutzbehörden.[66] Denn ihre Aufgabe ist ersichtlich nicht die Strafverfolgung. Ebenso ist die Verhinderung von Straftaten nicht unmittelbar Aufgabe der Verfassungsschutzbehörden. Ihre Aufgabe beschränkt sich auf die Vorfeldaufklärung, mithin auf die Beobachtung und Auswertung von Informationen. Selbst wenn man die Verhinderung von Strfatataten indes als mittelbares Ziel von Überwachungsmaßnahmen nach § 3 i.V.m. § 11 Abs. 1a Satz 1 und 2 G 10 anerkennen würde, ließe sich die Verhinderung von Straftaten nicht unter Art. 74 Abs. 1 Nr. 1 GG subsumieren.[67] Denn eine allgemeine Gesetzgebungskompetenz des Bundes für präventiv ausgerichtete Überwachungsmaßnahmen existiert nicht. Eine solche lässt sich für den Bund allein bereichsspezifisch begründen, wenn bestimmte Überwachungsmaßnahmen notwendig mit einem Sachbereich zusammenhängen, für den Bund eine Gesetzgebungskompetenz hat.[68] Dies ist vorliegend nicht der Fall.

Im Ergebnis folgt aus Art. 74 Abs. 1 Nr. 1 GG mithin keine Gesetzgebungskompetenz des Bundes für § 3 i.V.m. § 11 Abs. 1a G 10.

3. Keine Gesetzgebungskompetenz des Bundes durch Art. 73 Abs. 1 Nr. 10 lit. b und lit. c GG

Die Gesetzgebungskompetenz des Bundes für § 3 i.V.m. § 11 Abs. 1a G 10 folgt auch nicht aus Art. 73 Abs. 1 Nr. 10 lit. b oder lit. c GG. Danach ist der Bund ausschließlich dafür zuständig, die Zusammenarbeit des Bundes und der Länder zum Verfassungsschutz und zum Schutz gegen gewaltbereite inländische Bestrebungen, die auswärtige Belange der Bundesrepublik gefährden, zu regeln. Der Begriff der „Zusammenarbeit“ macht hierbei deutlich, dass es in der Sache um Kooperation zwischen Bundes- und Landesbehörden mit parallelen Aufgaben handelt, wobei die jeweiligen Bundes- und Landesbehörden stets (nur) innerhalb ihrer eigenen Kompetenzen handeln (können).[69] Die Länder sind darüber hinaus zum Erlass von Gesetzen zur Abwehr von Bestrebungen gegen die freiheitliche demokratische Grundordnung befugt, soweit sich diese im jeweiligen Land auswirken und damit in diesem Land Gefahren hervorrufen können.[70] Selbst bei extensiver Auslegung kann eine Gesetzgebungskompetenz hieraus nicht begründet werden. Denn auch die Tatsache, dass der Bund den Ländern Mindeststandards für die Aufgabenwahrnehmung und potentiell auch für bestimmte Befugnisse der Landesverfassungsschutzbehörden auferlegen

---

66 S. näher zu den Aufgaben der Nachrichtendienste in Abgrenzung zu Polizei- und Strafverfolgungsbehörden BVerfGE 133, 277, 325 ff.

67 Vgl. zur vorbeugenden Bekämpfung von Straftaten durch die Polizei BVerfGE 113, 348, 368 f.

68 BVerfGE 113, 348, 369, unter Verweis auf BVerfGE 109, 190, 215; ähnlich auch BVerfGE 110, 33, 48.

69 Vgl. BVerfGE 133, 277, 317 f.

70 BVerfGE 113, 63, 79.

kann, um eine hinreichend effektive Zusammenarbeit zwischen Bund und Ländern zu gewährleisten,[71] führt zu keiner anderen kompetenzrechtlichen Bewertung. Denn bei eine, solchen Vorgehen des bundes kann es allein um die Vorgabe eiens Rahmens für die Wahrnehmung von Aufgaben- und Befugnissen handeln. Innerhalb dieses Rahmens steht es den Ländern auch in diesem Fall Ländern weiterhin frei, zu entscheiden, zu welchen Maßnahmen sie ihre Verfassungsschutzbehörden ermächtigen und unter welchen Voraussetzungen dies geschieht.[72]

Dies entspricht auch dem vom Bundesverfassungsgericht entwickelten Doppeltürmodell, welches das angerufene Gericht zum Beispiel auf die Vorratsdatenspeicherung und die Bestandsdatenauskunft angewandt hat.[73] Der Bund erlaubt Unternehmen auf Anfragen von Behörden Auskünfte zu erteilen oder verpflichtet sie zur Kooperation (hier z.B. § 2 G 10). Dabei legt der Bund auch die Voraussetzungen und Zwecke fest sowie ggf. weitere datenschutzrechtliche Begleitregelungen. Inwieweit die Länder „durch diese Tür gehen" und einen Abruf dieser Daten zulassen, ist aber dem Landesgesetzgeber überlassen. Dies hat das Gericht zur Vorratsdatenspeicherung klargestellt.[74] Er kann zum Beispiel zu dem Ergebnis kommen, dass sein Landesamt für Verfassungsschutz nicht die Befugnis haben soll, einen so sensiblen Eingriff wie die Infiltration eines IT-Systems durchzuführen. Im Moment könnte sich das Landesamt für Verfassungsschutz unmittelbar auf § 3 Abs. 1 i.V.m. § 11a Abs. 1, § 1 Abs. 1 Nr. 1 G 10 stützen.

In der Folge kann der Bund nicht autark Eingriffsermächtigungen für die Landesverfassungsschutzbehörden schaffen, einmal weniger, wenn diese Ermächtigungen nicht unmittelbar die Zusammenarbeit von Bund und Ländern betreffen, wie es vorliegend der Fall ist. eine solche eigenständige Eingriffsermächtigung enthält § 3 i.V.m. § 11 Abs. 1a Satz 1 und 2 G 10, soweit diese Befugnisnorm auch für die Landesverfassungsschutzbehörden gilt. Sie lässt sich daher selbst bei weiter Auslegung nicht auf den Kompetenztitel in Art. 73 Abs. 1 Nr. 10 lit. b oder c GG auch bei extensivster Auslegung stützen.

4. Fehlen sonstiger (potenziell) die Bundeskompetenz begründender Kompetenznormen im Grundgesetz

Weitere Vorschriften des Grundgesetzes, die wenigstens potenziell die Gesetzgebungskompetenz des Bundes für § 3 i.V.m. § 11 Abs. 1a G 10

---

71 S. dazu etwa BVerwG, Beschluss vom 9. Januar 1995 – 1 B 231.94 1 C 34/94; *Uhle*, in: Maunz/Dürig, GG, 93. EL Oktober 2020, Art. 73 Rn. 233.

72 Vgl. BVerfGE 125, 260, 346.

73 S. zum sog. „Doppeltürmodell" BVerfGE 130, 151, 184.

74 BVerfGE 125, 260, 314 f. (dort zur Reichweite des Art. 73 Abs. 1 Nr. 7 [Telekommunikation]).

begründen könnten, sind nicht ersichtlich. Daher steht das Recht zur Gesetzgebung insoweit gem. Art. 70 Abs. 1 GG den Ländern zu.

Dadurch, dass der Gesetzgeber des Bundes die Kompetenz zur Gesetzgebung insoweit in Anspruch genommen hat, liegt ein Verstoß gegen die grundgesetzliche Kompetenzordnung vor, durch die zugleich die Beschwerdeführer in ihren Grundrechten aus Art. 10 Abs. 1 GG sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt werden.

II. Materielle Verfassungswidrigkeit der Ermächtigungsgrundlage in § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 1 G 10 zur Quellen-TKÜ im Hinblick auf Art. 10 Abs. 1 GG

Die Neuregelung der Eingriffsbefugnis zur Quellen-TKÜ in § 11 Abs. 1a G 10 übernimmt pauschal durch die gewählte Regelungstechnik die Schutzgüter und Tatbestandsvoraussetzungen in § 3 G 10.

Der insoweit in Bezug genommene Straftatenkatalog in § 3 Abs. 1 G 10 und die weiteren Tatbestandsvoraussetzungen des § 3 G 10 genügen den verfassungsrechtlichen Anforderungen nicht – und zwar *unabhängig* davon, ob man diese an Art. 10 Abs. 1 GG oder am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationsrechtlicher Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, im Folgenden *IT-Grundrecht* genannt) misst. In beiden Fällen verstößt § 3 G 10 i.V.m. § 11 Abs. 1a G 10 gegen den Grundsatz der Verhältnismäßigkeit i.F.d. Angemessenheit sowie gegen den Bestimmtheitsgrundsatz.

§ 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 stellt mit der Ermächtigung zur Quellen-TKÜ nach Auffassung des einfachen Gesetzgebers eine gesetzliche Eingriffsgrundlage in Art. 10 Abs. 1 GG dar.[75] Das Instrument der Quellen-TKÜ ist zuletzt vom angerufenen Gericht in der *BKA-Entscheidung* in BVerfGE 141, 220 im Grundsatz bestätigt worden, wonach die Quellen-TKÜ zwar technisch einen Zugriff auf das entsprechende informationstechnische System voraussetze, jedoch sofern sie ausschließlich Überwachungen erlaube, die sich auf den laufenden Telekommunikationsvorgang beschränkten, nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern an Art. 10 Abs. 1 GG zu messen sei.[76] Entsprechend beschränkt § 11 Abs. 1a Satz 1 HS 1 G 10 die Überwachung und Aufzeichnung auf die „laufende Telekommunikation“. Es liegt jedenfalls daher ein Eingriff in Art. 10 Abs. 1 GG vor.

---

75 Siehe Art. 6 des Gesetzes zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021, BGBl. 2021 I, 2274, 2279 sowie BT-Drs. 19/24785, S. 24.

76 BVerfGE 141, 220, 309; BVerfG, Beschluss vom 6. Juli 2016 – 2 BvR 1454/13.

Dieser Eingriff ist materiell verfassungsrechtlich nicht gerechtfertigt.

1. Materielle Mängel – Verstoß gegen den Grundsatz der Verhältnismäßigkeit

a. Verfassungsrechtlicher Maßstab

Die Überwachung der laufenden Telekommunikation begründet nach der Rechtsprechung des Bundesverfassungsgerichts einen schwerwiegenden Eingriff.[77] Zum einen wird die Intensität des Grundrechtseingriffs durch die Heimlichkeit der Überwachungsmaßnahme intensiviert, des weiteren jedoch auch dadurch, dass Schutzmaßnahmen umgangen werden, die der Betroffene zur Wahrung der Vertraulichkeit ergriffen hat. Die Streubreite der betroffenen Personen tritt als eingriffsintensivierender Umstand hinzu. Aus der Rechtsprechung des angerufenen Gerichts zum Sicherheitsrecht lassen sich die verfassungsrechtlichen Maßstäbe für Überwachungsermächtigungen im Nachrichtendienstrecht ableiten. Ausgangspunkt ist wie stets der Verhältnismäßigkeitsgrundsatz und hierbei insbesondere die Angemessenheit, also das Gebot der Verhältnismäßigkeit im engeren Sinne. Danach sind an die gesetzlichen Eingriffsschwellen desto höhere Anforderungen zu stellen, je schwerer der geregelte Überwachungseingriff wiegt. Dies kann zur Folge haben, dass eine bestimmte Überwachungsmaßnahme nicht durch Interessen des Allgemeinwohls gerechtfertigt werden kann, weil die Grundrechtsbeeinträchtigungen für den Betroffenen, die damit einhergehen, schwerer wiegen als die Belange der Allgemeinheit.[78]

Die verfassungsrechtlichen Anforderungen an gesetzliche Eingriffsschwellen knüpfen hierbei im Kern an zwei Parameter an: Zum einen muss das Gesetz einen hinreichend gewichtigen Anlass für die jeweilige Überwachungsmaßnahme regeln, und zwar in hinreichend normenklarer Form. Zum anderen muss das Gesetz sicherstellen, dass die Zielperson der Überwachungsmaßnahme in einer hinreichenden tatsächlichen Nähe zu dem Anlass der Maßnahme steht.

In der Rechtsprechung des angerufenen Gerichts ist seit Längerem anerkannt, dass die verfassungsrechtlichen Anforderungen an die gesetzlichen Eingriffsschwellen mit zunehmender Eingriffsintensität der jeweiligen Überwachungsmaßnahme höhere sind – dies gilt auch für das Nachrichtendienstrecht.[79] Das angerufene Gericht hat in der Vergangenheit

---

77 BVerfGE 141, 220, 310; 113, 348, 382; 129, 208, 240.

78 Vgl. BVerfGE 120, 274, 322.

79 Siehe etwa zu Eingriffen in das Fernmeldegeheimnis BVerfGE 120, 274, 342 f.; 155, 119, 186.

mehrfach deutlich gemacht, dass die Anforderungen an Überwachungsermächtigungen im Nachrichtendienstrecht bei besonders eingriffsintensiven Maßnahmen mit den Anforderungen an polizeirechtliche Ermächtigungen übereinstimmen. [80] Die verfassungsrechtliche Mindesteingriffsschwelle ist hierbei auch nicht deshalb abzusenken, weil die Nachrichtendienste aufgrund ihres Aufgabenbereichs nur im Vorfeld tätig sind und nicht konkrete Gefahren mit Exekutivmaßnahmen bekämpft.[81] Vielmehr hat das angerufene Gericht die Tätigkeiten von Nachrichtendiensten als besonders besonders schwerwiegende Eingriffe bewertet, weil ihre gesamte Tätigkeit weit im Vorfeld einer konkreten Gefahr geheim erfolgt und „das Gefühl des unkontrollierbaren Beobachtetwerdens" befördert.[82]

Das BKA-Urteil, in dem die verfassungsrechtlichen Anforderungen an präventivpolizeiliche Überwachungsmaßnahmen präzisiert und aktualisiert werden, erlaubt es, Maßstäbe auch für Eingriffsermächtigungen für heimtliche Überwachungsmaßnahmen im Nachrichtendienstrecht zu präzisieren und festzulegen. Das angerufene Gericht hat in der BKA-Entscheidung judiziert, dass eine Überwachung der Telekommunikation zur Abwehr des internationalen Terrorismus gerechtfertigt sein kann.[83]

> „Für Maßnahmen, die der Gefahrenabwehr dienen und damit präventiven Charakter haben, kommt es unmittelbar auf das Gewicht der zu schützenden Rechtsgüter an (vgl. BVerfGE 125, 260 [329]). Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig. Hierzu gehören Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes (vgl. BVerfGE 120, 274 [328]; 125, 260 [330]). Einen uneingeschränkten Sachwertschutz hat das Bundesverfassungsgericht demgegenüber nicht als ausreichend gewichtig für solche Maßnahmen angesehen. Es hat den Zugriff auf vorsorglich gespeicherte Daten (vgl. BVerfGE 125, 260 [330]) oder die Durchführung von Wohnraumüberwachungen jedoch auch bei einer gemeinen Gefahr (vgl. BVerfGE 109, 279 [379]) und Online-Durchsuchungen bei einer Gefahr für Güter der Allgemeinheit, die die Existenz der Menschen

---

80 S. ferner im Hinblick auf einen Eingriff in das informationelle Selbstbestimmungsrecht BVerfGE 154, 152, 239: „Für geheime Überwachungsmaßnahmen durch Sicherheitsbehörden hat das Bundesverfassungsgericht die sich hieraus ergebenden Anforderungen durch eine Vielzahl von Entscheidungen konkretisiert und insbesondere in der Entscheidung zum BKA-Gesetz zusammengefasst (vgl. BVerfGE 141, 220, 268 ff Rn. 103 ff.). Diese Maßstäbe, die auch für Überwachungsmaßnahmen der Nachrichtendienste gelten, bilden sowohl für die Anforderungen an die Datenerhebung und -verarbeitung als auch für die Anforderungen an die Übermittlung der Daten den Ausgangspunkt."; BVerfGE 155, 119, 189.

81 Vgl. zur Online-Durchsuchung BVerfGE 120, 274, 329 ff. und zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260, 331 f.

82 BVerfGE 125, 260, 332.

83 BVerfGE 141, 220, 310.

berühren (vgl. BVerfGE 120, 274 [328]), für im Grundsatz mit der Verfassung vereinbar gehalten."[84]

Die Grenze des verfassungsrechtlich Zulässigen wird insoweit klar gezogen:

„Mit der Verfassung nicht zu vereinbaren ist demgegenüber die nicht näher eingeschränkte Erstreckung der Telekommunikationsüberwachung nach § 20l Abs. 1 Satz 1 Nr. 2 BKAG auf Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie terroristische Straftaten vorbereiten. Die Vorschrift, die über die Abwehr einer konkreten Gefahr hinaus die Eingriffsmöglichkeiten mit dem Ziel der Straftatenverhütung vorverlagert, verstößt in ihrer konturenarmen offenen Fassung gegen den Bestimmtheitsgrundsatz und ist unverhältnismäßig weit. Es gelten insoweit die gleichen Erwägungen wie zu § 20g Abs. 1 Satz 1 Nr. 2 BKAG (siehe oben C V 1 d). Die geringfügigen Formulierungsunterschiede gegenüber jener Vorschrift begründen keinen substantiellen Unterschied. Dies erhellt auch die Gesetzesbegründung, die den Gehalt des § 20l Abs. 1 Satz 1 Nr. 2 BKAG zum Teil mit den Worten, die der Gesetzgeber in § 20g Abs. 1 Satz 1 Nr. 2 BKAG benutzt, paraphrasiert (vgl. BTDrucks 16/10121, S. 31). Soweit sich § 20l Abs. 2 BKAG auf diese Vorschrift bezieht, kann nichts anderes gelten."[85]

Die Ausführungen des angerufenen Gerichts zu § 20g Abs. 1 S. 1 Nr. 2 BKAG a.F. sind auch im vorliegenden Fall einschlägig:

„aa) § 20g Abs. 1 Satz 1 Nr. 2 BKAG ergänzt die auf die Gefahrenabwehr begrenzte Eingriffsgrundlage des § 20g Abs. 1 Satz 1 Nr. 1 BKAG und soll nach der Vorstellung des Gesetzgebers schon früher ansetzen und der Straftatenverhütung dienen.

Nach den oben dargelegten Maßstäben ist der Gesetzgeber hieran nicht grundsätzlich gehindert und zwingt ihn die Verfassung nicht, Sicherheitsmaßnahmen auf die Abwehr von – nach tradiertem Verständnis – konkreten Gefahren zu beschränken. Allerdings bedarf es aber auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (vgl. BVerfGE 110, 33 [56f., 61]; 113, 348 [377f.]; 120, 274 [328f.]; 125, 260 [330]). In Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in

84 BVerfGE 141, 220, 270 f.
85 BVerfGE 141, 220, 310.

> überschaubarer Zukunft terroristische Straftaten begeht […]. Die diesbezüglichen Anforderungen sind normenklar zu regeln.
>
> bb) Dem genügt § 20g Abs. 1 Satz 1 Nr. 2 BKAG nicht. Zwar knüpft die Vorschrift an eine mögliche Begehung terroristischer Straftaten an. Die diesbezüglichen Prognoseanforderungen sind hierbei jedoch nicht hinreichend gehaltvoll ausgestaltet. Die Vorschrift schließt nicht aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt. Sie enthält weder die Anforderung, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Damit gibt sie den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand und eröffnet Maßnahmen, die unverhältnismäßig weit sein können."[86]

Das angerufene Gericht hat im vorzitierten BKA-Urteil eingriffsintensive Überwachungsmaßnahmen dem Erfordernis einer konkreten Gefahr als einheitliche Mindesteingriffsschwelle unterworfen. Gleichzeitig hat das angerufene Gericht den verfassungsrechtlichen Begriff der konkreten Gefahr von dem polizeirechtlichen Gefahrbegriff getrennt und im Verhältnis zum polizeirechtlichen Gefahrbegriff erweitert:

Eine konkrete Gefahr im verfassungsrechtlichen Sinne liegt danach nicht nur dann vor, wenn situationsbezogen ein Schaden mit hinreichender Wahrscheinlichkeit droht – so verlangt es der polizeirechtliche Gefahrbegriff. Eine „hinreichend konkretisierte Gefahr" könne daneben auch schon dann bestehen, „wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen."[87] Diese Tatsachen müssten „zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann."[88] Im Hinblick auf terroristische Straftaten hat das angerufene Gericht es für ausreichend erhaltet, „wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird".[89]

---

86 BVerfGE 141, 220, 290 f.
87 BVerfGE 141, 220, 272.
88 BVerfGE 141, 220, 272.
89 BVerfGE 141, 220, 272 f.

Die gewählte Formulierung des angerufenen Gerichts zielt erkennbar auf eine Ergänzung der situationsbezogenen Schadensprognose des klassischen polizeirechtlichen Gefahrbegriffs um eine personenbezogene Gefährlichkeitsprognose; diese muss jedoch auf hinreichend aussagekräftigen Tatsachen beruhen. [90]

Der erweiterte verfassungsrechtliche Gefahrbegriff begrenzt das Risiko, das dadurch entsteht, dass gerade die Nachrichtendienste sehr einriffsintensive Überwachungsmaßnahmen vornehmen und diese im Wesentlichen (nur) auf allgemeine Erfahrungssätze stützen könnten. Ihr Gebrauch wird rechtlich nicht näher dargelegt, Prognosen sind in der Regel allenfalls in sehr grober Form mit dem Risiko entsprechender Fehleinschätzungen verbunden. Denn der erweiterte verfassungsrechtliche Gefahrbegriff ermöglicht Überwachungsmaßnahmen gerade nur gegenüber solchen Personen, die aufgrund ihres Vorverhaltens belastbar als „gefährlich" gekennzeichnet werden können.

Nach den verfassungsrechtlichen Korrekturen im Polizeirecht durch das Urteil zum BKA-Gesetz sind nunmehr die entsprechenden verfassungsgerichtlichen Anpassungen im Nachrichtendienstrecht von Nöten, da inbsoweit eine strukturelle Parallele besteht. Personengerichtete Überwachungsmaßnahmen mit hoher Eingriffsintensität sind auch im Nachrichtendienstrecht an eine situationsbezogene Schadens- oder eine personenbezogene Gefährlichkeitsprognose zu binden, so wie sie das angerufene Gericht für das Polizeirecht bereits verfassungsrechtlich entwickelt und festgelegt hat. Nach der Erweiterung des verfassungsrechtlichen Gefahrbegriffs ist eine Absenkung der verfassungsrechtlichen Mindesteingriffsschwelle für solche Überwachungsmaßnahmen nicht mehr angezeigt. [91]

Eine solchge Absenkung wäre auch nicht sachgerecht, da bei wesentlichen heimlichen Überwachungsmaßnahmen Nachrichtendienste im Rahmen ihrer Aufgabenwahrnehmung nicht weniger eingriffsintensiv agieren als Polizeibehörden, die im Vorfeld einer Gefahr Informationen erheben. Zu beachten ist hierbei stets, dass das Institut der Datenweitergabe mit den entsprechenden Übermittlungsvorschriften eine grundsätzliche Nutzung der weit im Vorfeld einer konkreten Gefahr gesammelten Informationen und Erkenntnisse an Behörden mit Exekutivbefugnissen stets ermöglicht, mehr noch, die Sammlung und Auswertung von Informationen durch

---

90 Vgl. für einen Ansatz zur rechtsdogmatischen Erfassung und Rationalisierung personenbezogener Prognoseurteile *Bäcker*, Kriminalpräventionsrecht, 2015, S. 205 ff.

91 Vgl. andeutungsweise bereits BVerfGE 141, 220, 340: danach bedürfen „ungeachtet ihres im Wesentlichen auf das Vorfeld von Gefahren beschränkten Handlungsauftrags" auch Datenerhebungen von Verfassungsschutzbehörden grundsätzlich einer „konkretisierte[n] Gefahrenlage".

Nachrichtendienste im Kern auf eine Weitergabe in welcher Form auch immer an Dritte funktional angelegt ist. Dies ist bei der Bewertung der Eingriffstiefe nachrichtendienlicher Überwachungsmaßnahmen zu beachten. Auch im Fall polizeilicher Ermittlungen sind imperative Folgemaßnahmen keine notwendige Konsequenz. Sofern die Möglichkeit imperativer Folgemaßnahmen eine erhöhte Eingriffsintensität begründet, steht dem bei den Nachrichtendiensten ein ein Handeln weit im Vorfeld mit niedrigeren Eingriffsschwellen gegenüber. Dies erhöht die Eingriffsintensität entsprechend.

b. Tatsächliche Anhaltspunkte für den Verdacht der Planung oder Begehung einer Straftat als unzureichende *tatsächlich-prognostische* Eingriffsschwelle für eine Quellen-TKÜ

Das Tatbestandsmerkmal in § 3 Abs. 1 G 10, wonach „tatsächliche Anhaltspunkte für den Verdacht bestehen" müssen, dass eine in § 3 Abs. 1 G 10 genannte Katalogstraftat geplant, begangen wird oder begangen worden ist, genügt nicht den oben skizzierten verfassungsrechtlichen Vorgaben an Ermächtigungen zu eingriffsintensiven Überwachungsmaßnahmen wie der Quellen-TKÜ. Der Grundsatz der Verhältnismäßigkeit sowie der Bestimmtheitsgrundsatz werden hierdurch verletzt.

Auf Bundesebene ist die Quellen-TKÜ als strafprozessuale Maßnahme gesetzlich in § 100a Abs. 1 Satz 2 und Satz 3 StPO geregelt. Gemäß §§ 5, 51 Abs. 2 BKAG kann das Bundeskriminalamt die Quellen-TKÜ zur Abwehr von Gefahren des internationalen Terrorismus einsetzen. Einige Landesverfassungsschutzgesetze sehen für ihre jeweiligen Landesämter für Verfassungsschutz die Befugnis zur Quellen-TKÜ vor (vgl. bspw. Art. 13 Bayerisches Verfassungsschutzgesetz sowie § 8 Abs. 12 Hamburgisches Verfassungsschutzgesetz), ebenso einzelne Polizeigesetze der Länder.[92]

Anders als in § 3 Abs. 1 G 10 sprechen die Polizeigesetze indes hinsichtlich der Eingriffsschwelle für eine Quellen-TKÜ von „bestimmten Tatsachen", so z.B. § 51 BKAG, § 54 PolG BW, § 24 PolDVG Hamburg. § 20c PolG NRW spricht von einer „Person […] deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 8 Absatz 4 [PolG NRW] begehen wird."

Die Eingriffsschwelle der „tatsächlichen Anhaltspunkte" ist dabei weniger streng als die der „bestimmten Tatsachen", wie sie auch in § 100a Abs. 1 Nr. 1 StPO gefordert werden. Sie ist zudem auch weniger konkret

92 S. etwa § 54 PolG BW, § 24 PolDVG Hamburg, § 20c PolG NRW.

als „zureichende tatsächliche Anhaltspunkte“ i.S.v. § 152 Abs. 2 StPO, um ein strafprozessuales Ermittlungsverfahren einleiten zu können.[93]

Zwischen diesen beiden Eingriffsschwellen wird – zu Recht – auch in der Praxis entsprechend differenziert, s. etwa:

> „Als ‚Tatsachen‘ werden dem Beweis zugängliche wahrnehmbare oder feststellbare äußere oder innere Zustände oder Vorgänge bezeichnet, die in der Gegenwart oder Vergangenheit liegen. Sie unterscheiden sich von bloßen ‚tatsächlichen Anhaltspunkten‘, die eine Annahme bereits rechtfertigen, wenn es nach polizeilicher oder gefahrenabwehrbehördlicher Erfahrung als möglich erscheint, dass ein bestimmter Sachverhalt vorliegt und hierfür bestimmte Indizien sprechen.“[94]

> „Tatsachen“ und „tatsächliche Anhaltspunkte“ sind mithin nicht identisch oder austauschbar, sondern umreißen graduell unterschiedliche konditionale Voraussetzungen.“[95]

Auch das Verwaltungsgericht Berlin unterscheidet insoweit:

> „Danach ist der Begriff der „tatsächlichen Anhaltspunkte“ weiter auszulegen als die entsprechenden Begriffe im Strafprozess- und Polizeirecht, will aber verhindern, dass die Sammlung und Auswertung von Informationen aufgrund bloßer Mutmaßungen, Hypothesen oder Prognosen bzw. der bloßen Annahme, dass verfassungsfeindliche Bestrebungen vorliegen, erfolgt.“[96]

Den Unterschied hat auch der Sächsische Verfassungsgerichtshof hervorgehoben:

> „§ 39 Abs. 1 Nr. 2 a SächsPolG steht in rechtsstaatlich unbedenklicher Weise darauf ab, daß Tatsachen – und nicht nur tatsächliche Anhaltspunkte – die Annahme rechtfertigen müssen, eine Person werde Straftaten von erheblicher Bedeutung begehen. Mit diesem tatbezogenen Ansatz wird in klarer und für den Bürger vorhersehbarer Weise sicher-gestellt, daß die vom Polizeivollzugsdienst zu treffende Prognoseentscheidung über die zukünftige Begehung bestimmter Straftaten stets nur auf hinreichend sicherer Faktenlage getroffen wird und nicht allein auf polizeilichem Erfahrungswissen und Vermutungen beruhen darf.“[97]

---

93 *Warg*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 13.
94 VG Frankfurt a.M. (5. Kammer), Urteil vom 1. Dezember 2014 – 5 K 2486/13.F, Rn. 24
95 VG Frankfurt a.M. (5. Kammer), Urteil vom 1. Dezember 2014 – 5 K 2486/13.F, Rn. 29.
96 VG Berlin, Urteil vom 25. September 2012 – 1 K 225.11, Rn. 43.
97 SächsVerfGH, Urteil vom 14. Mai 1996 – Vf. 44-II-94, Rn. 234.

Das angerufene Gericht verwendet zwar beide Begriffe teilweise synonym, allerdings nur mit dem Bezugspunkt einer „konkreten Gefahr“,[98] um die es unstreitig im G 10 *nicht* geht. § 1 Abs. 1 Nr. 1 G 10 lässt vielmehr eine „drohende Gefahr“ genügen. In § 3 Abs. 1 G 10 wird der Begriff der „tatsächlichen Anhaltspunkte“ mit dem „Verdacht“ der Planung oder Begehung einer Straftat verknüpft.

Es macht einen grundlegenden Unterschied, ob man „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Schutzgut“ als Eingriffsschwelle fordert oder lediglich „tatsächliche Anhaltspunkte für den Verdacht der Planung einer Straftat“ etwa nach § 130 StGB (Volksverhetzung) oder nach § 89a Abs. 2a StGB, des Unternehmens der Ausreise aus der Bundesrepublik zum Zwecke der Unterweisung in einem sog. „Terrorcamp“. Mithin sind die Begriffe „tatsächliche Anhaltspunkte“ vs. „bestimmte Tatsachen“ nicht isoliert zu lesen, sondern stets im entsprechenden Kontext, weil Sinnträger stets der ganze Normsatz ist.[99]

Wenn demgegenüber in Teilen des nachrichtendienstlichen Schrifttums aus BVerfGE 110, 33, 61 gefolgert wird, eine einengende, verfassungskonforme Auslegung des Begriffs der „tatsächlichen Anhaltspunkte“ (des § 39 Abs. 2 Satz 1 Nr. 2 AWG) sei möglich und dies könne man auf die Auslegung von § 3 G 10 übertragen,[100] so überzeugt das nicht, weil die Ausführungen des angerufenen Gerichts bei dieser Annahme aus dem Kontext gerissen werden:

In der zitierten Entscheidung erklärte das angerufene Gericht § 39 Abs. 1 und 2 AWG, der die Überwachung des Brief- und Telekommunikationsverkehrs zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz ermächtigte, als mit Art. 10 Abs. 1 und 2 Satz 1 GG unvereinbar. § 39 Abs. 2 Satz 1 AWG ermöglichte entsprechende Anordnungen, wenn „Tatsachen die Annahme rechtfertigen“, dass die von der Anordnung betroffenen Personen bestimmte Straftaten von erheblicher Bedeutung planen. § 39 Abs. 2 Satz 1 Nr. 2 AWG war eine Sondervorschrift für dritte Personen,

---

98 Vgl. BVerfGE 120, 274, 328: „Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen.“.

99 Vgl. dazu nur *Reimer*, Juristische Methodenlehre, 2. Aufl. 2020 Rn. 284; *Jakobs*, System der strafrechtlichen Zurechnung, 2012, S. 54: „Zudem ist es verfehlt (wenn auch geläufig), sich einen Tatbestand als eine Ansammlung von Gegenständen vorzustellen, die mit Worten bezeichnet werden, welche *je für sich* verständlich sind. Verständlich ist nur der *Zusammenhang*, nicht das einzelne Wort.“.

100 So *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 3 Rn. 6.

wonach Maßnahmen auch gegen Personen oder Personenvereinigungen, für die die verdächtige Person tätig ist, zulässig seinen

> „soweit *tatsächliche Anhaltspunkte* die Annahme rechtfertigen, dass die Person an dem Postverkehr der natürlichen oder juristischen Person oder Personenvereinigung teilnimmt oder deren Fernmeldeanschluss benutzt."
>
> (Hervorhebung diesseits)

In dieser Sondervorschrift wurde der Begriff der tatsächlichen Anhaltspunkte also gar nicht mit der Planung einer Straftat verknüpft, sondern mit der Benutzung eines Fernmeldeanschlusses. Folglich kann für die Auslegung des § 3 Abs. 1 G 10, bei dem es um die Planung von Straftaten geht, aus ihr nichts abgeleitet werden.

Das angerufene Gericht hat selbst an anderer Stelle eine entsprechende Differenzierung im Rahmen des G 10 vorgenommen. In BVerfGE 100, 313, 393 heißt es:

> „Ferner ist die tatsächliche Basis, die die Annahme eines Tatverdachts rechtfertigt, verglichen mit derjenigen, die etwa § 100 a StPO für Überwachungen der Telekommunikation fordert, relativ niedrig angesetzt. Während dort „bestimmte Tatsachen" den Verdacht begründen müssen, daß jemand Straftaten begeht oder, falls der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, genügen für die Übermittlung nach § 3 Abs. 5 in Verbindung mit Abs. 3 G 10 „tatsächliche Anhaltspunkte". Schließlich findet durch die Einbeziehung des Planungsstadiums, das dem strafbaren Versuch gemäß § 100 a StPO vorausliegt, eine Erstreckung der Übermittlung in ein kaum begrenztes Vorfeld der Begehung von Straftaten statt."

Im strafprozessualen Schrifttum wird entsprechend eindeutig differenziert: Bei § 100a StPO, der „bestimmte Tatsachen" als Verdachtsgrundlage fordert, handelt es sich um einen „qualifizierten Verdacht", ein mehr gegenüber dem strafprozessualen Anfangsverdacht i.S.d. § 152 Abs. 2 StPO; als Gegenbegriff wird oftmals der Begriff der „tatsächlichen Anhaltspunkte" verwendet.[101] Zudem unterscheidet der Wortlaut des § 100c StPO zwischen „bestimmten Tatsachen" in § 100c Abs. 1 Nr. 1 StPO einerseits sowie „tatsächlichen

---

101 *Greco*, in: SK-StPO, 5. Auflage 2016, § 100a Rn. 43: „Nach Absatz 1 Nr. 1 darf die Überwachung und Aufzeichnung von Telekommunikation –vergleichbar mit den §§ 100f Abs. 1, 100c Abs. 1 Nr. 1 – nur erfolgen, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer (…) eine in Absatz 2 bezeichnete schwere Straftat begangen hat (zu diesem qualifizierten Verdacht näher § 100f Rdn. 9; Wolter § 100c Rdn. 41): Vage, auch bloße tatsächliche Anhaltspunkte, kriminalistische Erfahrungen oder bloße Vermutungen reichen nicht aus".

Anhaltspunkten“ in Nr. 3 StPO andererseits. Die einfachgesetzlichen Regelungen zu (heimlichen) Überwachungsmaßnahmen haben mithin mittlerweile eine eindeutige Nomenklatur herausgebildet.

Der Grundsatz der Normenklarheit und Normenbestimmtheit verlangt daher jedenfalls bei einer speziellen Eingriffsgrundlage für die Quellen-TKÜ die Verwendung eines eindeutigen Tatbestandsmerkmals. Das angerufene Gericht hat hierzu für Überwachungsmaßnahmen ausgeführt:

> „Die Anforderungen an die Bestimmtheit und Klarheit der Norm dienen ferner dazu, die Verwaltung zu binden und ihr Verhalten nach Inhalt, Zweck und Ausmaß zu begrenzen (vgl. BVerfGE 56, 1 [12]; BVerfGE 110, 33 [54]). [….] Dem Gesetz kommt im Hinblick auf den Handlungsspielraum der Exekutive eine begrenzende Funktion zu, die rechtmäßiges Handeln des Staates sichern und dadurch auch die Freiheit der Bürger schützen soll. Dieser Aspekt der Bindung der Verwaltung ist bei einer Überwachungsmaßnahme besonders wichtig, da der Betroffene von ihr nichts weiß und daher keine Möglichkeit hat, in einem vorgeschalteten Verfahren Einfluss auf das eingreifende Verhalten der Verwaltung zu nehmen. Der Schutz durch begrenzende Maßstäbe erhält zusätzlich besondere Bedeutung dadurch, dass auch betroffene Dritte - hier die anderen Telekommunikationsteilnehmer, gegebenenfalls auch Kontakt- und Begleitpersonen - mit einer staatlichen Überwachung nicht rechnen und sich deshalb vor einem Einblick in ihren Privatbereich nicht schützen können (vgl. BVerfGE 110, 33 [54]).“[102]

Zudem hat das angerufene Gericht nach 2004 für geheime Überwachungsmaßnahmen durch Sicherheitsbehörden, die sich aus dem Grundgesetz ergebenden Anforderungen durch eine Vielzahl von Entscheidungen konkretisiert und insbesondere in dem *BKA-Urteil* in BVerfGE 141, 220 zusammengefasst.

Ausweislich des *BKA-Urteils* ist

> „Die Erhebung von Daten durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität (…) im Bereich der Gefahrenabwehr zum Schutz der genannten Rechtsgüter [Anm.: u.a. Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes] grundsätzlich nur verhältnismäßig, wenn eine Gefährdung dieser Rechtsgüter im Einzelfall hinreichend konkret absehbar ist und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist.“[103]

---

102 BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04, Rn. 118.

103 BVerfGE 141, 220, 271.

Diese Maßstäbe gelten, wie das angerufene Gericht jüngst noch einmal klargestellt hat, *auch* für Überwachungsmaßnahmen der Nachrichtendienste.[104]

Das angerufene Gericht hat im *BKA-Urteil* dabei einschränkend ausgeführt:

> „Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. [….] In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird. Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist.“[105]

Über diese vom angerufenen Gericht in den Blick genommenen Konstellationen, die im Übrigen bereits häufig strafprozessuale Überwachungsmaßnahmen sowie die Möglichkeit von Untersuchungshaft eröffnen würde,[106] geht allerdings § 3 Abs. 1 G 10 weit hinaus:

Nach dem Wortlaut des § 3 Abs. 1 Nr. 2 i.V.m. § 11 Abs. 1a G 10 und den dort in Bezug genommenen Straftatbestand des § 89a Abs. 2a StGB könnte eine geheime Überwachungsmaßnahme in Form der Quellen-TKÜ schon dann angeordnet werden, wenn „tatsächliche Anhaltspunkte“ dahingehend vorliegen, dass jemand plant, irgendwann ins Ausland zu reisen, um dort ein terroristisches Ausbildungslager zu besuchen und andere in Schusswaffen-Fertigkeiten zu unterweisen, ohne dass es für § 89a Abs. 2a Alt. 2 StGB einer darüber

---

104 BVerfGE 154, 152, 239; 155, 119, 189.

105 BVerfGE 141, 220, 272 f.

106 Der Besuch eines terroristischen Ausbildungslagers in jedem (auch außereuropäischen) Staat der Erde wäre nach deutschem Strafrecht strafbar, sofern die vorbereitete schwere Gewalttat im Inland begangen werden soll, §§ 89a Abs. 1 i.V.m. Abs. 2 Nr. 1, Abs. 3 StGB, es bedürfte nur einer Strafermächtigung gemäß § 89a Abs. 4. Reist also eine Person in die Bundesrepublik ein, der man nachweisen kann, dass sie ein Terrorcamp besucht hat und bzgl. der ein qualifizierter Anfangsverdacht bzgl. der Intention besteht, dass sie das Terrorcamp besucht hat, um später in der Bundesrepublik eine schwere staatsgefährdende Gewalttat zu begehen, wäre § 100a StPO eröffnet; bei dringendem Tatverdacht, auch ohne dass ein Haftgrund im technischen Sinne gemäß § 112 Abs. 2 StPO vorliegt, wäre auch Untersuchungshaft möglich, § 112 Abs. 3 StPO.

hinausgehenden Anschlagsabsicht bedarf.[107] Dies würde bedeuten, dass schon bei der Internet-Suche nach einem Flugticket und geringfügigen Indizien, dass der Käufer zu Ausbildungszwecken in ein Terrorcamp ausreisen will, eine Quellen-TKÜ gegen ihn angeordnet werden könnte. Diese Konstellation unterscheidet sich fundamental von denen des angerufenen Gerichts in BVerfGE 141, 220. Denn es handelt sich um einen viel längeren, noch gar nicht genauer absehbaren Kausalverlauf bis zu einem eventuellen Schaden in Form eines Anschlages, der teilweise zudem über fremde Willensentschlüsse vermittelt wird.[108] Damit liegt gerade in zeitlicher Hinsicht und damit auch im Hinblick auf die Frage einer Rechtsgutsgefährdung eine gänzlich andere Situation vor, als wenn ein ausgebildeter Kämpfer in die Bundesrepublik einreist, um einen Anschlag zu begehen.

Zudem muss die Katalogstraftat ausweislich des § 3 Abs. 1 G 10 lediglich „geplant" werden. Zu diesem Tatbestandsmerkmal hat das angerufene Gericht in der *Zollkriminalamt-Entscheidung* in BVerfGE 110, 33 plastisch ausgeführt:

> „Das Merkmal des Planens bringt hinsichtlich seines Beginns und seines Endes Klärungsbedarf mit sich. […] Eine Ermächtigung zur Straftatenverhütung unterscheidet sich hinsichtlich der Tatsachenlage, an die sie eine Maßnahme anknüpft, erheblich von Normen wie beispielsweise § 100 a StPO, die die Begehung einer Straftat, einen strafbaren Versuch oder eine strafbare Vorbereitung, mithin einen in der Vergangenheit liegenden, zumindest teilweise abgeschlossenen Sachverhalt voraussetzen. Die vorliegende Ermächtigung gilt nicht einmal zwingend einem schon in der Entwicklung begriffenen Vorgang, sondern bereits seiner Planung. Diese soll auf der Grundlage von Tatsachen feststellbar sein, die nicht auf die Gewissheit eines solchen Planens verweisen müssen; es reicht, wenn sie eine entsprechende „Annahme" rechtfertigen. § 39 Abs. 2 Satz 1 Nr. 1 AWG verlangt vom Zollkriminalamt daher schwerpunktmäßig eine Prognose künftiger Entwicklungen, die sich in wesentlichen Teilen noch in der Vorstellungswelt des potenziellen Straftäters abspielen. An die Stelle des bei der Strafverfolgung maßgebenden Verhaltens, das in einem gesetzlichen Straftatbestand umschrieben ist, tritt bei der Vorverlagerung des Eingriffs in das Planungsstadium ein zunächst meist nur durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichnetes, in der Bedeutung der beobachteten Einzelheiten häufig noch schwer fassbares

---

107 Vgl. dazu *Gazeas*, in: AnwKom-StGB, 3. Aufl. 2020, § 89a Rn. 74; *Sternberg-Lieben*, in: Schönke/Schröder, StGB, 20. Auflage 2019, § 89a Rn. 18; die Norm pönalisiert laut BGHSt 62, 102, 112 faktisch bereits „den Versuch der Vorbereitung zur Vorbereitung einer in § 89a Abs. 1 StGB genannten Gewalttat.".

108 Der präsumtive Ausreisewillige, dem der Verdacht zugeschrieben wird dort als Ausbilder zu fungieren, hat nach seinem Tatplan keinerlei Einfluss auf das „Ob" und „Wie" der Begehung von Terroranschlägen, dies liegt allein in der Hand der später Ausgebildeten.

> Geschehen. Die in Bezug genommenen Straftatbestände sind in diesem Stadium damit nur wenig geeignet, den maßgeblichen Sachverhalt einzugrenzen, der Indizien für eine geplante Straftat enthalten soll. Sachverhaltsfeststellung und Prognose sind mit vorgreiflichen Einschätzungen über das weitere Geschehen, aber auch über die erst noch bevorstehende strafrechtliche Relevanz der festgestellten Tatsachen verkoppelt. Die Feststellung des voraussichtlich weiteren Verlaufs ist auch dadurch erschwert, dass das Außenwirtschaftsrecht durch weit ausgreifende Gefährdungs- und Vorbereitungstatbestände gekennzeichnet ist, so dass der Eingriff in tatsächlicher wie rechtlicher Hinsicht in den Grenzbereich eines Verhaltens verlagert sein kann, das sich möglicherweise zu einer Rechtsgutverletzung weiterentwickelt, eventuell aber auch nicht."[109]

Diese Umstände treffen auch auf den Straftatenkatalog des § 3 Abs. 1 G 10 zu, der ebenfalls weit ausgreifende Gefährdungs- und Vorbereitungstatbestände enthält, namentlich etwa die §§ 80a[110], 83[111], 84 Abs. 1 und 2[112], 86[113], 87[114], 88[115], 89[116], 89a[117], 89b[118], 89c[119], 96[120], 98[121], 99 Abs. 1[122], 100[123], 100a Abs. 2[124], 109f[125] StGB. Wie oben bereits illustriert, eröffnet etwa § 3 Abs. 1 Nr. 2 G 10 i.V.m. § 89a Abs. 2a, 89b StGB exorbitant weite Überwachungsmöglichkeiten, wenn das Planungsstadium einbezogen wird:

---

109 BVerfGE 110, 33, 58.

110 Vgl. *Fischer*, StGB, 68. Aufl. 2021, § 80a Rn. 2, 2a; *Anstötz*, in: MüKo-StGB, 4. Aufl. 2021, § 80a Rn. 1.

111 Vgl. *Fischer,* StGB, 68 Auf. 2021, § 83 Rn. 1; *Anstötz* in: MüKo-StGB, 4. Aufl. 2021, § 83 Rn. 1.

112 Vgl. *Fischer*, StGB, 68. Aufla. 2021, § 84 Rn. 2; *Anstötz* in: MüKo-StGB, 4. Auflage 2021, § 84 Rn. 2, siehe auch BGH, Urteil vom 10.3.2005 – 3 StR 245/04.

113 Vgl. *Fischer*, StGB, 68. Aufl. 2021, § 86, Rn. 2 und 13; *Anstötz* in: MüKo-StGB, 4. Aufl. 2021, § 86 Rn. 2.

114 Vgl. *Fischer,* StGB, 68. Aufl. 2021, § 87 Rn. 2; *Anstötz* in: MüKo-StGB, 4. Aufl. 2021, § 87 Rn. 2, siehe auch BVerwG Urteil vom 24.2.2010 – 6 A 7.08; BT-Drs. V/2860, S. 10.

115 Vgl. *Fischer,* StGB, 68. Aufl. 2021, § 88 Rn. 2; *Anstötz* in: MüKo-StGB, 4. Aufl. 2021, § 88 Rn. 2.

116 Vgl. *Anstötz* in: MüKo-StGB, 4. Aufl. 2021, § 89 Rn. 2.

117 Vgl. *Fischer*, StGB, 68 Aufl. 2021, § 89a Rn. 3; *Anstötz/Schäfer* in: MüKo-StGB, 4. Aufl. 2021, § 89a Rn. 9.

118 Vgl. *Fischer*, StGB, 68. Aufl. 2021, § 89b Rn. 3; *Anstötz/Schäfer* in: MüKo-StGB, 4. Aufl. 2021, § 89b Rn. 7.

119 Vgl. *Fischer*, StGB, 68. Aufl. 2021, § 89c Rn. 1; *Anstötz/Schäfer* in: MüKo-StGB, 4. Aufl. 2021, § 89c Rn. 3.

120 Vgl. *Fischer,* StGB, 68. Aufl. 2021, § 96 Rn. 1; *Hegmann/Stuppi* in: MüKo-StGB, 4. Aufl. 2021, § 96 Rn. 1.

121 Vgl. *Fischer*, StGB, 68. Auf. 2021, § 98 Rn. 1; *Hegmann/Stuppi* in: MüKo-StGB, 4. Aufl. 2021, § 98 Rn. 1.

122 Vgl. *Fischer*, StGB, 68. Aufl. 2021, § 99 Rn. 3; *Hegmann/Stuppi* in: MüKo-StGB, 4. Aufl. 2021, § 99 Rn. 3; siehe auch BGHSt 29, 325, 335.

123 Vgl. *Hegmann/Stuppi* in: MüKo-StGB, 4. Aufl. 2021, § 100 Rn. 2.

124 Vgl. *Fischer,* StGB, 68. Aufl. 2021, § 100a Rn. 7; *Hegmann/Stuppi*, in: MüKo-StGB, 4. Aufl. 2021 § 100a Rn. 10.

125 Vgl. *Fischer*, StGB, 68. Aufl. 2021, § 109f Rn. 1; *Müller*, in: MüKo-StGB, 4. Aufl. 2021, § 109f Rn. 2; siehe auch BGHSt 23, 308, 311.

Nach § 89c Abs. 1 StGB ist es bereits strafbar, wenn jemand Vermögenswerte mit dem Wissen oder in der Absicht sammelt, dass diese von einer anderen Person zur Begehung etwa einer Geiselnahme (§ 239b StGB i.V.m. § 89a Abs. 1 Nr. 2 StGB) oder zur Zerstörung wichtiger Arbeitsmittel (§ 305 i.V.m. § 89a Abs. 1 Nr. 3 StGB) verwendet werden sollen. Die Verknüpfung dieser extrem weiten Strafvorschrift, gegen die auch schon der Vorwurf des Gesinnungsstrafrechts erhoben worden ist,[126] mit einem bloßen Planungsstadium führt dazu, dass isoliert absolut neutrale Handlungen die Befugnis zur Vornahme einer heimlichen Überwachungsmaßnahme (einschließlich der Quellen-TKÜ) nach dem G 10 böten. In dem vorgenannten Beispielsfall würde eine irgendwie verdächtig anmutende Eröffnung eines Kontos genügen oder die Erstellung einer Liste, auf welchen Veranstaltungen Personen nach einer Spende gefragt werden sollen oder gar die Recherche im Internet, auf welchem Wege Spendengelder, die erst gesammelt werden sollen, an den Adressaten ins Ausland transferiert werden können. All dies sind Planungshandlungen. In allen Fällen „plant" der Betreffende die Begehung einer Straftat nach § 89c Abs. 1 StGB.

c. Keine Anpassung der verfassungsrechtlich notwendigen rechtlichen Eingriffsschwellen an die Quellen-TKÜ

Durch die gewählte Form der Neuregelung der Verfahrens-Norm des § 11 G 10[127] wird die Festlegung der Schutzgüter und Tatbestandsvoraussetzungen in § 3 G 10 pauschal übernommen. Insoweit entsprechen der Straftatenkatalog und die weiteren Tatbestandsvoraussetzungen, die die nunmehr neu eingeführte Quellen-TKÜ legitimieren sollen, nicht den verfassungsrechtlichen Anforderungen. § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 verstoßen damit gegen den Grundsatz der Verhältnismäßigkeit i.F.d. Angemessenheit. Sie verstoßen zudem gegen den verfassungsrechtlichen Bestimmtheitsgrundsatz i.V.m. dem Erfordernis der Normenbestimmtheit und Normenklarheit, die unmittelbar aus Art. 10 Abs. 1 GG folgen.[128]

aa. Unzureichende rechtliche Eingriffsschwelle für die Quellen-TKÜ – der Straftatenkatalog des § 3 Abs. 1 G 10 i.V.m. § 1 Abs. 1 G 10

Der Straftatenkatalog des § 3 Abs. 1 G 10 ist sehr weitgehend.[129] Dieser wurde mit der Einführung der Quellen-TKÜ und der beschränkten Online-

126 *Paeffgen*, in: NK-StGB, 5. Aufl. 2017, § 89c Rn. 7.

127 § 11 G 10 findet sich in Abschnitt 4 „Verfahren" des Artikel 10-Gesetzes.

128 BVerfGE 110, 33, 52.

129 *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, S. 14 f.; *Poscher*, Stellungnahme zu dem Entwurf der Bundesregierung eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Mai 2021, S. 8 f.; *Rusteberg*,

Durchsuchung im G 10 nicht geändert, sondern verblieb in seiner bisherigen Form. Er umfasst auch Vorfeldtatbestände, deren bevorstehende Verwirklichung nicht zwingend auf eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut wie Leben, Leib und Freiheit der Person rekurriert.[130] Im Straftatkatalog finden sich neben Erfolgsdelikten auch Gefährdungstatbestände, die Handlungen weit im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor.

Das angerufene Gericht hat für die Telekommunikationsüberwachung zu Zwecken der Strafverfolgung die Verfolgung von Straftaten mit einer Höchstfreiheitsstrafe von fünf Jahren als hinreichend gewichtig akzeptiert, wobei auch im Einzelfall eine besondere Schwere gegeben sein muss.[131]

Im Hinblick auf den in Bezug genommenen Straftatenkatalog verstoßen zumindest die folgenden Straftatenbezüge gegen den Grundsatz der Verhältnismäßigkeit, weil der mit der heimlichen Überwachung im Wege der Quellen-TKÜ einhergehende Grundrechtseingriff nicht mehr verhältnismäßig ist.

bb. § 3 Abs. 1 Nr. 2 i.V.m. § 20 VereinsG

Unvereinbar ist die Aufnahme von § 20 Abs. 1 - 4 VereinsG, der lediglich eine Höchststrafe von einem Jahr vorsieht.[132] Bei der Zuwiderhandlung gegen ein Vereinsverbot handelt sich demnach um einen Auffangtatbestand im Bagatellbereich.[133] Der Strafrahmen von bis zu einem Jahr Freiheitsstrafe ist nicht nur der niedrigste Strafrahmen für Freiheitsstrafen in Straftatbeständen; er entspricht dem der einfachen Beleidigung (§ 185 StGB). Die Planung und selbst die Begehung dieser Straftat kann eine so grundrechtsinvasive Maßnahme wie die Quellen-TKÜ nicht rechtfertigen.

cc. § 3 Abs. 1 Nr. 6 lit. a i.V.m. § 130 StGB

Die pauschale Einbeziehung des Volksverhetzungstatbestandes ist zu weitgehend, um eine heimliche Überwachungsmaßnahme durch einen

---

Stellungnahme zur Vorbereitung der öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, 15. Mai 2021, S. 17.

130 Siehe BVerfGE 141, 220, 270: „Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig. Hierzu gehören Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes“.

131 BVerfGE 129, 208, 243 ff.

132 *Bäcker*, in: Dietrich/Gärditz/Graulich/Gusy/Warg, Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 146; krit. auch *Roggan*, in: NOMOS-G 10, 2018, § 3 Rn. 10.

133 *Wache*, in: Erbs/Kohlhaas, 234. EL Januar 2021, VereinsG, § 20 Rn. 1.

Nachrichtendienst im Wege der Quellen-TKÜ zu rechtfertigen. Bei § 130 Abs. 1 StGB handelt es sich um ein bloß potenzielles Gefährdungsdelikt. Hier gilt,

> „dass also […] die Herbeiführung einer auch nur entfernten Gefahr für die allgemeine Rechtssicherheit oder das Friedensgefühl der Bevölkerung zur Erfüllung dieses Tatbestandsmerkmales ausreicht, ohne dass eine tatsächliche Störung des Friedens erforderlich ist.“[134]

Bereits die bloße Planung des Aufhängens von Plakaten, der Kauf der Bestandteile dafür, die Herstellung sowie wie die Anfertigung einer Schablone zur Erstellung eines volksverhetzenden Plakates könnten unter § 3 Abs. 1 Nr. 6 lit. a Alt. 2, § 130 Abs. 1 StGB subsumiert werden.

Zwar müssen für eine Überwachungsmaßnahme zusätzlich die Voraussetzungen des § 1 Abs. 1 Nr. 1 G 10 vorliegen, dass die Überwachung zudem dazu dient, Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes, eines Landes oder der in Deutschland stationierten NATO-Truppen abzuwehren. Dieses weitere Erfordernis begrenzt allerdings die Eingriffsbefugnis kaum: Denn zur freiheitlich demokratischen Grundordnung gehört als Kernelement die Achtung vor der Menschenwürde und den im Grundgesetz konkretisierten Menschenrechten.[135] Gerade diese wird indes durch das mit § 130 Abs. 1 StGB inkriminierte Verhalten angegriffen.

Die § 3 Abs. 1 i.V.m. § 1 Abs. 1 G 10 enthalten demgegenüber anders als § 100a StPO Nr. 2 StPO keine sog. Tatschwereklausel, setzen also nicht voraus, dass die “Tat auch im Einzelfall schwer wiegt“. Für die repressive Telekommunikationsüberwachung wurde durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007[136] diese zusätzliche Anordnungsvoraussetzung ins Gesetz aufgenommen. Damit wurde den Anforderungen der neueren verfassungsgerichtlichen Rechtsprechung Rechnung getragen.[137] Auf diese Weise sollen jene Sachverhalte ausgeschieden werden, welche zwar dem Anlasstatenkatalog grundsätzlich unterfallen, jedoch mangels hinreichender Schwere im konkreten Einzelfall den mit einer (*notabene* „normalen“) Telekommunikationsüberwachung verbundenen Eingriff in das Fernmeldegeheimnis nicht zu rechtfertigen vermögen.

Auch die Einbeziehung des § 130 Abs. 4 StGB ist vor diesem Hintergrund nicht mehr verhältnismäßig. Die Vorschrift schützt den öffentlichen Frieden. Die

---

134 OLG Stuttgart, Urteil vom 19. Mai 2009 – 2 Ss 1014/09, Rn. 22; ebenso BGHSt 46, 212.

135 BVerfGE 2, 1, 12 f.; *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI § 4 Rn. 34.

136 BGBl. 2007 I, S. 3198.

137 Vgl. BVerfGE 109, 279, 346; 115, 166, 197 f.; 129, 208.

Befürwortung der nationalsozialistischen Gewaltherrschaft ist in Deutschland ein Angriff auf die Identität des Gemeinwesens nach innen mit friedensbedrohendem Potential. Wie das BVerfG ausgeführt hat, ist das

> „Ziel […] der Schutz vor Äußerungen, die ihrem Inhalt nach erkennbar auf rechtsgutgefährdende Handlungen hin angelegt sind, das heißt den Übergang zu Aggression oder Rechtsbruch markieren. Die Wahrung des öffentlichen Friedens bezieht sich insoweit auf die Außenwirkungen von Meinungsäußerungen etwa durch Appelle oder Emotionalisierungen, die bei den Angesprochenen Handlungsbereitschaft auslösen oder Hemmschwellen herabsetzen oder Dritte unmittelbar einschüchtern. […] Es geht um einen vorgelagerten Rechtsgüterschutz, der an sich abzeichnende Gefahren anknüpft, die sich in der Wirklichkeit konkretisieren.“[138]

Bereits im Stadium der Planung einer solchen Straftat eine Zielperson bereits nachrichtendienstlich mittels Quellen-TKÜ heimlich zu überwachen, verstößt ebenso gegen den Grundsatz der Verhältnismäßigkeit. Nach der derzeit geltenden Gesetzesfassung kann bereits im Stadium der Planung von Inhalten einer volksverhetzenden Rede nach § 130 Abs. 4 StGB eine Quellen-TKÜ angeordnet werden. Der Kausalverlauf, bis es zu einer konkreten Gefährdung oder Verletzung hochrangiger Rechtsgüter kommt, ist zu diesem Zeitpunkt noch ein enorm langer und unabsehbarer. Wenn demgegenüber im nachrichtendienstlichen Schrifttum der Straftatbestand des § 130 Abs. 4 StGB dahingehend charakterisiert wird, dass in ihm ein „teils lebensbedrohliches Gefährdungspotenzial steckt“,[139] so spiegelt sich dies zumindest nicht im Strafrahmen wieder, der nur bis zu drei Jahren Freiheitsstrafe reicht. Der Strafrahmen entspricht damit dem einer einfachen Nötigung (§ 240 StGB) oder Unterschlagung (§ 246 StGB). [140] Eine Körperverletzung wird in der gesetzgeberischen Wertung mit einem Strafrahmen von bis zu fünf Jahren Freiheitsstrafe als gewichtigere Straftat bewertet.

dd. § 3 Abs. 1 Nr. 2 G 10 i.V.m. § 86 StGB

Katalogstraftat ist auch das abstrakte Gefährdungsdelikt[141] des Verbreitens von Propagandamitteln verfassungswidriger Organisationen. Anders als die gesetzliche Überschrift suggeriert, genügt als Tathandlung auch das Vorrätig-

---

138 BVerfGE 123, 300, 335.

139 *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 3 Rn. 3.

140 Kritisch auch *Roggan* in: NOMOS-G10, 2018, § 3 Rn. 10 mit Verweis auf den Strafrahmen von lediglich bis zu drei Jahren.

141 *Paeffgen*, in: NK-StGB, 5. Auflage 2017, § 86 Rn. 2; *Sternberg-Lieben*, in: Schönke/Schröder, 30. Auflage 2019, § 86 Rn. 1.

Halten zum Verbreiten.[142] Dann genügt für eine Überwachung unter Einbeziehung des Planungsstadiums etwa auch das Sich-Bemühen um Druckplatten für SS-Runen etc., um mit diesen entsprechende Propagandamittel herzustellen und zu verbreiten. Auch eine Quellen-TKÜ in diesem Fall hält einer verfassungsrechtlichen Prüfung nicht stand und verstößt gegen den Grundsatz der Verhältnismäßigkeit. Besonders gewichtige Rechtsgüter wie Leben, Leib, Freiheit der Person etc. werden durch diese Verhaltensweisen nicht einmal abstrakt gefährdet.

ee. § 3 Abs. 1 Nr. 2 G 10 i.V.m. § 89a, 89b, 89c StGB

Die vorbehaltlose Einbeziehung der §§ 89a, 89b und § 89c StGB überdehnt ebenso die Grenze des verfassungsrechtlich Zulässigen im Hinblick auf eine Überwachungsmaßnahme nach § 3 Abs. 1 G 10.

Für die Planung der Ausreise gem. § 89a Abs. 2a StGB, die des Sammelns von Vermögenswerten i.S.d. § 89c StGB, wurde dies schon mit Beispielen illustriert.[143] Zur Veranschaulichung sollen noch für zwei weitere Tatbestandskonstellationen beispielhaft skizziert werden, um die Weite der Überwachungsbefugnis zu verdeutlichen:

Nach § 89a Abs. 1, Abs. 2 Nr. 3 StGB macht sich unter anderem strafbar, wer sich Stoffe beschafft, um daraus Mittel für einen terroristischen Anschlag herzustellen. Erfasst sind insbesondere auch vielfältig nutzbare Stoffe, deren deliktischer Bezug sich erst aus den Vorstellungen des Handelnden ergibt.[144] Der Kauf von Unkrautvernichtungsmittel mit dem Ziel, daraus eine explosionsfähiges Mittel zu machen, erfüllt etwa den Straftatbestand. In der Folge können gem. § 3 Abs. 1 G 10 Nachrichtendienste die Telekommunikation einer Person bereits dann überwachen, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass diese Person plant, Unkrautvernichtungsmittel zu kaufen, etwa indem sie im Internet nach Händlern für Unkrautvernichtungsmittel sucht. Dies wäre bereits ein „Planen" i.S.d. § 3 Abs. 1 G 10. Auf welcher Grundlage ein solcher Verdacht fußen könnte, bleibt offen. Fast zwangsläufig wird es sich hierbei vor allem um vage und wenig aussagekräftige Faktoren wie die persönlichen, politischen oder religiösen Überzeugungen und sozialen Beziehungen des Betroffenen handeln, die für eine verfassungsrechtlich tragfähige Schadensprognose jedoch nicht ausreichen:

---

142 Siehe nur *Paeffgen*, in: NK-StGB, 5. Auflage 2017, § 86 Rn. 34.

143 Siehe oben bei und nach Fn.105.

144 Siehe zu den Auslegungsschwierigkeiten der Vorschrift nur *Gazeas*, in: HK-StGB, 3. Auflage 2020, § 89 a Rn. 60: „Diese Tatvariante stellt die Vorbereitung einer Tat nach Abs. 2 Nr. 2 unter Strafe und geht damit bedenklich weit ins Vorfeld einer späteren schweren staatsgefährdenden Gewalttat („*Vorbereitung der Vorbereitung*"). Der Gesetzgeber hatte hier insbesondere das Geschehen um die sog. *Sauerland-Gruppe*, die u.a. Wasserstoffperoxid in beträchtlichen Mengen zur Vorbereitung eines Anschlags aufbewahrte, vor Augen."

> „Dagegen wird dem Gewicht eines Eingriffs durch heimliche polizeirechtliche Überwachungsmaßnahmen nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weiter in das Vorfeld einer in ihren Konturen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird. Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur relativ diffuse Anhaltspunkte für mögliche Gefahren bestehen. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet (vgl. BVerfGE 120, 274 [329]; vgl. auch BVerfGE 110, 33 [59]; 113, 348 [377]). Solche Offenheit genügt für die Durchführung von eingriffsintensiven heimlichen Überwachungsmaßnahmen nicht. Nicht ausreichend für solche Maßnahmen ist insoweit etwa allein die Erkenntnis, dass sich eine Person zu einem fundamentalistischen Religionsverständnis hingezogen fühlt.“[145]

§ 89b StGB, die Aufnahme von Beziehungen zur Begehung einer schweren staatsgefährdenden Gewalttat, gehört ebenso zum Katalog des § 3 Abs. 1 Nr. 2 G 10. Damit soll u.a. folgender (Beispiels-)Fall unter Strafe gestellt werden:

A will ein Ausbildungslager im mittleren Osten aufsuchen, um anschließend in den Dschihad zu ziehen, ohne dabei eine bestimmte terroristische Vereinigung zu unterstützen. Dazu setzt er sich telefonisch mit *B* in Verbindung, einem flüchtigen Kontakt aus der Moschee, von dem er glaubt, dass dieser Kontakte zur islamistischen Szene habe. Zum Besuch des Ausbildungslagers kommt es nicht mehr.[146]

Es handelt sich bei § 89b StGB um eine Vorbereitungstat zu § 89 Abs. 2 Nr. 1 StGB, dem Unterweisen und Sich-Unterweisen-Lassen im Umgang mit gefährlichen Gegenständen, der wiederum Vorbereitungstat zur Herstellung bzw. zum Umgang mit diesen Gegenständen i.S.d. § 89a Abs. 2 Nr. 2 StGB ist, was schließlich in Vorbereitung auf die spätere Gewalttat geschieht („Vorbereitung der Vorbereitung der Vorbereitung”).[147] Wenn nunmehr zudem noch die Planung dieser „Vorbereitung der Vorbereitung der Vorbereitung“ für eine Überwachungsmaßnahme nach § 3 Abs. 1 G 10 genügt, könnte die Frage etwa in einer Hinterhofmoschee, wie man Kontakt zu Mittelspersonen erhalten kann, die einem eine Reise in ein terroristisches

---

145 BVerfGE 141, 220, 273.

146 Siehe *Gazeas/Grosse-Wilde/Kießling*, NStZ 2009, 593, 601.

147 *Gazeas/Grosse-Wilde/Kießling* NStZ 2009, 593, 601.

Ausbildungslager vermitteln, ebenso hinreichend sein, wie die Frage, was man von solchen Überlegungen, mal mit jemandem Kontakt aufzunehmen, halte. Gemessen an dem verfassungsrechtlichen Maßstab in der BKA-Entscheidung ist eine Quellen-TKÜ in diesem Fall auf dieser Verdachtslage unverhältnismäßig.[148]

ff. § 3 Abs. 1 Nr. 7 G 10 i.V.m. § 95 Abs. 1 Nr. 7 AufenthaltsG

Katalogtat ist auch ein Verstoß gegen § 95 Abs. 1 Nr. 7 AufenthaltsG, die Zugehörigkeit zu einer geheimen Gruppe oder Vereinigung. Der Strafrahmen beträgt lediglich bis zu einem Jahr und ist damit mit einer einfachen Beleidigung, (§ 185 StGB) vergleichbar. Die Strafvorschrift wird überdies jedenfalls praktisch als unbedeutend bezeichnet.[149] Der Verdacht der Planung oder der Begehung eines solchen Bagatell-Delikts rechtfertigt nach der verfassungsrechtlichen gefestigten Rechtsprechung keine Überwachungsmaßnahme nach § 3 Abs. 1 G 10, auch wenn ein entsprechendes Informationsinteresse der Behörden an solche Gruppen bestünde.

gg. § 3 Abs. 1 Satz 2 G 10 (Mitglied einer Vereinigung)

Auch § 3 Abs. 1 Satz 2 G 10 ermöglicht eine Telekommunikationsüberwachung bereits weit im Vorfeld konkreter Gefahren. Der Verdacht der Mitgliedschaft in einer Vereinigung kann bereits bestehen, wenn die genauen Ziele und das Gefährdungspotenzial der Vereinigung noch weitgehend unbekannt sind. Die Norm lässt hierbei bereits einen strafrechtlich relevanten Zweck der Vereinigung genügen. Anhaltspunkte für bereits begangene Straftaten sind danach nicht erforderlich. Der in § 3 Abs. 1 Satz 2 G 10 enthaltene Eingriffstatbestand schränkt zudem den Kreis der Straftaten nicht ein, auf welche die Zwecke oder die Tätigkeit der mutmaßlichen Vereinigung gerichtet sein müssen. Eine Überwachung im Wege der Quellen-TKÜ ist in der Folge auch an den Verdacht der Mitgliedschaft in einer Vereinigung geknüpft, von der lediglich minder schwere Straftaten wie Beleidigungen oder einfache Sachbeschädigungen erwartet werden, sofern diesen Straftaten allein eine verfassungsfeindliche Motivation zugrunde liegt.[150] Es ist unschwer zu erkennen, dass diese Vorschrift

---

148 S. BVerfGE 141, 220, 310.

149 *Fahlbusch*, in: NK-AuslR, 2. Auflage 2016, AufenthG § 95 Rn. 169: „Zu Abs. 1 Nr. 8 liegt keine veröffentlichte Rechtsprechung vor. Dies lässt sich nur damit erklären, dass der Vorschrift keine praktische Bedeutung zukommt.“.

150 Siehe *Löffelmann* in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VI § 4, Rn. 40. – Vgl. bspw. BGH (3. Strafsenat), Urteil vom 20.08.2020 – 3 StR 40/20 mit Vorinstanz LG Koblenz, Urteil vom 16.07.2019 – 2090 Js 29752/10 12 KLs: Nach den vom LG getroffenen Feststellungen besprühten der Angeklagte und seine Komplizen in der Nacht vom 19. auf den 20.07.2011, um Propaganda für ihre politische Anschauung zu betreiben, vier Schulgebäude mit zahlreichen Graffitiparolen an, so etwa mit "Hitzefrei statt Völkerbrei", "Die Deutsche Jugend wehrt sich" und "Bad G. bleibt deutsch". Das LG Koblenz hatte die Angeklagten deswegen wegen gemeinschädlicher Sachbeschädigung (§ 304 StGB) verurteilt, der

die Befugnisse zur Telekommunikationsüberwachung von der durch den Straftatenkatalog des § 3 Abs. 1 Satz 2 G 10 beabsichtigten Einhegung (u.a. § 3 Abs. 1 Nr. 6 lit. a i.V.m. § 129a StGB) weitgehend ablöst.[151]

d. Keine wirksame Begrenzung der Ermächtigungsgrundlage durch den Begriff der „drohenden Gefahr" in § 1 Abs. 1 G 10

Schließlich vermag auch das Erfordernis der drohenden Gefahr in § 1 Abs. 1 Nr. 1 G 10 die Ermächtigungsgrundlage in § 3 G 10 nicht auf ein angemessenes Maß zu beschränken. Es ist allgemeine Meinung, dass der Begriff nicht als konkrete Gefahr im polizeirechtlichen Sinne auszulegen ist, sondern allgemeine Gefahrenlagen bereits im Vorfeld konkreter Gefahren umfasst.[152] Diese Vorfeldaufklärung gehört zur klassischen Aufgabe der Nachrichtendienste. Teilweise wird der Begriff auch dahingehend verstanden, dass bereits die entfernte Möglichkeit eines Schadenseintritts ausreicht.[153] In seinem Urteil zur Vorratsdatenspeicherung fordert das angerufene Gericht für die Verfassungsmäßigkeit eines Eingriffs in das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG durch die Gefahrenabwehrbehörden auf der einen und die Nachrichtendienste auf der anderen Seite das Vorliegen derselben Voraussetzungen: Die gesetzliche Ermächtigungsgrundlage müsse zumindest „tatsächliche Anhaltspunkte einer konkreten Gefahr" für die zu schützenden Rechtsgüter verlangen.[154] Demgegenüber geht es bei der „drohenden Gefahr" gemäß § 1 Abs. 1 G 10 der Sache nach um bloße Gefahrenvorbeugung. Polizeirechtlich ließe sich die „drohende Gefahr" am ehesten mit der – begrifflich immer noch unscharfen – „allgemein bestehenden Gefahr" vergleichen.[155]

e. Schlussfolgerung

Die Kombination der unbestimmten Tatbestandsmerkmale „tatsächliche Anhaltspunkte", „Planung einer Straftat", „drohende Gefahr" und der extrem weite Straftatenkatalog des § 3 G 10 genügen nicht dem

---

BGH bemängelte, dass das Landgericht in der Strafzumessung nicht die gemäß § 46 Abs. 2 StGB zu beachtenden fremdenfeindlichen, rassistischen oder sonstigen menschenverachtenden Beweggründe und Ziele der Angeklagten berücksichtigt hatte. Ggfls. könnte man eine solche Vereinigung daher unter § 3 Abs. 1 Satz 2 i.V.m. § 1 Abs. 1 Nr. 1 G 10 subsumieren, eine drohende Gefahr für die freiheitliche demokratische Grundordnung könnte sich aus der rechtsextremen Motivation ergeben.

151 *Löffelmann* in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI § 4, Rn. 40.

152 *Roggan*, in: NOMOS-G 10, 2018, § 1 Rn. 4; *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, G 10, § 1 Rn. 33; *Löffelmann* in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI § 4, Rn. 33.

153 *Borgs*: in: Borgs/Ebert, § 1 Rn. 4.

154 BVerfGE 125, 260, 330.

155 *Roggan*, in: NOMOS-G 10, 2018, § 1 Rn. 6.

Verhältnismäßigkeitsgrundsatz. Das angerufene Gericht hat in seiner Entscheidung BVerfGE 100, 313 die Eingriffsschwellen des tatsächlich-prognostischen Gefahrurteils einerseits und der zu schützenden Rechtsgüter andererseits in der Sache als kommunizierende Röhren charakterisiert:

> „Soweit es um die Verhinderung von Straftaten geht, wird die Regelung den grundrechtlich geschützten Interessen nicht gerecht. Zusammengenommen führen die Umstände, daß als Verdachtsbasis tatsächliche Anhaltspunkte ausreichen, daß bereits an das Planungsstadium angeknüpft wird und daß auch minderschwere Straftaten einbezogen werden, zu einer deutlichen Unausgewogenheit zu Lasten der betroffenen Grundrechte. Insbesondere bewirkt die Verknüpfung tatsächlicher Anhaltspunkte mit der Planung von Straftaten, daß die Befugnis weit im Vorfeld einer drohenden Verletzung des Rechtsguts - mit der Folge einer Herabsetzung des Wahrscheinlichkeitsgrades und der Prognosesicherheit - ansetzen und sich zugleich auf verhältnismäßig niedrige Anforderungen an die Tatsachengrundlage stützen darf.
> Der Gesetzgeber kann daher nicht an allen Elementen der Übermittlungsregelung zur Straftatenverhinderung gleichzeitig festhalten. Nimmt man die vom Gesetzgeber gewählte Tatsachenbasis und die Vorverlagerung in das Planungsstadium zusammen mit dem Straftatenkatalog, der die Verwendung der Erkenntnisse des Bundesnachrichtendienstes rechtfertigt, so können die beiden ersten Voraussetzungen nur bei einem weiter beschränkten Katalog verfassungsmäßig sein. Umgekehrt läßt sich der Umfang des Katalogs nur bei höheren Anforderungen an die Sicherheit der Prognose rechtfertigen. Überdies kann das Tatbestandsmerkmal „tatsächlicher Anhaltspunkt“ den verfassungsrechtlichen Anforderungen im Ansatz nur genügen, wenn eine einengende Auslegung sicherstellt, daß nicht im wesentlichen Vermutungen, sondern konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorliegen.”[156]

So verhält es sich auch in der vorliegenden Konstellation: Die Ermächtigungsgrundlage zur Quellen-TKÜ in § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 1 G 10 kombiniert zu niedrige Eingriffsschwellen sowohl für die Gefahrenschwelle als auch für die zu schützenden Rechtsgüter. Damit verstößt sie gegen den Grundsatz der Verhältnismäßigkeit.

f. Zur enormen potenziellen Reichweite des Telekommunikationsbegriffs und des veränderten Nutzerverhaltens – Auswirkungen auf die Verhältnismäßigkeit und Bestimmtheit

156 BVerfGE 100, 313, 395.

Die Ermächtigungsgrundlage zur Quellen-TKÜ in § 1 Abs. 1 Nr. 1 i.V.m. § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 1 G 10 verstößt mit der unklaren Reichweite zur Überwachung und Aufzeichnung der „Telekommunikation" gegen den Verhältnismäßigkeitsgrundsatz sowie gegen das Gebot der Normenklarheit und Bestimmtheit.

Der Gesetzgeber ist insbesondere vor dem Hintergrund eines geänderten Nutzerverhaltens gehalten, den Begriff der Telekommunikation einschränkend-klarstellend genauer gesetzlich zu bestimmen. Für den Normanwender ist in der gegenwärtigen Rechtslage nicht hinreichend klar voraussehbar, welches Verhalten von der Norm umfasst wird und welches nicht.

aa. Die Nutzung von Cloud-Diensten als neuer Standard

(a) Historische Entwicklung seit 2008

Seit der Begründung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Jahre 2008[157] hat sich das IT-Nutzungsverhalten der Bürgerinnen und Bürger massiv gewandelt. Im Jahr 2008 existierten die meisten heute populären Cloud-Speicherdienste wie z.B. *iCloud*[158], *Microsoft OneDrive*[159] und *Dropbox*[160] noch nicht oder waren noch nicht nennenswert verbreitet. Während im Jahre 2008 ein IT-Systemnutzer seine Daten im Regelfall nur lokal auf seinen Endgeräten gespeichert hatte, ist mittlerweile die Nutzung von sog. Cloud-Speicherdiensten zum neuen Standard geworden. So gaben bei einer Umfrage im Jahr 2021 82 % der befragten Unternehmen an, Cloud-Dienste in Anspruch zu nehmen.[161] Im privaten Bereich nutzen einer Umfrage aus dem Jahre 2019 zufolge 51 % der Befragten einen Cloud-Speicher.[162] Diese Zahl dürfte in den letzten drei Jahren auch durch die beschleunigte technische Entwicklung in der Pandemie und die erhebliche Erhöhung des dislokalen Arbeitens noch einmal deutlich gestiegen sein. Hierin liegt eine gravierende Änderung des IT-Nutzerverhaltens der Bundesbürger.

---

157 BVerfGE 120, 274 ff.

158 Apple, Apple stellt iCloud vor, 6. Juni 2011, abrufbar unter https://www.apple.com/de/newsroom/2011/06/06Apple-Introduces-iCloud/; zuletzt abgerufen am 8. Juli 2021.

159 PC- Magazin, SkyDrive: So funktioniert der Cloud-Speicher von Microsoft, abrufbar unter https://www.pc-magazin.de/ratgeber/harmonischer-dreiklang-1504992.html, zuletzt abgerufen am 8. Juli 2021.

160 Dropbox, Dropbox hits 1.0, 16. Dezember 2010, abrufbar unter https://blog.dropbox.com/topics/product/dropbox-hits-1-0, zuletzt abgerufen am 8. Juli 2021.

161 Bitkom Research, Cloud-Monitor 2021, abrufbar unter https://www.bitkom-research.de/system/files/document/Bitkom_KPMG_Charts_Cloud%20Monitor%202021_final.pdf; zuletzt abgerufen am 8. Juli 2021.

162 Forsa, Cloud-Studie im Auftrag von Strato, abrufbar unter https://www.strato.de/cloud-speicher/studie/, zuletzt abgerufen am 8. Juli 2021.

(b) Zur technischen Funktionsweise von Cloud-Diensten

Cloud-Speicherdienste speichern die vom Nutzer übermittelten Daten auf ihren eigenen Servern ab. Die Daten befinden sich also nicht, wie umgangssprachlich oft ausgedrückt, in der nicht greifbaren „Cloud" in einer „Wolke", sondern vereinfacht gesagt nur auf einer Festplatte des Cloud-Dienste-Anbieters. Cloudspeicherdienste erfreuen sich dabei zentral aus zwei Gründen ihrer großen Beliebtheit im privaten wie auch im unternehmerischen Bereich: Zum einem bieten sie den Vorteil, dass alle Daten immer auf allen Endgeräten in der aktuellsten Version verfügbar sind. Zum anderen schützen sie den Nutzer vor mit einem Verlust oder einer Störung des Endgeräts verbundenen Datenverlusten.

Die praktische Verwendung von Cloud-Speicherdiensten erfolgt dabei regelmäßig so, dass der Nutzer auf seinen Endgeräten, das auch ein Smartphone sein kann, ein Programm installiert, das die Synchronisation der Daten auf dem Endgerät und den Daten in der Cloud steuert. Der Nutzer kann dabei auswählen, ob er seine gesamte Festplatte oder nur einzelne Ordner mit der Cloud und damit mit seinen anderen Endgeräten synchron halten möchte. Als Standarteinstellungen sehen die Programme auf PCs oder Smartphones oft die Synchronisation des zentralen Dokumentenordners sowie der Fotodateien vor. Das Hin- und Herschicken der Dateien wird dabei durch das Programm ausgeführt, ohne dass der Nutzer dies unmittelbar in jedem Einzelfall selbst anstoßen muss.

Die Synchronisation erfolgt dabei standartmäßig im Hintergrund über eine sog. *Zwei-Wege-Synchronisation*. Hierbei wird immer die aktuellste Version einer Datei vom Endgerät zum Cloudspeicher und dann ggf. weiter zu den anderen verbundenen Endgeräten geschickt. Dass eine Datei verschickt wird, kann dabei einerseits daran liegen, dass der Nutzer auf seinem Endgerät eine neue Datei erstellt (z.B. mit seinem Smartphone ein Foto aufnimmt) bzw. eine bestehende Datei verändert (z.B. Änderungen an einem Word-Dokument vornimmt). Aber auch die bloße Änderung von sog. *Meta-Daten* einer Datei (z.B. Zeitpunkt des letzten Öffnens oder der Speicherort) kann dazu führen, dass diese vom Synchronisationsprogramm als verändert erkannt und synchronisiert wird, ohne dass dies konkret durch bewusste Erstellung oder Veränderung vom Nutzer angestoßen wurde.

Auf diese Art und Weise wird regelmäßig nahezu der gesamte Datenbestand bzw. zumindest die Dateien, die ein Nutzer nutzt und bearbeitet und die daher für ihn relevant sind, zwischen der Cloud und den Endgeräten hin- und hergeschickt. Besonders viele Daten werden dabei übertragen, wenn der Nutzer ein neues Endgerät einrichtet. In diesem Fall wird der gesamte Inhalt der in der

Cloud gespeicherten Daten auf das neue Endgerät übertragen. Das Gleiche gilt bei sog. Backup-Diensten (z.B. populär Backblaze.com), bei denen ein gesamtes Abbild einer Festplatte auf den Cloud-Server geladen wird.

(c) Zum Telekommunikationsbegriff

Auf Grund der tendenziell weiten Auslegung des Begriffs der Telekommunikation durch das angerufene Gericht[163] besteht das reale Risiko, dass alle Datenübertragungen von der und in die Cloud als Telekommunikation i.S.d § 1 Abs. 1 G 10 sowie „laufende Kommunikation" i.S.d. § 11 Abs. 1a Satz 1 G 10 sowie „Inhalte und Umstände der Kommunikation" i.S.d. § 11 Abs. 1a Satz 2 G 10 verstanden werden.[164] Das angerufene Gericht hat danach bereits entschieden, dass „Telekommunikation" und der Schutz des Art. 10 Abs. 1 GG nicht notwendigerweise ein sozialkommunikatives menschliches Verhalten umfassen, sondern vielmehr jeder technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können, Telekommunikation i.S.d. § 100a StPO ist. Danach fällt die Internetkommunikation darunter (d.h. das Surfen im Internet).[165] Kerngedanke ist hierbei, dass das Schutzbedürfnis bei auch bei einer Mensch-Maschine-Kommunikation oder menschlich veranlassten Maschine-Maschine-Kommunikation sich nicht von dem einer zwischenmenschlichen Kommunikation unterscheidet, wenn hierfür auf die Hilfe Dritter zur Übermittlung der Informationen zurückgegriffen werden muss. Folgt man dieser Linie, wäre etwa auch die Übermittlung von Sensordaten von vernetzten Geräten („Internet der Dinge") vom Telekommunikationsbegriff umfasst, die Rückschlüsse auf das Leben und die Interessen von Personen geben können. Umfasst wäre aber möglicherweise vom Telekommunikationsbegriff auch die Kommunikation eines Nutzers mit der Cloud. Auch eine automatische Synchronisation ist dabei initial von dem Nutzer und damit von einem Menschen veranlasst. Zumindest einfachrechtlich lässt sich daher nicht ausschließen, dass die Nachrichtendienste § 3 Abs. 1 i.V.m. § 11 Abs. 1a G 10 so auslegen, dass auch diese Datenströme als Kommunikation überwacht werden können. Bekanntlich haben deutsche Nachrichtendienste und die ihnen übergeordneten obersten Dienstbehörden schon in ganz anderen Situationen Ansichten zur Rechtsauslegung im Überwachungsrecht eingenommen, die bei

---

163 BVerfG, Beschluss v. 6. Juli 2016 – 2 BvR 1454/13, Rn. 34; s. etwa zur Ableitung eines weiten Verständnisses nur *Köhler,* in: Meyer-Goßner/Schmidt, StPO, 64. Auflage 2021, § 100a Rn. 6.

164 S. zum Meinungsstand sowie mit überzeugender eigener Argumentation gegen ein solches Verständnis *Grötzinger,* Die Überwachung von Cloud-Storage, 2018, S. 70 ff.

165 Vgl. BVerfG, Beschluss vom 6. Juli 2016 – 2 BvR 1454/13, Rn. 37 f.

Licht betrachtet schwerlich bis gar nicht vertretbar erscheinen; genannt sei als Stichwort an dieser Stelle allein die „Weltraumtheorie“ des BND.[166]

Da die Quellen-TKÜ die Verschlüsselung umgeht, mit der die Übertragung der Daten zwischen Cloud und Endgeräten geschützt wird, könnten nach einem weiten Verständnis des Telekommunikationsbegriffs somit in nicht wenigen Fällen nahezu alle Daten – seien es Dokumente, Finanzunterlagen, Fotos, etc. – mit abgefangen werden. Damit wird deutlich, dass die Quellen-TKÜ bei Licht betrachtet je nach Lesart einer Online-Durchsuchung viel nähersteht als einer gewöhnlichen TKÜ. Bei der Quellen-TKÜ handelt es sich bei diesem Verständnis somit mitnichten um eine bloße Anpassung altgedienter Überwachungsmethoden, „um eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist.“[167] Es existierte schlicht keine alte TKÜ-Überwachungstechnik, mit der man die auf dem Computer einer Zielperson befindlichen Daten unter Umständen bis zur Gesamtheit hin auslesen konnte. Es gab auch keinen Zeitpunkt im Stand der Technik, in der die Behörden über eine gewöhnliche TKÜ in einen Cloudspeicher übermittelte Daten mitlesen konnten. Dies schlicht, weil es vor dem „Verschlüsselungszeitalter“ noch keine Cloud-Speicher gab.

Somit kann es in der Praxis – nicht nur ausnahmsweise – Fälle geben, in denen zwischen der Quellen-TKÜ und der Online-Durchsuchung faktisch kein Unterschied besteht. Der Umfang der Informationen, die im Rahmen einer Quellen-TKÜ gewonnen werden können, ist nicht immer nur punktuell und begrenzt, sondern kann einen Umfang annehmen, der einer Online-Durchsuchung gleichkommt, weil er ein erheblich genaueres Bild über das Leben, die Interessen, Gedanken und Beziehungen einer Person erlaubt als eine klassische Telekommunikationsüberwachung. Genau diese Erwägungen haben auch den österreichischen Verfassungsgerichtshof dazu geführt, die österreichischen Regelungen zur Quellen-TKÜ für verfassungswidrig zu erklären:

> „Die Bestimmung ermöglicht es, Daten zu überwachen, die der Betroffene niemals an eine andere Person übermitteln wollte. Dadurch kommt die Ermittlungsmaßnahme einer Online-Durchsuchung gleich. Denn es ist den Strafverfolgungsbehörden möglich, auch ohne Übermittlungsvorgang an eine andere Person, die Aktivitäten des

166 S. dazu etwa *Deutsche Welle*, Der BND glaubt an die _Weltraumtheorie“, abrufbar unter: https://www. dw .com/de/der-bnd-glaubt-an-die-weltraumtheorie/a-18846817, zuletzt abgerufen am 8. Juli 2021; *Biermann*, in: ZEIT online, „Die Anarchos des BND“, abrufbar unter https://www.zeit.de/politik/deutschland/2014-11/bnd-bundesnachrichtendienst-gesetz-grundrecht, zuletzt abgerufen am 8. Juli 2021.

167 So BVerfGE 141, 220, 309.

> Betroffenen nahezu vollständig zu überwachen. Voraussetzung ist lediglich, dass der Betroffene Daten nicht (nur) lokal abspeichert, sondern sich Cloud-Server oder auch nur E-Mail-Programme bedient. Eine Vielzahl an Personen speichert etwa private Dokumente bereits in Clouds ab, um später von anderen Geräten darauf zugreifen zu können. Ihr Inhalt war jedoch nie für eine andere Person gedacht. Ebenso ist es mittlerweile gängige Praxis, sich Notizen oder Erinnerungen in E-Mail Entwürfen abzuspeichern, um darauf unabhängig vom benutzten Gerät Zugriff zu haben. Diese Notizen sind eher mit Tagebüchern vergleichbar. Die Bezeichnung 'Überwachung von Nachrichten' erweist sich in diesem Zusammenhang somit als irreführend. Fotos, Videos, Kontakte oder Kalendereinträge werden von einem Großteil der Bevölkerung ebenso bereits in einer Cloud abgespeichert, um im Falle eines Verlusts des Computersystems (zB Handy) nicht auch noch sämtliche Kontaktdaten und Erinnerungen zu verlieren. Sobald mehrere Personen an einem Dokument arbeiten ist es ebenso praktisch, dieses in einer Cloud zu speichern, damit alle Beteiligte parallel daran arbeiten können. Mit 'Kommunikation' im ursprünglichen Sinne der Überwachung von (verschlüsselten) Nachrichten hat dies freilich wenig zu tun. Trotzdem ermöglicht es das Gesetz (worauf die Materialien explizit hinweisen) in den genannten Fällen eine Überwachung dieser, bloß an einen anderen Server, übermittelter Daten, was de facto zu einer Online-Durchsuchung führt. Eine solche ist jedoch, wie dies auch die Materialien explizit erwähnen, grob unverhältnismäßig.“[168]

Auch das angerufene Gericht folgte in seiner Entscheidung zum BKA-Gesetz ähnlichen Gedanken, indem es den Schutz des IT-Grundrechts nicht nur auf eigene IT-Systeme bezog, sondern auch auf vernetzte Geräte und Cloud-Anwendungen:

> „a) § 20k Abs. 1 BKAG ermächtigt zu einem Zugriff auf informationstechnische Systeme und erlaubt die geheime Durchführung von Online-Durchsuchungen, mit denen private, von den Betroffenen auf eigenen **oder vernetzten fremden Computern (wie etwa der sogenannten Cloud)** abgelegte oder hinterlassene Daten erhoben und deren Verhalten im Netz nachvollzogen werden kann. Die Vorschrift begründet damit einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).
>
> Mit dieser eigenständigen Ausprägung des allgemeinen Persönlichkeitsrechts trägt die Verfassung der heute weit in die Privatsphäre hineinreichenden Bedeutung der Nutzung

168 Verfassungsgerichtshof Österreich, Urteil vom 11. Dezember 2019, Az. G 72-74/2019-48, G 181-182/2019-18.

> informationstechnischer Systeme für die Persönlichkeitsentfaltung Rechnung (vgl. BVerfGE 120, 274 <302 ff.>). Tagebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens, Film- oder Tondokumente werden heute zunehmend in Dateiform angelegt, gespeichert und teilweise ausgetauscht. Weite Bereiche auch der höchstpersönlichen Kommunikation finden elektronisch mit Hilfe von Kommunikationsdiensten im Internet oder im Rahmen internetbasierter sozialer Netzwerke statt. Dabei befinden sich die Daten, auf deren Vertraulichkeit die Betroffenen angewiesen sind und auch vertrauen, in weitem Umfang nicht mehr nur auf eigenen informationstechnischen Systemen, sondern auf denen Dritter. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf diese Daten und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie **persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind,** erfasst und Bewegungen der Betroffenen im Netz verfolgt werden. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar."[169]
>
> (Hervorhebungen diesseits)

Es ist folglich nicht ausgeschlossen, dass unter den Begriff der Telekommunikation i.S.d. G 10 Kommunikationsvorgänge fallen können, die – wie die Kommunikation zwischen einem Nutzer und seinen vernetzten Geräten einschließlich Cloud-Anwendungen – nicht nur durch Art. 10 Abs. 1 GG geschützt sind, sondern sogar durch das IT-Grundrecht, für das sehr viel höhere Hürden gelten. Dies macht umso deutlicher, dass der einfache Gesetzgeber nicht genau bestimmt hat, wie weit die Ermächtigung zur Durchführung einer Quellen-TKÜ in der Praxis gehen darf.

bb. Besonderheit Cloud-Backups von Chatverläufen

(a) Zur Arbeitsweise und Nutzung von Cloud-Backups von Chatverläufen

Die mittlerweile vorherrschende Nutzung von Cloud-Speicherdiensten im Zusammenspiel mit einem weiten Telekommunikationsbegriff bringt dabei auch auf andere Weise eine deutlich schwerere Eingriffstiefe mit sich. Die mittlerweile

169 BVerfGE 141, 220, 303 f.

standard- und regelmäßig durchgeführten sog. Cloud-Backups gesamter Chatverläufe in nahezu allen modernen Kommunikations-Anwendungen könnten dazu führen, dass über die Quellen-TKÜ nach dem G 10 in vielen Fällen *menschliche Kommunikation*, die weit über den Anordnungszeitraum hinausgeht, rechtmäßiger Weise mit überwacht wird.

Nahezu alle aktuellen Smartphones haben von Werk aus eine Anbindung zu einem Cloud-Speicherdienst. Für *Android-Smartphones* ist dies regelmäßig *Google Drive* oder *Samsung-Cloud*, für *Apple iPhones* die sog. *iCloud*. Anwendungen, wie z.B. *WhatsApp* oder *iMessage*, laden bei entsprechender Einstellung regelmäßig – meistens wöchentlich – ein vollständiges Backup aller auf einem Endgerät gespeicherten Chatverläufe samt gesendeter Mediendateien zur Datensicherung in den Cloud-Speicherdienst. Diese Einstellung zur Datensicherung wird den Benutzern dabei standartmäßig beim Einrichten der entsprechenden Geräte (z.B. iPhone) empfohlen. Es kann davon ausgegangen werden, dass ein weit überwiegender Teil der Benutzer hiervon Gebrauch macht, da so Chatverläufe und Mediendateien bequem automatisiert gesichert werden können und bei Abhandenkommen, Defekt oder eines Wechsels des Smartphones insoweit nichts verloren geht.

Bei dieser Datensicherung werden die Chatverläufe und übersendeten Mediendateien in ihrer Gesamtheit in den Cloud-Speicherdienst hochgeladen. In nicht wenigen Fällen umfasst diese Datensammlung daher die gesamte über eine Anwendung geführte Kommunikation mit allen Kontakten über mehrere Jahre. Die Übertragung der Datensammlung erfolgt dabei in beide Richtungen. Richtet der Nutzer beispielsweise ein neu gekauftes Smartphone ein, so wird die gesamte Datensammlung aus dem Cloud-Speicherdienst auf das Endgerät des Nutzers wieder heruntergeladen, sodass die Chatverläufe auch auf diesem Gerät zur Verfügung stehen. Es liegt auf der Hand, dass es sich hierbei um hochsensible Datensammlungen handelt, die auf Grund dessen von den Anwendungen auch nur verschlüsselt übertragen werden. Auf diese Verschlüsselung legt der Anwender in aller Regel auch Wert. Insgesamt ist die Sensibilität der Nutzer für die Nutzung verschlüsselter Kommunikationswege (End-zu-End-Verschlüsselung) in den letzten Jahren enorm gestiegen.

(b) Übertragung von Chatverläufen und Backups als Telekommunikation

Bei der Übertragung dieser gesammelten Chatverläufe von und in die Cloud handelt es sich nach einem weiten Telekommunikationsbegriff ebenfalls um Telekommunikation, die im Anordnungszeitraum stattfindet. Sie umfasst aber *menschliche Kommunikation*, die den Anordnungszeitraum ggf. weit überschreitet. Die schützende Verschlüsselung wird von der Quellen-TKÜ gerade umgangen.

(c) Folgen für die Eingriffsintensität einer Quellen-TKÜ

Damit kommt der Quellen-TKÜ bei einem weit verstandenen Telekommunikationsbegriff auch hier eine deutlich gewichtigere Eingriffstiefe zu, die über eine gewöhnliche TKÜ weit hinausgeht und einer Online-Durchsuchung faktisch weitgehend gleichkommt. Es handelt sich bei entsprechender Lesart damit auch hier bei der Quellen-TKÜ in keiner Weise um eine gewöhnliche TKÜ im modernen Zeitalter. Es ist vor dem „Verschlüsselungszeitalter" nicht vorgekommen, dass die überwachte Zielperson während der Überwachung neben der laufenden Kommunikation noch die Kommunikation etwa der letzten drei Jahre mit all seinen Kontakten samt Fotos mitübersandt hat, sodass diese zufällig von der Behörde mit abgefangen werden konnte.

cc. Bewusstsein um Verschlüsselung

Neben diesen beiden entscheidenden Gründen, kommt der Quellen-TKÜ auch aus einem weiteren Gesichtspunkt eine im Vergleich zur gewöhnlichen TKÜ erheblich intensivere Eingriffstiefe zu. Dies liegt in dem mittlerweile gesteigerten „Verschlüsselungs-Bewusstsein" der IT-nutzenden Bürger begründet.

Verschlüsselungstechnik war lange Zeit ein Thema, dass nur Experten und IT-affine Menschen beschäftigte. Ein Großteil der Bürger dürfte sich lange Zeit nicht einmal darüber bewusst gewesen sein, ob eine bestimmte Internetverbindung – beispielsweise über das https-Protokoll – verschlüsselt war. Im Gegenteil ging man davon aus, dass Telekommunikationstechnik grundsätzlich sowohl vom Staat als auch von Dritten abgehört werden kann. Dementsprechend gab es Informationen aus Privat- oder Intimsphäre, die man – wie es geläufig hieß – „nicht am Telefon" besprach.

Auf Grund der Einführung der Ende-zu-Ende-Verschlüsselung in zahlreichen Telekommunikationsanwendungen, mit der Anbieter heute aktiv werben,[170] ist die Thematik der Verschlüsselung in der Mitte der Gesellschaft angekommen. Hiermit hat sich auch das Kommunikationsverhalten der Bürger verändert. Selbst auf Smartphones werden regelmäßig Zertifikate für eine (nur) verschlüsselte E-Mail-Kommunikation installiert. Diese höhere Sensibilität für

170 Für WhatsApp s. https://www.whatsapp.com/privacy?lang=de, zuletzt abgerufen am 12. Juli 2021; für iMessage s. Heise, E-Privacy: Apple pocht auf Ende-zu-Ende-Verschlüsselung, abrufbar unter: https://www.heise.de/news/E-Privacy-Apple-pocht-auf-Ende-zu-Ende-Verschluesselung-4983045.html#:~:text=Bei%20den%20hauseigenen%20Kommunikationsdienste%20iMessage,betonte%20Federighi%20%E2%80%93%20auch%20Apple%20erhalte, zuletzt abgerufen am 12. Juli 2021; für Signal s. https://support.signal.org/hc/de/articles/360007318911-Woher-wei%C3%9F-ich-dass-meine-Kommunikation-vertraulich-ist-, zuletzt abgerufen am 12. Juli 2021.

IT- und Datensicherheit ist auch gesellschaftlich gewollt, geht es dabei nicht nur um den Schutz privater Informationen, sondern auch von Betriebsgeheimnissen gegenüber Kriminellen sowie vor rechtswidriger privater Auswertung oder ausländischen Staaten.

Übertragen auf die analoge Welt der Briefe lässt sich dies an folgenden Beispielen verdeutlichen:

Im ersten Fall schreibt eine Person einer anderen einen gewöhnlichen Brief. Dieser Brief wird auf dem Postweg vom Staat abgefangen und so von dessen Inhalt Kenntnis genommen.

Im zweiten Fall schreibt eine Person wieder einen Brief an eine andere Person. Sie schickt den Original-Brief jedoch nicht selbst ab, sondern übersetzt diesen auf einem neuen Blatt mit einem nur dem Empfänger bekannten Codierschlüssel. Dieses codierte Blatt schickt sie nun ab. Das Original „im Klartext" legt sie in ihre Schreibtischschublade. Am nächsten Tag kommen Beamte in die Wohnung und nehmen den Original-Brief aus der Schreibtischschublade an sich mit der Argumentation, man hätte ja auch den codierten Brief abfangen können. Der Unterschied zum ersten Fall ist evident, auch wenn man den Schutzbereich des Art. 13 GG außer Acht lässt. Es liegt auf der Hand, dass die Person, die den Brief schreibt, grundsätzlich bereit ist, andere Informationen in den codierten Brief zu schreiben als in den uncodierten. In vielen Fällen wird die Person gerade einen codierten Brief schreiben, weil sie privatere, womöglich intimere bzw. vertrauliche und insgesamt für schutzwürdig erachtete Informationen übermitteln möchte.

Dieses Beispiel aus der analogen Welt lässt sich ohne Weiteres auf die digitale übertragen. Auf Grund eines veränderten Bewusstseins in der Bevölkerung zur Thematik der Verschlüsselung, werden Bürgerinnen und Bürger andere Informationen übermitteln, wenn sie sich in der Sicherheit der Ende-zu-Ende-Verschlüsselung wiegen als ohne eine solche. Auch hierin liegt eine erhöhte Eingriffstiefe der Quellen-TKÜ gegenüber der gewöhnlichen TKÜ begründet.

dd. Erhöhung der Eingriffsschwere durch Kooperationspflichten der Telekommunikationsunternehmen (§ 2 Abs. 1a Satz 1 Nr. 4 G 10)

Die Schwere des Eingriffs in Art. 10 Abs. 1 GG wird noch vertieft durch die Kooperationspflichten der Telekommunikationsunternehmen in § 2 Abs. 1a Satz 1 Nr. 4 G 10. Danach sind die Telekommunikationsunternehmen verpflichtet, Datenströme auf Verlangen der Nachrichtendienste „zur Einbringung von technischen Mitteln zur Durchführung einer Maßnahme nach § 11 Abs. 1a" umzuleiten. Dies bedeutet praktisch, dass die Nachrichtendienste auf diesem Wege die Möglichkeit erhalten, die von

Telekommunikationsanbietern übermittelten Inhalte so zu manipulieren, dass sie sich Zugang zum IT-System der Zielperson verschaffen können. Denkbar wäre es etwa, an den Datenstrom ein kleines Programm anzudocken, das dann automatisch auf dem Zielsystem einen sog. Staatstrojaner installiert. Denkbar wäre auch eine inhaltliche Manipulation einer Nachricht, um die Zielperson „zu überlisten" und sie zu veranlassen, unbewusst selbst die Infiltration ihres IT-Systems zu ermöglichen.

Ihr besonderes Gewicht erhält diese Regelung dadurch, dass in einer digitalen Welt, in der Internet, vernetzte Geräte und Telekommunikation allgegenwärtig sind, das Vertrauen in die Integrität dieser von Telekommunikationsunternehmen bereitgestellten essenziellen Infrastruktur erheblich beeinträchtigt wird.

2. Ergebnis

Die angegriffenen Normen § 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 verstoßen in formeller sowie materieller Hinsicht gegen Art. 10 Abs. 1 GG.

III. Verstoß gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG (IT-Grundrecht) durch die beschränkte Online-Durchsuchung (§ 11 Abs. 1a Satz 2 G 10)

Die Eingriffsermächtigung zur beschränkten Online-Durchsuchung gemäß § 11 Abs. 1a Satz 2 i.V.m. § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 verstößt gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG.

1. Eingriff

Der Gesetzgeber geht bei der Einführung des § 11 Abs. 1a G 10 davon aus, dass insgesamt mit der Überwachungsbefugnis lediglich in Art. 10 Abs. 1 GG eingegriffen wird.[171] Diese Einordnung ist verfassungsrechtlich unzutreffend. Die beschränkte Online-Durchsuchung (auch „Quellen-TKÜ plus" oder „erweiterte Quellen-TKÜ" genannt) gemäß § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 stellt einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG (IT-Grundrecht) dar.

---

171 *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste: Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, VerfBlog, 2021/7/06, https://verfassungsblog.de/staatstrojaner-nachrichtendienste/, abgerufen am 8. Juli 2021.

a. Rechtliche Einordnung und Abgrenzung von Art. 10 Abs. 1 GG zum IT-Grundrecht

Das Bundesverfassungsgericht hat die sog. Quellen-TKÜ privilegiert, indem es für diese Form der Online-Durchsuchung mit begrenztem Funktionsumfang eine Schutzbereichsausnahme vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorgenommen hat:

Obwohl sich die Quellen-TKÜ – wie eine Online-Durchsuchung – dadurch auszeichnet, dass bei ihr verdeckte Eingriffe in informationstechnische Systeme notwendig sind, soll sie grundsätzlich keinen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darstellen, sondern sich ausschließlich nach den Vorgaben richten, die auch sonst für Telekommunikationsüberwachung gelten.[172] Ausdrückliche Voraussetzung ist insofern jedoch, dass die hierfür notwendigen Eingriffe in das informationstechnische System rechtlich voraussetzen und technisch sicherstellen, dass eine Überwachung nur für die *laufende* Telekommunikation erfolgt. Andernfalls komme allein ein Vorgehen nach den Vorschriften in Betracht, die für einen Eingriff in informationstechnische Systeme gelten.[173] Maßgeblich sei insoweit, „ob das Programm so ausgestaltet ist, dass es – hinreichend abgesichert auch gegenüber Dritten – den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern […] inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht."[174] Hingegen komme es nicht darauf an, „ob durch eine technisch aufwendige Änderung des Überwachungsprogramms selbst – sei es durch die Behörde, sei es durch Dritte – dessen Begrenzung auf eine Erfassung der laufenden Telekommunikation aufgehoben werden" könne.[175] Die Schutzbereiche beider Grundrechte sind daher komplementär angelegt: Sobald die engen Grenzen der „laufenden Kommunikation" überschritten sind, also der verfassungsrechtlich abgesteckte Anwendungsbereich der Quellen-TKÜ verlassen wird, stellt sich der Eingriff ohne weiteres als Online-Durchsuchung und damit als Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar.[176]

---

172 BVerfGE 120, 274, 309; *Buermeyer*, StV 2013, 470, 473.
173 BVerfGE 141, 220, 311 f.
174 BVerfGE 141, 220, 312.
175 BVerfGE 141, 220, 311 f.
176 S. nur *Buermeyer*, StV 2013, 470, 473.

b. Anwendung des Maßstabs auf den vorliegenden Fall – Eingriff in das IT-Grundrecht

Die in § 11 Abs. 1a Satz 2 G 10 vorgesehene Form der Quellen-TKÜ wird zum Teil als „eine Mischform zwischen Quellen-TKÜ und Online-Durchsuchung" bezeichnet, wobei weder aus dem Gesetz noch aus der Gesetzesbegründung hinreichend hervorgeht, in welchem Umfang auf gespeicherte Informationen zugegriffen werden können soll.[177]

Das Gesetz versucht insofern eine Grenze zu ziehen, als nur Kommunikationsinhalte und -umstände erhoben werden können, die bereits ab dem Zeitpunkt der Anordnung – allein bei der Durchführung – auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten erhoben werden können, § 11 Abs. 1a Satz 2 G 10. Dieser lautet:

> „Auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können,"

Ausweislich der Gesetzesbegründung orientiert sich die Regelung des neuen Absatz 1a „an dem Modell der Strafprozessordnung (§ 100a Absatz 1 Satz 2 und 3 sowie Absatz 5 und 6)."[178] § 100a Abs. 1 Satz 3 StPO lautet fast textidentisch:

> „Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können."

Dieser Versuch einer Grenzziehung durch den Gesetzgeber sowohl im Nachrichtendienst- wie im Strafprozessrecht genügt aber nicht, um die Quellen-TKÜ und die Online-Durchsuchung hinreichend voneinander abzugrenzen.[179]

---

177 *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste: Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, VerfBlog, 2021/7/06, https://verfassungsblog.de/staatstrojaner-nachrichtendienste/, abgerufen am 8. Juli 2021.

178 BT-Drs. 19/24785, S. 22.

179 *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste: Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, VerfBlog, 2021/7/06, https://verfassungsblog.de/staatstrojaner-nachrichtendienste/, abgerufen am 8. Juli 2021; ebenso *Kruse/Grzesiek*, KritV 2017, 331, 335: Quellen-TKÜ als „kleine" Online-Durchsuchung.

Dies sieht auch die *ganz h.M. im Strafprozessrecht* zum strukturgleichen § 100a Abs. 1 Satz 3 StPO so, die folgerichtig einen Eingriff in das IT-Grundrecht annimmt.[180]

Dabei geht bereits der Wortlaut des Gesetzes der hier angegriffenen Norm davon aus, dass mit der Ermächtigung des § 11a Abs. 1a Satz 2 G 10 die Überwachung über die laufende Kommunikation *hinaus* ausgedehnt wird auf die *hypothetisch laufende*, aber in Wahrheit abgeschlossene, übertragene Kommunikation. Zur Ermöglichung der Maßnahme ist eine Infiltration eines Endgerätes erforderlich, um entweder den Schlüssel zur Ermöglichung einer weiteren Telekommunikationsüberwachung mit Hilfe einer Entschlüsselungstechnik oder aber die auf dem Rechner entschlüsselt vorhandenen Telekommunikationsinformationen auszuleiten. Damit geht die Maßnahme über eine hypothetische konventionelle Telekommunikationsüberwachung hinaus.[181] Unabhängig von der gesetzmäßig geforderten Begrenzung des technischen Mittels auf laufende Telekommunikation erfolgt die Installation in diesen Fällen durch einen Eingriff in die Integrität des informationstechnischen Systems. Eine solche Integritätsverletzung betrifft immer das gesamte IT-System, denn dabei wird technisch der Zugriff auf das gesamte informationstechnische System erlangt.[182] Das technische Mittel leitet zunächst – vergleichbar mit einer Online-Durchsuchung – soweit ersichtlich alle Daten aus. Eine Beschränkung auf laufende Kommunikation erfolgt, soweit ersichtlich, erst nachträglich über die Bedienkonsole der Sicherheitsbehörden.[183] Dass erst im Anschluss eine Beschränkung auf nur bestimmte Daten erfolgt, vermag die Tatsache des Eindringens in das gesamte System jedoch nicht zu ändern.

Die Ratio des gegenüber des IT-Grundrechts abgesenkten Grundrechtsschutzes des Art. 10 Abs. 1 GG passt in dieser Konstellation erkennbar nicht. Das angerufene Gericht führt zur Abgrenzung zutreffend aus:

> „Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich allerdings nicht auf die nach Abschluss eines Kommunikationsvorgangs im

---

180 *Hauck*, in: LR-StPO, 27. Auflage 2018, § 100a Rn. 146 f.; *Eschelbach*, in: SSW-StPO, 4. Auflage 2020, § 100a Rn. 2: „Soweit § 100a Abs. 1 S. 3 dies auf Informationen aus einer Telekommunikation erstreckt, die bereits vor Anbringung der Überwachungssoftware geführt wurde, handelt es sich praktisch um eine thematisch beschränkte »kleine Online-Durchsuchung«."; Rn. 48 f.; *Großmann* JA 2019, 241, 243; *Freiling/Safferling/Rückert*, JR 2018, 9, 21; *Singelnstein/Derin*, NJW 2017, 2646, 2648; *Martini/Frölingsdorf*, NVwZ-Extra 2020, 3, 7 f.: „In der Sache erlaubt § 100a I 3iVm V Nr.2 StPO eine Online-Durchsuchung, die – trotz der vorgesehenen Schutzmechanismen, insbesondere der richterlichen Anordnung – nicht den Anforderungen an einen zulässigen Eingriff in das IT-Grundrecht genügt."

181 *Eschelbach*, in: SSW-StPO, 4. Auflage 2020, § 100a Rn. 39; *Freiling/Safferling/Rückert*, JR 2018, 9, 11 f.

182 *Martini/Fröhlingsdorf*, NVwZ-Extra 2020, 3.

183 *Martini/Fröhlingsdorf*, NVwZ-Extra 2020, 9.

> Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann."[184]

Solange der Kommunikationsvorgang andauert, kann man sich als Kommunikationsteilnehmer (wenigstens bei unverschlüsselter Kommunikation) gewissermaßen nicht endgültig sicher sein, dass die kommunizierten Inhalte und Umstände nicht vom Staat bei gewichtigen Verdachtsgründen abgehört werden, weil man sich ihrer in einem Sozialraum der Kommunikation entäußert hat,[185] während die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände gewissermaßen zum „digitalen Hausfrieden" („my home is my castle"), zu einer digitalen „Intimsphäre"[186] gehören,[187] in den nur zugunsten überragend wichtiger Rechtsgüter eingegriffen werden kann.

Der Unterschied zwischen den verschiedenen Maßnahmen lässt sich anhand eines Beispiels aus der „analogen Welt" verdeutlichen:

Eine Briefbeschlagnahme nach Zugang der Sendung beim Empfänger (also wenn dieser die alleinige Verfügungsgewalt erlangt), indem etwa ein Amtsträger den Brief aus dem Briefkasten „fischt" oder nach einer Durchsuchung in der Schreibtischschublade oder gar zwischen anderen Unterlagen abgelegt findet, wird nicht dadurch zu einem bloßen Eingriff in das Postgeheimnis gemäß Art. 10 Abs. 1 GG, weil der Brief auf dem Postweg hätte rechtmäßig abgefangen werden können. Es handelt sich vielmehr, sobald der Brief in den Herrschaftsbereich des Empfängers in den Briefkasten gelangt ist, um einen

---

184 BVerfGE 120, 274, 307 f.

185 Siehe BVerfGE 115, 166, 184: „Post und Telekommunikation bieten die Voraussetzungen für die private Kommunikation zwischen Personen, die nicht am selben Ort sind, und eröffnen so eine neue Dimension der Privatsphäre (vgl. Gusy, in: v. Mangoldt/Klein/Starck, Grundgesetz, 5. Aufl. 2005, Art. 10 Rn. 18 f.). Damit verbunden ist ein Verlust an Privatheit; denn die Kommunizierenden müssen sich auf die technischen Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten Kommunikationsmittler anvertrauen. Inhalt und Umstände der Nachrichtenübermittlung sind dadurch dem erleichterten Zugriff Dritter ausgesetzt. Die Beteiligten, die ihre Kommunikation mit Hilfe von technischen Hilfsmitteln über Distanz unter Nutzung fremder Kommunikationsverbindungswege ausüben, haben nicht die Möglichkeit, die Vertraulichkeit der Kommunikation sicherzustellen.".

186 Vgl. die Pressemitteilung des Chaos Computer Clubs v. 27.2.2008: „Bundesverfassungsgericht schafft neues Grundrecht auf digitale Intimsphäre", https://www.ccc.de/updates/2008/trojaner-notschlachten?language=de, abgerufen am 8. Juli 2021.

187 Siehe zur Parallele des IT-Grundrechts mit Art. 13 GG („digitale Wohnung") *Hauser*, Das IT-Grundrecht, 2015, S. 66 ff.; siehe auch *Britz*, DÖV 2008, 411, 412: „spezifisch technologiebezogene Vertraulichkeitserwartung", „gewisse Parallelisierung des Vertrauens in den informationellen Schutz der Wände einer Wohnung"; vgl. auch *Drallé*, Vertraulichkeit und Integrität informationstechnischer Systeme, 2010, S. 46: „systematische Parallele zum Schutz der Wohnung".

Eingriff in Art. 13 GG[188] sowie in das Briefgeheimnis i.S.d. Art. 10 Abs. 1 GG, und nicht bloß um einen Eingriff in das Postgeheimnis.[189]

Entsprechend handelt es sich bei der vermeintlich nur „erweiterten Quellen-TKÜ" oder „Quellen-TKÜ plus" nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2, 3 Nr. 1 lit. b G 10 in der Sache um eine „faktische Online-Durchsuchung" in die „virtuelle Wohnung" des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG. Daher ist terminologisch die Bezeichnung als „beschränkte Online-Durchsuchung", wie sie hier erfolgt, oder als „faktische Online-Durchsuchung" präziser und zutreffender. Dies ist nicht nur eine terminologische Frage. Denn die Bezeichnung „Quellen-TKÜ plus" legt nahe, dieser Eingriff sei letztlich eine logische Anpassung der TKÜ an die technische Entwicklung. Wie gezeigt werden wird, ist dies aber nicht der Fall, weil bereits eine so eingeschränkte Art der Online-Durchsuchung einen Zugriff auf Informationen über eine Zielperson erlaubt, der in keiner Weise mit einer TKÜ im klassischen Sinne vergleichbar wäre und einer vollwertigen Online-Durchsuchung nahekommen kann.

Darüber hinaus ist im Hinblick auf die Schwere des Grundrechtseingriffs zu bedenken, dass mit dem neu geschaffenen § 2 Abs. 1a Satz 1 Nr. 4 G 10 Telekommunikationsdienstleister, die vom Bürger als absolut integer betrachtet werden und diesem gegenüber vertragliche Treuepflichten haben, in weitem Umfang zur heimlichen Mitwirkung an der Überwachung verpflichtet werden.

2. Keine verfassungsrechtliche Rechtfertigung

a. Verstoß gegen den Grundsatz der Verhältnismäßigkeit

Für die Online-Durchsuchung hat das angerufene Gericht entschieden, dass ein derartiger Eingriff nur dann verfassungsrechtlich zu rechtfertigen ist, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen.[190] Wie bereits zu § 11 Abs. 1a S. 1 dargelegt, entsprechen die Voraussetzungen des § 3 Abs. 1 G 10 diesen Anforderungen hinsichtlich der notwendigen Eingriffsschwelle nicht einmal annähernd, weil § 3 Abs. 1 GG keine konkrete Gefahr voraussetzt.

---

188 Siehe zur weiten Auslegung des Wohnungsbegriffs in Art. 13 GG, der auch das gesamte befriedete Besitztum umfasst, BGH, Beschluss vom 14. März 1997 – 1 BGs 65/97.

189 Siehe zur Abgrenzung von Brief- und Postgeheimnis *Durner*, in: Maunz/Dürig, GG, 93. EL Oktober 2020, Art. 10 Rn. 99.

190 BVerfGE 120, 274, 328.

Gleiches gilt für die Anforderungen an das zu schützende Rechtsgut. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person, ferner solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.[191] Die Ermächtigungsgrundlage in § 3 Abs. 1 i.V.m. § 11 Abs. 1a S. 2 G 10 dient in weiten Teilen keinen Rechtsgütern, die hinreichend gewichtig sind, um in der Verhältnismäßigkeit i.e.S. die beschränkte Online-Durchsuchung zu rechtfertigen. [192]

So dient beispielsweise die Überwachung der Person, die eine volksverhetzerische Rede plant oder eine verbotene Vereinigung fortführt, nicht der Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit der Person.

b. Weiterer Verstoß gegen den Grundsatz der Verhältnismäßigkeit durch § 3 Abs. 2 Satz 2 G 10 (Überwachung nichtverdächtiger Dritter)

Die Ausweitung der Eingriffsbefugnisse der Nachrichtendienste durch § 11a G 10 hat zur Folge, dass der durch § 3 Abs. 2 Satz 2 G 10 beschriebene Kreis von Zielpersonen nicht mehr den verfassungsrechtlichen Anforderungen in Form des Verhältnismäßigkeitsgrundsatzes entspricht. Gemäß § 3 Abs. 2 Satz 2 G 10 darf sich die Überwachungsmaßnahme nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Ein kollusives Zusammenwirken mit dem Verdächtigen ist nicht erforderlich. Es ist daher möglich, gutgläubige Dritte gezielt zu überwachen. [193] Zwar hat das BVerfG die Erstreckung der allgemeinen Telekommunikationsüberwachung und Quellen-TKÜ auf Nachrichtenmittler gemäß einer entsprechenden polizeirechtlichen Norm (§ 20l Abs. 1 Nr. 3 und 4 BKAG) bei verfassungskonformer Auslegung für mit Art. 10 Abs. 1 GG vereinbar erklärt; das Urteil bezog sich aber gerade nicht auf den massiveren Grundrechtseingriff der beschränkten Online-Durchsuchung (auch sog. „erweiterte Quellen-TKÜ“ oder „Quellen-TKÜ plus“) gemäß § 11 Abs. 1a Satz 2 G 10, der richtigerweise am IT-Grundrecht zu messen ist. Hierzu hat das angerufene Gericht zutreffend ausgeführt:

> „Der Zugriff auf informationstechnische Systeme und die Wohnraumüberwachung dürfen sich unmittelbar nur gegen diejenigen als Zielperson richten, die für die drohende oder dringende Gefahr verantwortlich sind (vgl. BVerfGE 109, 279 [351, 352]; 120, 274 [329,

191 BVerfGE 120, 274, 328.

192 Zum viel zu weiten Straftatenkatalog siehe bereits ausführlich oben *sub* C. II. 1. c.

193 *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 3 Rn. 33.

> 334]). Diese Maßnahmen dringen so tief in die Privatsphäre ein, dass sie auf weitere Personen nicht ausgedehnt werden dürfen. Verfassungsrechtlich nicht zu beanstanden ist allerdings, wenn die gegen die Verantwortlichen angeordneten Maßnahmen, soweit unvermeidbar, auch Dritte miterfassen […]. […] Ebenso kann eine Online-Durchsuchung auf informationstechnische Systeme Dritter erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht. (…) Ihre Erstreckung auf Dritte steht unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische individuelle Nähe der Betroffenen zu der aufzuklärenden Gefahr oder Straftat voraus. Hierfür reicht es nicht schon, dass sie mit einer Zielperson überhaupt in irgendeinem Austausch stehen. Vielmehr bedarf es zusätzlicher Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Gefahr dienlich sein wird (vgl. BVerfGE 107, 299 [322f.]; 113, 348 [380f.]).“[194]

Die allgemeine, durch das Gesetz zur Anpassung des Verfassungsschutzrechts unverändert gebliebene Adressaten-Norm des § 3 Abs. 2 Satz 2 G 10 genügt diesen Anforderungen nicht.[195] Die Norm schließt alle Nachrichtenmittler ein, „*von denen auf Grund bestimmter Tatsachen* anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt.“ Die vom angerufenen Gericht geforderte strenge Verhältnismäßigkeitsprüfung und spezifische individuelle Nähe des betroffenen Dritten zum Verdächtigen verlangt aber ein gesteigertes Wahrscheinlichkeitsurteil der Kontaktaufnahme des Verdächtigen mit dem Dritten, dem der Terminus „bestimmter Tatsachen“ nicht genügt.

Der österreichische Verfassungsgerichtshof hat zu der fast wortgleichen österreichischen Parallelnorm im Strafprozessrecht (§ 135a Abs. 1 Z 3 lit b ÖStPO[196]) eindrücklich ausgeführt:

---

194 BVerfGE 141, 220, 273 f.

195 So auch etwa *Poscher*, Stellungnahme zu dem Entwurf der Bundesregierung eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Mai 2021, S. 9.

196 § 135a Abs. 1 Z 3 lit. b ÖStPO lautete: „Überwachung verschlüsselter Nachrichten ist zulässig: […] wenn […] auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.“

> „Der Kreis der durch die Überwachung verschlüsselter Nachrichten potenziell betroffenen Personen geht weit über den unter Verdacht stehenden hinaus. Die Formulierung in § 135a Abs 1 Z 3 lit b StPO 'auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem [...] benützen oder mit ihm eine Verbindung herstellen werde' ermöglicht es, Personen zu überwachen, die mit den verdachtsbegründenden Momenten weder zu tun haben, noch davon wissen oder die verdächtige Person überhaupt kennen. Da die Bestimmung einzig und allein auf das Computersystem, nicht aber auf die Person abstellt, ist sie geeignet, Angehörige, Freunde, Bekannte, Arbeitskollegen oder Mitbewohner eines Verdächtigen, aber zum Beispiel auch Betreiber von Internet-Cafes in relativer Nähe des Aufenthalts eines Verdächtigen überwachen zu lassen, weil sich jeweils ohne großen Aufwand argumentieren lassen wird, dass 'aufgrund bestimmter Tatsachen' (es bedarf sohin bloß einer gewissen Wahrscheinlichkeit) anzunehmen sei, dass der Verdächtige ihren PC, Laptop, Mobiltelefon, Tablet etc. benützen oder Kontakt mit ihnen aufnehmen werde, also eine Verbindung damit herstellen könnte. Gerade Personen, die geschäftlich mit vielen Menschen zu tun haben, ohne diese gut zu kennen, könnten leicht davon betroffen sein.“[197]

Verfassungsrechtlich erforderlich für die beschränkte Online-Durchsuchung ist vielmehr eine eigenständige Regelung für Drittbetroffene, die erhöhte Anforderungen an die Wahrscheinlichkeit stellt, dass es zu einer Kontaktaufnahme zum Verdächtigen kommt, und die einschränkende Kriterien wie ein Näheverhältnis zum Verdächtigen aufstellt; ansonsten ist die Streubreite potenzieller Grundrechtseingriffe gegenüber Drittbetroffenen unübersehbar. Die strafprozessuale Parallelnorm für die Online-Durchsuchung des § 100b Abs. 3 Satz 2 StPO entspricht insofern auch nicht den verfassungsrechtlichen Anforderungen.

c. Verstoß gegen den Bestimmtheitsgrundsatz – Unklarheiten im Hinblick auf die technische Reichweite der Ermächtigungsgrundlage des § 11 Abs. 1 a S. 2, 3 Nr. 1 lit. b G 10

Unklar ist bei der gesetzlichen Ausgestaltung des § 11 Abs. 1a Satz 2, 3 Nr. 1 lit. b G 10, ob es sich nur um Daten handeln darf, die ab diesem Zeitpunkt kommuniziert wurden, oder ob die Regelung auch gespeicherte Kommunikationsverläufe erfassen soll, die möglicherweise Jahre zurückreichen, aber nach dem Anordnungszeitpunkt über einen Dienst noch mit der aktuellen Kommunikation mitkommuniziert werden können.

---

197 Verfassungsgerichtshof Österreich, Urteil vom 11. Dezember 2019, Az. G 72-74/2019-48, G 181-182/2019-18.

WhatsApp und andere Messengerdienste sind gerade für viele jüngere Nutzer/-innen heutzutage ein Hauptkommunikationsmittel, das quasi alle anderen Kommunikationsmittel wie E-Mail, Fax etc. ersetzt. WhatsApp-Backups können evtl. große Mengen an monate- oder jahrelanger Kommunikation enthalten, die *realiter* vor der Anordnung erfolgt ist, aber vom weiten Telekommunikationsbegriff mitumfasst ist. Wie der österreichische VGH eindrücklich dargelegt hat, nähert sich die beschränkte Online-Durchsuchung damit quasi einer „vollwertigen" Online-Durchsuchung an.

Mit dem Dienst werden Audionachrichten, Dokumente etc. versendet, die ein umfassendes Bild der Persönlichkeit der Nutzer/innen abgeben können. Unklar ist zudem, wie festgestellt werden soll, welche Kommunikation in verschlüsselter Form hätte erhoben werden können, da der Umfang der Kommunikation von Kommunikationsverläufen jedenfalls bei einigen Diensten von individuellen Nutzereinstellungen abhängig ist, z.B. wenn Messenger Dienste bei der Aufnahme neuer Mitglieder auch alte Nachrichten übermitteln.[198]

Mithin bleibt es völlig unklar, welche Kommunikation rückwirkend bis zum Anordnungszeitpunkt ausgespäht werden darf.

§ 11 Abs. 1a Satz 2 G 10 sieht eine retrospektive Überwachung ab dem Anordnungszeitpunkt vor. Das Gesetz lässt jedoch eine Pflicht zur Festlegung des konkreten Anordnungs*zeitpunktes* vermissen. Nach § 11 Abs. 1a Satz 2 G 10 ist eine Überwachung und Aufzeichnung „ab dem Zeitpunkt der Anordnung" zulässig. Der konkrete Zeitpunkt muss jedoch nicht schriftlich festgehalten werden. § 10 G 10 enthält die verfahrensrechtlichen Vorgaben zur Anordnung. Absatz 2 sieht allein vor, dass die Anordnung schriftlich ergeht. Die konkrete Uhrzeit, wann die Anordnung ergangen ist, muss nicht schriftlich dokumentiert werden. Dies wäre jedoch essentiell für eine klare Abgrenzung, inwieweit retrospektiv gespeicherte Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden dürfen. Durch die fehlende Dokumentationspflicht des Zeitpunktes der Anordnung entstehen jedoch Ungewissheiten, bis wann konkret retrospektiv eine Überwachung zulässig ist. Korrespondierend zu § 100e Abs. 3 Nr. 3 StPO, der eine zwingende Angabe des Endzeitpunktes verlangt, ist eine – gesetzliche – Regelung dahingehend erforderlich, dass auch der Zeitpunkt der Anordnung der Überwachungsmaßnahme mit konkreter Uhrzeit schriftlich dokumentiert wird. Allein das Datum genügt nicht. Andernfalls ist eine Ausleitung auch von auf einem Endgerät gespeicherten Nachrichten vor dem konkreten Zeitpunkt des Erlasses der Anordnung möglich.

198 *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste: Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, VerfBlog, 2021/7/06, https://verfassungsblog.de/staatstrojaner-nachrichtendienste/, zuletzt abgerufen am 8. Juli 2021.

Mithin bleibt es völlig unklar, welche Kommunikation rückwirkend bis zum Anordnungszeitpunkt ausgespäht werden darf.

3. Ergebnis

Bei der beschränkten Online-Durchsuchung gemäß § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2, 3 Nr. 1 lit. b G 10 handelt es sich in der Sache um eine echte Online-Durchsuchung in die „virtuelle Wohnung" des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG, die verfassungsrechtlich nicht gerechtfertigt ist.

IV. Verstoß gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG (IT-Grundrecht) als Schutzpflichtverletzung

Die Ermächtigungsgrundlagen zur Quellen-TKÜ und zur beschränkten Online-Durchsuchung im G 10 und ihre konkrete Ausgestaltung, namentlich in § 11 Abs. 1a i.V.m. § 3 Abs. 1 G 10 verletzen die Beschwerdeführer in ihrem Schutzanspruch gegenüber dem Staat, sich in zumutbarer Weise schützend vor die IT-Sicherheit in der Bundesrepublik zu stellen. Dieser Schutzanspruch folgt aus dem IT-Grundrecht nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.

Durch die Schaffung von Ermächtigungsgrundlagen zur Quellen-TKÜ und zur (begrenzten) Online-Durchsuchung und damit zum Einsatz des Staatstrojaners werden die Sicherheitsbehörden und damit auch die Adressaten des G 10 geradezu herausgefordert, sich ein Arsenal an (i.d.R. besonders gefährlichen) *Zero-Day*-Sicherheitslücken zu verschaffen, um überhaupt in der Lage zu sein, eine Quellen-TKÜ durchführen zu können. Gleichzeitig hat der Gesetzgeber es im Zuge der Regelung der Quellen-TKÜ unterlassen, Regelungen dazu zu treffen, wie mit der staatlichen Kenntnis dieser Sicherheitslücken im Lichte des Risikos für die Allgemeinheit umzugehen ist (sog. Schwachstellenmanagement). Solche Regelungen sind weder im G 10 noch in irgendeinem anderen Gesetz jemals geschaffen worden.

1. Existenz einer Schutzpflicht aus dem IT-Grundrecht nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

Aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme i.S.d. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG folgt eine objektive Schutzpflicht des Staates, sich in zumutbarer Weise schützend vor die IT-Sicherheit in der Bundesrepublik zu stellen.

Es entspricht ständiger Rechtsprechung des angerufenen Gerichts, dass die Grundrechte nicht lediglich subjektive Abwehrrechte des Einzelnen gegen die staatliche Gewalt enthalten, sondern diese zugleich objektivrechtliche Wertentscheidungen darstellen, aus denen sich Richtlinien auch für die Gesetzgebung ergeben. Hieraus können sich verfassungsrechtliche Schutzpflichten ergeben, die es gebieten, rechtliche Regelungen so auszugestalten, dass die Gefahr von Grundrechtsverletzungen in einem zumutbaren Maß bleibt. Die Existenz und der Umfang solcher Schutzpflichten hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen ab.[199] Dabei hat das angerufene Gericht bereits zu Art. 10 Abs. 1 GG festgestellt, dass das Grundrecht auch einen Auftrag an den Staat enthalte, Schutz insoweit vorzusehen, als sich Dritte Zugriff auf die Telekommunikation verschaffen.[200] Auch zum allgemeinen Persönlichkeitsrecht hat das Gericht bereits Schutzpflichten anerkannt.[201]

2. Bedeutung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Für das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist die Existenz einer Schutzpflicht bereits im Wortlaut („Gewährleistung“) angelegt. Diese folgt auf der einen Seite unter Zugrundelegung der oben dargelegten Kriterien aus der enormen Bedeutung, die das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für die Funktionsfähigkeit und die Sicherheit von Staat und Gesellschaft erlangt hat. Auf der anderen Seite ergibt sich die Schutzpflicht aus den hohen, gegenwärtigen Gefahren, die Sicherheitslücken in IT-Systemen für (mitunter sehr) gewichtige Rechtsgüter mitbringen und daneben aus der hohen Zahl an Grundrechtsträgern, die von Sicherheitslücken betroffen sind. Betroffen sind quantitativ jedenfalls sämtliche Grundrechtsträger in der Bundesrepublik Deutschland, mithin über 83 Millionen Menschen.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat in der heutigen Gesellschaft einen Stellenwert erlangt, der selbst zum Zeitpunkt seiner verfassungsgerichtlichen Konstitution durch das angerufene Gericht im Jahre 2008 nicht vorhersehbar war. Bereits zum damaligen Zeitpunkt stellte das angerufene Gericht zutreffend fest, dass die Nutzung der Informationstechnik für die Persönlichkeit und Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt habe. Die jüngere Entwicklung habe dazu geführt, dass informationstechnische

---

199 BVerfGE 49, 89, 142.
200 BVerfGE 106, 28, 37.
201 BVerfGE 63, 131, 142; 73, 118, 201; 96, 56, 64; 100, 271, 284.

Systeme allgegenwärtig seien und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung sei.[202] Zudem ergeben sich Risiken für Funktionieren unserer Demokratie und wesentlicher gesellschaftlicher Grundfunktionen.

Dabei muss bedacht werden, dass zum Zeitpunkt der damaligen Entscheidung im Jahr 2008 informationstechnische Systeme trotz ihrer damals schon hohen Bedeutung noch nicht ihre heutige Allgegenwärtigkeit erreicht hatten. Zum Zeitpunkt der Entscheidung am 27. Februar 2008 gab es noch kein iPhone. Dieses wurde erst im Oktober desselben Jahres in seiner ersten Version präsentiert. Auch wenn das angerufene Gericht damals bereits die enorme Bedeutung der Informationstechnik für die Persönlichkeit des Einzelnen gesehen hat, war es zum damaligen Zeitpunkt – letztlich für niemanden – vorhersehbar, dass – auch bedingt durch die Pandemie – sich heute für viele Bürger ein essentieller Großteil ihrer Lebens- und Arbeitswelt im digitalen Raum abspielt. Alle Bereiche des öffentlichen Lebens und nicht nur des Wirtschaftslebens sind heute ohne eine funktionierende IT-Infrastruktur nicht mehr in der Form funktionsfähig. Heute kann ohne ein funktionierendes IT-System noch nicht einmal ein Corona-Test als Bürgertest ordnungsgemäß durchgeführt werden.

Gleiches gilt für die Bedeutung informationstechnischer Systeme für die freie Entfaltung der Persönlichkeit nahezu jeden Bundesbürgers. So ist allein die Anzahl der Smartphone-Nutzer in Deutschland von 2009 bis 2020 von 6,31 Millionen auf 60,74 Millionen gestiegen.[203] Hinzugekommen sind zahllose vernetzte Geräte - vom Auto bis zur Glühbirne. Diese finden immer mehr Verbreitung.

3. Art, Nähe und Ausmaß möglicher Gefahren

a. Zur Art und Nähe der Gefahr

Es kann davon ausgegangen werden, dass alle IT-Systeme, die letztendlich auch nur von Menschenhand geschaffen werden, Schwachstellen und Fehler enthalten. Diese Schwachstellen und Fehler können sowohl vom Staat als auch von beliebigen Dritten ausgenutzt werden, um sich unbemerkt vom Nutzer des Systems Zugang zu diesem zu verschaffen und Schad- oder Überwachungssoftware auf dem System zu installieren.

---

202 BVerfGE 120, 274, 304.

203 Statista, Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2020, abrufbar unter https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/, zuletzt abgerufen am 9. Juli 2021.

Hierbei sind zwei Kategorien von Sicherheitslücken zu unterscheiden. Dies sind zum einen Sicherheitslücken, von denen der Hersteller des IT-Systems vor der Ausnutzung durch Dritte Kenntnis erlangt. In diesem Fall wird der Hersteller regelmäßig bemüht sein – sei es auf Grund vertraglicher Verpflichtung, Reputationsschutz, etc. – die Sicherheitslücke (in der Regel über ein Software-Update) zu schließen, bevor es zur Ausnutzung kommt. In der Praxis haben sich unter den Herstellern und in der IT-Sicherheitsbranche Kriterien zur Beurteilung von Sicherheitslücken und den Risiken durch sie herausgebildet; anhand dieser Kriterien wird entschieden, ob und wie schnell die Sicherheitslücke zu schließen ist. Solche Sicherheitslücken werden auch *n-Day*-Sicherheitslücken genannt, weil der Hersteller zwischen seiner Kenntniserlangung und der Ausnutzung der Sicherheitslücke *n* Tage Zeit hat, die Sicherheitslücke zu beheben.

Hiervon sind die sog. *Zero-Day*-Sicherheitslücken zu unterscheiden. Hierbei handelt es sich um Sicherheitslücken, die zum Zeitpunkt ihrer Entdeckung bereits aktiv von Angreifern ausgenutzt werden. Für die Hersteller der IT-Systeme besteht somit keine Zeit (0 Tage = *zero days*), um die Sicherheitslücke vor der Ausnutzung zu schließen. Solche Sicherheitslücken sind daher besonders gefährlich.

Bereits zum jetzigen Zeitpunkt ist die IT-Sicherheitslage in Deutschland nach Einschätzung des zuständigen Bundesamtes für Sicherheit in der Informationstechnik (BSI) angespannt.[204] Das BSI registrierte im Jahr 2020 117,4 Millionen neue (!) Schadprogramm-Varianten. Dies sind im Durchschnitt 322.000 neue pro Tag (!). Die Gefahr von Cyberangriffen umgibt den Nutzer von IT-Systemen dabei allgegenwärtig. Allein in Regierungsnetzen wurden im Jahr 2020 52.000 Websites wegen enthaltener Schadprogramme durch den Webfilter des BSI gesperrt und 35.000 Mails mit Schadprogrammen wurden durchschnittlich pro Monat (!) abgefangen.[205]

Das durch die Regelung zur Quellen-TKÜ geradezu herausgeforderte Verhalten der Nachrichtendienste und übrigen Sicherheitsbehörden zur Kenntnisverschaffung und Geheimhaltung von *Zero-Day*-Exploits trägt dabei zu der aufgezeigten Gefährdungslage insbesondere in zweierlei Art schwerwiegend bei:

---

204 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 9. Juli 2021.

205 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 36 f., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 9. Juli 2021.

Zum einem verwehrt der Staat durch die Geheimhaltung den Herstellern der IT-Systeme die Möglichkeit, eine entdeckte Sicherheitslücke mit ihrer i.d.R. überlegenen Kenntnis ihrer Hard- und Software zu bewerten sowie zu schließen und so ggf. eine Vielzahl von Nutzern deutschland- und weltweit vor den Gefahren von Cyberangriffen mittels der Schwachstelle zu schützen. Je länger die Sicherheitslücke geheim gehalten wird, desto höher ist die Wahrscheinlichkeit, dass diese nicht nur durch den Staat für Überwachungsmaßnahmen, sondern auch durch kriminelle Dritte für großflächige und verheerende Cyberangriffe genutzt wird. Dies zeigt eindrucksvoll das Beispiel der Schadsoftware *WannaCry*, die im Jahre 2017 weltweit zu massiven Schäden geführt hat. Das Schadprogramm nutzte dabei eine *Zero-Day*-Sicherheitslücke im Betriebssystem Windows 7 für den Angriff aus. Diese hatten die Täter nach verbreiteter Einschätzung bei dem US-amerikanischen Geheimdienst NSA ausgespäht, der die Sicherheitslücke seinerseits bereits für mehrere Überwachungsmaßnahmen geheim gehalten und ausgenutzt hatte.[206] Chinesische Geheimdienste hatten die Sicherheitslücke bereits im Jahr 2016 von der National Security Agency in den USA (NSA) erlangt und für ihre Zwecke ausgenutzt.[207] Es sind keine Anhaltspunkte dafür erkennbar, dass deutsche Nachrichtendienste Informationen über *Zero-Day*-Schwachstellen besser schützen könnten als die US-amerikanische NSA. Die Geheimhaltung solcher Sicherheitslücken durch staatliche Institutionen ist dabei längst Realität, wie die Auskunft des BKA zu einer Anfrage nach dem IFG durch netzpolitik.org ergeben hat.[208]

Zum anderen kann der Prozess der Kenntnisverschaffung selbst zur Gefährdung der IT-Sicherheitslage in Deutschland massiv beitragen. Sicherheitslücken in IT-Systemen kann der Staat grundsätzlich auf zwei Wegen erlangen. Einerseits durch eigene „Forschung", andererseits durch den Ankauf solcher Sicherheitslücken auf dem (Schwarz-)Markt. Dass dies kein unrealistisches Szenario ist, ergibt sich daraus, dass noch in jüngerer Vergangenheit der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) eingeräumt hat, die Stelle verfüge noch nicht über die technische Expertise, um Sicherheitslücken im benötigten Umfang selbst aufzudecken.[209] Die staatliche – zahlungskräftige – Teilnahme an dem

206 ZEIT ONLINE, Microsoft gibt US-Regierung Mitschuld an Hackerangriff, 15. Mai 2017, abrufbar unter https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung?utm_referrer=https%3A%2F%2Fwww.google.com, zuletzt abgerufen am 9. Juli 2021.

207 NY Times, How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks, abrufbar unter https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html, zuletzt abgerufen am 9. Juli 2021.

208 Netzpolitik.org, Das BKA verhindert, dass Sicherheitslücken geschlossen werden, 12. November 2018, abrufbar unter https://netzpolitik.org/2018/it-sicherheit-das-bka-verhindert-dass-sicherheitsluecken-geschlossen-werden/, zuletzt abgerufen am 9. Juli 2021.

209 Vgl. Heise.de, Schlagabtausch zu ZITiS: IT-Sicherheitslücken schließen oder ausnutzen?, 23. Februar 2018, abrufbar unter https://www.heise.de/newsticker/meldung/Schlagabtausch-

bestehenden (Schwarz-)Markt für Sicherheitslücken, in der Regel im Dark-Net, auf dem sich auch **Kriminelle** bedienen, verschafft einen Anreiz für Expertinnen und Experten von Sicherheitslücken, solche auf diesem Markt anzubieten, anstatt diese an die Hersteller der IT-Systeme weiterzugeben. Denn ein Staat als Kaufinteressent hat die beste Bonität als Kunde. Ein Staat als Kaufinteressent sorgt zugleich für ein dauerhaftes, langfristiges Kaufinteresse von immer wieder neu angebotenen Sicherheitslücken, weil er sie schließlich fortwährend – und gesichert auch in der Zukunft – braucht. Der Staat als Kaufinteressent ist nicht nur zahlungswillig, sondern auch zahlungsfähig und vor allem als „Stammkunde" ein interessanter Geschäftspartner, vom dem dann keine Strafverfolgung droht. Es steht zu erwarten, dass ein solches „*going dark*" des Staates zum Kauf von Sicherheitslücken signifikante Auswirkungen auf dem Markt für Sicherheitslücken haben wird. Zumal auch Unternehmen versuchen, Sicherheitslücken ihrer Produkte zu erwerben, indem sie Prämien ausloben. Dieses Unterfangen wird durch eine staatliche Steigerung der Nachfrage nicht einfacher. Negativ für die IT-Sicherheit wirkt sich zudem aus, dass der Staat, wenn er eine Sicherheitslücke erworben hat, einen Anreiz hat, dass diese Lücke möglichst lange geheim bleibt, um sie häufiger zu nutzen. Er benötigt aber in der Regel aber schon für die erste Nutzung der Sicherheitslücke eine gewisse Anlaufzeit, weil zunächst die „Trojaner-Software" programmiert werden muss. Der Staat befindet sich während dieser Zeit in einem Wettrennen mit dem Hersteller, der jederzeit die Lücke entdecken und schließen könnte.

b. Zum Ausmaß möglicher Gefahren

Dem Ausmaß der Gefahr durch Cyberangriffe sind auf Grund der Allgegenwärtigkeit informationstechnischer Systeme – wie aktuelle Beispiele zeigen – nahezu keine Grenzen gesetzt. Dies reicht vom Ausspähen von Patientendaten – nach Schätzungen des BSI waren 2020 24,3 Millionen Patientendatensätze im Internet frei zugänglich[210] – bis hin zu großflächigen Angriffen auf kritische Infrastruktur, die unmittelbare Auswirkungen auf eine Vielzahl von Grundrechtsträgern mit sich bringen.

aa. Beispiele größerer Cyberangriffe der letzten Jahre

Zur Darstellung des Ausmaßes der Gefahren sollen nachfolgend nur beispielshaft einige der größeren Cyberangriffe der letzten Jahre angeführt werden.

---

zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html, zuletzt abgerufen am 9. Juli 2021.

210 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 36 f., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 9. Juli 2021.

Hier sind zum einen Angriffe auf Unternehmen der kritischen bzw. systemrelevanten Infrastruktur und staatliche Einrichtungen zu nennen.

(a) *WannaCry*-Angriff im Mai 2017

Bei dem bereits angeführten *WannaCry*-Angriff im Mai 2017 wurden weltweit IT-Systeme angegriffen. Wie bereits dargelegt, handelte es sich bei der ausgenutzten Sicherheitslücke um eine Zero-Day-Schwachstelle, die zuvor mehrere Jahre durch die NSA ausgenutzt und geheim gehalten wurde. Weltweit waren mehr als 75.000 Rechner in rund 100 Ländern von dem Angriff betroffen.[211] Darunter auch der britische Gesundheitsdienst National Health Service (NHS) in mehreren Krankenhäusern. Diese mussten Operationen verschieben und konnten zeitweise keine Notfälle mehr aufnehmen.[212] Des Weiteren wurden auch Systeme der Deutsche Bahn und der Bahn-Logistiktochter Schenker kompromittiert.[213] In Russland war die IT-Infrastruktur mehrerer Banken Ziel des Angriffs.[214] Der *WannaCry*-Angriff erfolgte dabei über eine Schwachstelle im absolut markbeherrschenden Windows-Betriebssystem.

Dies zeigt eine weitere zentrale Gefahr auf. Da ein Großteil von IT-Software (z.B. Windows, Android, MacOS, iOS) sowohl von Privatanwendern als auch von Unternehmen (der kritischen Infrastruktur) und öffentlichen Stellen genutzt wird, sind es die gleichen Schwachstellen, die sowohl von den Nachrichtendiensten zur Überwachung als auch von Kriminellen zu großflächigen, verheerenden Cyber-Angriffen genutzt werden können.

(b) Angriff auf IT-System der Uniklinik Düsseldorf in 2020

Ein weiteres Beispiel ist der Cyberangriff auf die IT-Systeme der Uniklinik Düsseldorf im Herbst 2020. In der Folge musste das Krankenhaus Operationen verschieben und die Notaufnahme musste für mehrere Tage schließen.[215] Ein

---

211 ZEIT-Online, Großer Schaden für 31.000 Dollar, 14. Mai 2017, abrufbar unter https://www.zeit.de/digital/datenschutz/2017-05/wannacry-ransomware-cyberattacke-bitcoin-windows-microsoft, zuletzt abgerufen am 10. Juli 2021.

212 S. BBC, NHS cyber-attack: GPs and hospitals hit by ransomware, 13. Mai 2017, abrufbar unter https://www.bbc.com/news/health-39899646, zuletzt abgerufen am 9. Juli 2021.

213 SPON, 450 Computer der Bahn von „WannaCry"-Virus betroffen, 16. Mai 2015, abrufbar unter https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html, zuletzt abgerufen am 9. Juli 2021.

214 Reuters, WannyCry cyber-attack compromised some Russian banks: central bank, 19. Mai 2017, abrufbar unter https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V, zuletzt abgerufen am 9. Juli 2021.

215 Deutschlandfunk, Der Hackerangriff auf die Uniklinik Düsseldorf und die Folgen, abrufbar unter https://www.deutschlandfunk.de/notaufnahme-geschlossen-der-hackerangriff-auf-die-uniklinik.1773.de.html?dram:article_id=484310, zuletzt abgerufen am 8. Juli 2021.

behandlungsbedürftiger Mensch kam in der Folge sogar zu Tode. Nach dem Angriff nahm die Staatsanwaltschaft Ermittlungen wegen eines Tötungsdelikts auf. Sie leitete ein Todesermittlungsverfahren wegen des Verdachts ein, dass durch den Hackerangriff eine Frau verstorben ist, die in ein weiter entferntes Krankenhaus gebracht werden musste und somit nicht mehr rechtzeitig in der erforderlichen Weise behandelt werden konnte.[216] Bei diesem Hackerangriff waren es Medienberichten zufolge offenbar die unbekannten Täter selbst, die freiwillig eingelenkt und so einen noch größeren Schaden verhindert hatten.[217]

(c) Hackerangriff auf Pipeline in den USA im Mai 2021

So wurde 7. Mai 2021 die Colonial Pipeline Company, die eine der größten Pipelines USA betreibt, Ziel eines Hackangriffs. In der Folge musste die Pipeline vorübergehend stillgelegt werden.[218] Die hierdurch in der Bevölkerung ausgelöste Panik vor einer Benzinknappheit führte zu chaotischen Zuständen an Tankstellen im gesamten Südosten der USA.[219] In der Folge sahen sich mehrere Staaten gezwungen, den nationalen Notstand auszurufen.[220]

(d) Angriff des IT-Dienstleisters Kaseya im Juli 2021

Im Juli 2021 wurde der IT-Dienstleister Kaseya von der mittlerweile berüchtigten Hackergruppierung REvil angegriffen. Die Software des IT-Dienstleisters diente den Hackern als Einfallstor, um die IT-Systeme von weltweit geschätzt bis zu 1.500 Unternehmen zu infizieren. Darunter befanden sich auch deutsche Unternehmen. Dabei spielten die Hacker auf die angegriffenen Systeme – wie auch beim *Wannacry*-Angriff – eine sog. *Ransomware* auf, die alle auf einem System befindlichen Daten verschlüsselt und diese dann nur gegen Zahlung eines Lösegeldes wieder entschlüsselt. Das von REvil geforderte Lösegeld beträgt 70 Millionen US-Dollar.[221] Der Angriff und das

---

216 Süddeutsche Zeitung, Polizei ermittelt nach Hacker-Angriff in einem Todesfall, 17. September 2020, abrufbar unter https://www.sueddeutsche.de/panorama/duesseldorf-uniklinikum-erpressung-hacker-angriff-1.5035140, zuletzt abgerufen am 8. Juli 2021.

217 Süddeutsche Zeitung, Polizei ermittelt nach Hacker-Angriff in einem Todesfall, 17. September 2020, abrufbar unter https://www.sueddeutsche.de/panorama/duesseldorf-uniklinikum-erpressung-hacker-angriff-1.5035140, zuletzt abgerufen am 8. Juli 2021.

218 NY-Times, Cyberattack Forces a Shutdown of a Top U.S. Pipeline, 8. Mai 2021, abrufbar unter https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html, zuletzt abgerufen am 8. Juli 2021.

219 NY-Times, Gas Pipeline Hack Leads to Panic Buying in the Southeast, 11. Mai 2021, abrufbar unter: https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html, zuletzt abgerufen am 8. Juli 2021.

220 Fox-KTVU, Colonial Pipeline attack: White House launches 'all of government' response, 11. Mai 2021, abrufbar unter https://www.ktvu.com/news/colonial-pipeline-attack-amid-service-outage-nc-declares-state-of-emergency-to-help-ensure-fuel-supply, zuletzt abgerufen am 8. Juli 2021.

221 SPIEGEL online, »REvil« erpresst bis zu 1500 Firmen, abrufbar unter https://www.spiegel.de/netzwelt/web/ransomware-bis-zu-1500-firmen-werden-von-revil-erpresst-a-4144c655-54d2-454a-b50c-c8ddbe8f161e, zuletzt abgerufen 8. Juli 2021.

Erpressungsszenario ist zum Zeitpunkt der Erhebung dieser Verfassungsbeschwerde noch gegenwärtig.

(e) Cyber-Angriff auf Landkreis Anhalt-Bitterfeld im Juli 2021

Am 7. Juli 2021 hat der Landkreis Anhalt-Bitterfeld wegen einer schweren Cyberattacke auf das Netzwerk seiner Verwaltung den Katastrophenfall ausgerufen. Dazu sah sich der Kreis gezwungen, nachdem mehrere Server mit einer Schadsoftware infiziert worden waren. Die Verwaltungstätigkeit kam daraufhin vollständig zum Erliegen, sodass Anliegen der Bürgerinnen und Bürger nicht mehr bearbeitet werden konnten. Hierzu zählten auch finanzielle Belange der Bürger, wie etwa die Auszahlung von Sozialleistungen zur Beschreitung des Lebensunterhalts.[222] Zudem wurden personenbezogene Daten von Bürgerinnen und Bürgern veröffentlicht.

bb. Zur Aktualität und Frequenz der Cyberangriffe

Von den fünf vorstehend nur *pars pro toto* aufgezeigten Cyberangriffen fanden drei in den letzten zwei Monaten statt, vier innerhalb des letzten Jahres.

Die tatsächliche Lage im Hinblick auf die Intensität von Cyber-Angriffen durch Ausnutzen von Sicherheitslücken und die Schwere ihrer Folgen hat sich seit der Entscheidung des angerufenen Gerichts in BVerfGE 120, 274 im Jahr 2008 signifikant geändert.

cc. Gefahren für weitere Rechtsgüter

Auch abseits von Angriffen auf kritische bzw. systemrelevante Infrastruktur bringen Cyberattacken gewichtige Gefahren mit sich.

So können Cyberangriffe beispielsweise auch genutzt werden, um Wahlen zu beeinflussen oder zu manipulieren. Dass es sich auch hierbei nicht um eine theoretische Gefahr handelt, haben die Hackerangriffe auf E-Mail-Server im Umfeld der US-amerikanische Präsidentschaftskandidatin Hillary Clinton[223] sowie des ebenfalls US-amerikanischen *Democratic National Comitee* gezeigt.[224] Die

---

222 RND, Katastrophenfall nach Cyberattacke im Landkreis Anhalt-Bitterfeld, https://www.rnd.de/politik/hackerangriff-in-anhalt-bitterfeld-lka-bestaetigt-loesegeldforderung-VQQRFMF7MCAJJXWKMB5OPDQ67U.html, zuletzt abgerufen am 13. Juli 2021.

223 SPIEGEL online, Hillarys schwächste Stelle, 13. Oktober 2016, abrufbar unter https://www.spiegel.de/politik/ausland/hillary-clinton-und-der-email-hack-stecken-donald-trump-und-russland-dahinter-a-1116367.html, zuletzt abgerufen am 10. Juli 2021.

224 Washington Post, How the Russians hacked the DNC and passed its E-Mails to WikiLeaks, 13. Juli 2018, abrufbar unter https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html, zuletzt abgerufen am 10. Juli 2021.

bei dem Angriff erbeuteten Daten wurden dabei von einer ganzen Reihe von Akteuren benutzt, um im Vorfeld der US-Präsidentschaftswahl im Jahre 2016 die Wählerinnen und Wähler zu beeinflussen. Eine Reihe von Experten vermuten dabei, dass ausländische Geheimdienste hinter den Angriffen stehen könnten.[225]

Letztendlich ist das Ausmaß der Gefahr, die von der nicht gesetzlich geregelten staatlichen Geheimhaltung von *Zero-Day*-Schwachstellen ausgeht, nicht abschätzbar und nicht vollends zu erfassen. Klar ist jedoch, dass das Ausmaß der entstehenden Gefahren gravierend ist.

Ohne gesetzliche Regelungen, insbesondere ohne Vorgaben dazu, wann und unter welchen Bedingungen eine Schwachstelle zu melden ist, besteht für die Adressaten des G 10, Nachrichtendienste, die – rechtlich wie faktisch eingeräumte – Möglichkeit, selbst die gefährlichsten *Zero-Day*-Schwachstellen geheim zu halten. Denn die Schaffung einer Ermächtigungsgrundlage zur Quellen-TKÜ ohne gleichzeitige Schaffung rechtlicher Vorgaben für ein Schwachstellenmanagement ist gleichsam ein Persilschein zur autarken Sammlung von Sicherheitslücken, letztlich nach eigenem Gutdünken der Sicherheitsbehörden. Und dies, ohne dass auch nur im Ansatz gesetzlich irgendeine Kontrolle der Sammlung von Sicherheitslücken und Schwachstellen vorgesehen ist. Auch die für die Kontrolle von Maßnahmen nach dem G 10 vorgesehenen Institutionen müssen insoweit nicht über diese Thematik ausdrücklich informiert werden.

4. Art und Rang der verfassungsrechtlich geschützten Rechtsgüter

Aus dem Beispiel wird ersichtlich, dass nicht nur Nähe und Ausmaß der Gefahr durch Cyberangriffe hoch sind, sondern dass gewichtige Rechtsgüter von Verfassungsrang sowie oftmals im Rahmen nur eines Angriffs eine Vielzahl von Grundrechtsträgern betroffen sind. Der tragische Beispielsfall des Hackerangriffs auf die Uniklinik Düsseldorf zeigt, dass letztendlich alle grundrechtlich geschützten Rechtsgüter bis hin zum Leben i.S.d. Art. 2 Abs. 2 Satz 1 GG durch Cyberangriffe gefährdet sind. Dies liegt schlicht in der Tatsache begründet, dass mittlerweile alle Lebensbereiche von Informationstechnik durchzogen sind, sodass Gefahren für das Eigentum (Art. 14 Abs. 1 GG), die Berufsausübung (Art. 12. Abs. 1 GG), das Leben und die Gesundheit (Art. 2 Abs. 2 Satz 1 GG), Informationen aus dem Kernbereich privater Lebensgestaltung eines Menschen (Art. 1 Abs. 1 GG), aber auch wie aufgezeigt andere verfassungsrechtlich geschützte Güter wie freie,

225 Washington Post, How the Russians hacked the DNC and passed its E-Mails to WikiLeaks, 13. Juli 2018, abrufbar unter https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html, zuletzt abgerufen am 10. Juli 2021.

demokratische Wahlen (Art. 38 Abs. 1 Satz 1 GG) durch Cyberangriffe, die Sicherheitslücken und Schwachstellen in IT-Systemen ausnutzen, bestehen.

Hierbei ist auch zu berücksichtigen, dass der Effektivitätsverlust bei einem Nachrichtendienst im Falle einer Entscheidung, eine IT-Schwachstelle nicht zu nutzen, sondern sie wegen der erheblichen Gefahren zu melden, damit sie rasch geschlossen werden kann, wesentlich geringer ist als bei Gefahrenabwehrbehörden wie Polizeibehörden. Denn die Überwachungsmaßnahme weit im Vorfeld dient keiner unmittelbaren Gefahrenabwehr.

5. Verletzung der Schutzpflicht

Durch die Schaffung von Ermächtigungsgrundlagen zur Quellen-TKÜ (*notabene* nicht nur im G 10) und damit zum Einsatz des Staatstrojaners werden die Sicherheitsbehörden – wie dargelegt – geradezu herausgefordert, sich ein Arsenal an (i.d.R. besonders gefährlichen) *Zero-Day*-Sicherheitslücken zu verschaffen. Der Gesetzgeber hat es gleichzeitig unterlassen, gesetzliche Regelungen zu schaffen, wie mit der staatlichen Kenntnis dieser Sicherheitslücken im Lichte des Risikos für die Allgemeinheit konkret umzugehen ist.

Hierdurch wird die aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG folgende grundrechtliche Schutzpflicht verletzt.

Auch der Erlass von Regelungen, die die Infiltration von IT-Systemen vorsehen und hierbei erkennbar auf die Ausnutzung solcher Sicherheitslücken abzielen (wie vorliegend § 11 Abs. 1a G 10), berühren das IT-Grundrecht, wenn nicht zugleich Regelungen zum Umgang mit diesen Sicherheitslücken erlassen werden.

Dabei wird durch die Beschwerdeführer nicht verkannt, dass dem Gesetzgeber bei der Erfüllung der festgestellten Schutzpflicht ein weiter Einschätzungs-, Wertungs- und Gestaltungsbereich zukommt, der auch Raum lässt, konkurrierende öffentliche und private Interessen zu berücksichtigen. Nach der Rechtsprechung des angerufenen Gerichts hängt der Einschätzungsspielraum des Gesetzgebers dabei von verschiedenen Faktoren ab, insbesondere von der Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden und der Bedeutung der auf dem Spiel stehenden Rechtsgüter. Mit Blick darauf ist der grundrechtliche Schutzanspruch nur darauf gerichtet, dass die öffentliche Gewalt Vorkehrungen zum Schutze des Grundrechts trifft, die nicht gänzlich ungeeignet oder völlig unzulänglich sind.[226]

---

226 BVerfGE 77, 170, 214 f.

a. Vorhandene Regelungen reichen nicht aus

Die „vorhandenen“ Regelungen zum Umgang mit *Zero-Day*-Schwachstellen reichen nicht aus, um der grundrechtlichen Schutzpflicht zu genügen.

Ein effektives Schwachstellenmanagement ist über das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht gewährleistet. Gem. § 3 Abs. 1 Nr. 14 BSIG ist eine der Aufgaben des BSI, die

> „Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen“.

Zur Erfüllung dieser Aufgabe ermächtigt § 7 Abs. 1 Nr. 1 lit. a BSIG das BSI dazu, Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten an die Öffentlichkeit oder betroffene Kreise zu richten.

Ein effektives Schwachstellenmanagement setzt aber zwingend voraus, dass das zuständige BSI Kenntnis von den Sicherheitslücken erlangt, um über die Frage einer Warnung entscheiden zu können. Dies ist bei Kenntniserlangung der Nachrichtendienste (und übrigen Sicherheitsbehörden) von den für die Quellen-TKÜ benötigten *Zero-Day*-Sicherheitslücken nicht gewährleistet. Zwar regelt § 4 Abs. 3 BSIG, dass Bundesbehörden unverzüglich das BSI zu unterrichten haben, sofern ihnen Informationen über Sicherheitslücken bekannt werden, die für die Erfüllung von Aufgaben des BSI oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind. Dies steht jedoch zum einem unter den Vorbehalt, dass andere Vorschriften dem nicht entgegenstehen. Zum anderen nimmt § 4 Abs. 4 BSIG von der oben genannten Unterrichtungspflicht solche Informationen aus, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen. Somit fallen gerade Sicherheitslücken, die von Nachrichtendienste zum Zwecke der Quellen-TKÜ ausgenutzt werden, auf Grund der Geheimschutzregelungen aus der Unterrichtungspflicht hinaus.[227] Vielmehr ist es in der gegenwärtigen einfachgesetzlichen Ausgestaltung für die Nachrichtendienste (ebenso wie für die übrigen Sicherheitsbehörden) legal, Sicherheitslücken im Hinblick auf die beabsichtigte eigene Ausnutzung nicht dem BSI zu melden. Auch durch das IT-Sicherheitsgesetz 2.0 vom Mai 2021 blieb diese Rechtslage unverändert.

---

227 Vgl. *Buchberger,* in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, BSIG, § 4 Rn. 4

b. Ungeeignete und völlig unzulängliche Maßnahmen – kein hinreichendes Schwachstellenmanagement

Auch außerhalb gesetzlicher Regelungen besteht in der Bundesrepublik Deutschland kein hinreichendes Schachstellenmanagement, das der aus dem IT-Grundrecht folgenden Schutzpflicht genügen würde. Dies zeigt bereits ein Blick in den Entwurf der Cybersicherheitsstrategie für Deutschland 2021 des Bundesministeriums des Innern, für Bau und Heimat.[228] In dem Entwurf heißt es:

> „**Was wollen wir erreichen?** Eine ausgewogene behördenübergreifende Strategie zum Umgang mit 0-day-Schwachstellen nach den jeweils geltenden gesetzlichen Vorgaben bei den Strafverfolgungs- und Sicherheitsbehörden über bereits vorhandene interne Behördenvorgaben hinaus bringt die Interessen der Cyber- und Informationssicherheit sowie der Strafverfolgungs- und Sicherheitsbehörden in einen angemessenen Ausgleich. Grundlage dafür sind standardisierte Prozesse bei den Sicherheitsbehörden für einen sicheren und sachgerechten Umgang mit Schwachstellen und Exploits.“[229]
>
> „**Woran lassen wir uns messen?** Die Bundesregierung wird die Erreichung des Ziels anhand des folgenden Kriteriums überprüfen:
>
> Es ist ein verbindliches Vorgehen etabliert, das den verantwortungsvollen Umgang mit 0-day Schwachstellen und Exploits regelt.“[230]

Fakt ist damit: Vier Jahre nach Einrichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich beim Bundesinnenministerium und 30 Jahre nach der Einrichtung des Bundesamtes für Sicherheit in der Informationstechnik bestehen noch nicht einmal behördenübergreifend geltende interne allgemeine Verfahrensregelungen bzw. Abwägungskriterien für den Umgang mit Zero-Day Schwachstellen. Schwachstellen, die – wie

---

228 Bundesministerium des Innern, für Bau und Heimat, Entwurf einer Cybersicherheitsstrategie für Deutschland 2021, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/06/entwurf-cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 10. Juli 2021.

229 Bundesministerium des Innern, für Bau und Heimat, Entwurf einer Cybersicherheitsstrategie für Deutschland 2021, S. 88, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/06/entwurf-cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 10. Juli 2021.

230 Bundesministerium des Innern, für Bau und Heimat, Entwurf einer Cybersicherheitsstrategie für Deutschland 2021, S. 89, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/06/entwurf-cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 10. Juli 2021.

mittlerweile mehr als deutlich durch viele Vorfälle gezeigt – erhebliche Gefahren für eine Vielzahl von Grundrechtsträgern und für gewichtige Rechtsgüter von Verfassungsrang mit sich bringen.

Die Vereinigten Staaten von Amerika haben den Schwachstellenmanagementprozess (*Vulnerability Equities Process*), an dem nach dem *Entwurf* der Cybersicherheitsstrategie 2021 (!) des Bundesinnenministeriums hierzulande gegenwärtig „gearbeitet“[231] wird, bereits im Jahre 2008 etabliert.[232] Die Gefahren fehlender behördenübergreifender Prozesse in sicherheitsrelevanten Fragen hat etwa der Anschlag auf dem Berliner Breitscheidplatz im Dezember 2016 auf tragische Weise gezeigt.

Wenn der Gesetzgeber trotz dieser fehlenden Regelungen nicht nur unzweifelhaft Anreize, sondern den Sicherheitsbehörden einschließlich der Nachrichtendienste durch Schaffung der Quellen-TKÜ[233] faktisch den Auftrag erteilt, *Zero-Day*-Schwachstellen zu sammeln (einschließlich des Erwerbs), zu horten und geheim zu halten, ist dies mit Blick auf die grundrechtliche Schutzpflicht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG unzulänglich und völlig unzureichend. Dies jedenfalls dann, wenn der Gesetzgeber die oben angesprochenen Verfahrensregelungen nicht im gleichen Zuge trifft.

Zu berücksichtigen ist hierbei auch, dass inzwischen neben den Nachrichtendiensten des Bundes und der Länder im G 10 eine Vielzahl weiterer Sicherheitsbehörden im Bund und in den Ländern sowie daneben alle Strafverfolgungsbehörden durch entsprechende Befugnisse zum Einsatz von Staatstrojanern in dieselbe Lage mit demselben Anreiz versetzt werden. Das Interesse, Sicherheitslücken zu horten, wird damit nur noch größer.

c. Erfordernis einer gesetzlichen Regelung – Parlamentsvorbehalt

Selbst wenn eine solche – längst überfällige – behördenübergreifende Regelung als verwaltungsinterne Vorgabe, etwa in einer Dienstvorschrift, existieren würde, würde sie der grundrechtlichen Schutzpflicht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG *sub specie* des IT-Grundrechts nicht genügen.

---

231 Bundesministerium des Innern, für Bau und Heimat, Entwurf einer Cybersicherheitsstrategie für Deutschland 2021, S. 88, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/06/entwurf-cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 10. Juli 2021.

232 S. Epic.org, Vulnerabilities Equities Process, abrufbar unter https://epic.org/privacy/cybersecurity/vep/, zuletzt abgerufen am 10. Juli 2021.

233 Dasselbe gilt für das Instrument der Online-Durchsuchung, das auf derselben technischen Basis des Ausnutzens von IT-Sicherheitslücken basiert.

Nach der Rechtsprechung des angerufenen Gerichts verpflichten das Rechtsstaatsprinzip und das Demokratieprinzip den Gesetzgeber, wesentliche Entscheidungen selbst zu regeln und nicht der Exekutive zu überlassen (sog. Parlamentsvorbehalt).[234]

Unabhängig davon, dass keine gesetzliche Verordnungsermächtigung zur Regelung eines hinreichenden Schwachstellenmanagements existiert, bedarf es einer parlamentsgesetzlichen Ausgestaltung des Schwachstellenmanagements. Sowohl die Vielzahl der betroffenen Grundrechtsträger als auch der Rang und das Gewicht der gefährdeten Rechtsgüter macht die Entscheidung darüber ob, wann und wie eine aufgedeckte *Zero-Day*-Schwachstelle bewusst dem Hersteller oder der Öffentlichkeit nicht bekannt gegeben werden soll, um sie als Einfallstor für heimliche Überwachungsmaßnahmen durch staatliche Sicherheitsbehörden zu nutzen, zu einer absolut Wesentlichen. Der Gesetzgeber muss dabei in einem absoluten Mindestmaß festlegen, (a) dass die zuständige Stelle von allen staatlichen Stellen über bekannte IT-Sicherheit informiert wird und (b) nach welchen Kriterien eine Schwachstelle zu bewerten ist und unter welchen Voraussetzungen und in welchem Verfahren sie geheim gehalten werden kann oder an den Hersteller des IT-Systems bzw. an die Öffentlichkeit gemeldet werden muss, damit Abhilfe geschaffen werden kann und die Sicherheitslücke geschlossen oder zumindest das mit ihr einhergehende Risiko reduziert wird. Wenn eine Regelung geheim gehalten wird, wird diese Abwägungsentscheidung zudem zu begründen und regelmäßig zu überprüfen sein.

6. Ergebnis

Die gegenwärtige Lage verletzt die Beschwerdeführer in ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Ausgestaltung von Schutzpflichten nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

V. Verfahrensrechtliche Mängel der Quellen-TKÜ und der beschränkten Online-Durchsuchung

1. Unzureichender Schutz des Kernbereichs privater Lebensgestaltung

§ 3a G 10 genügt nicht den verfassungsrechtlichen Anforderungen an verfahrensrechtliche Schutzvorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

Heimliche Überwachungsmaßnahmen staatlicher Stellen haben ausweislich der Rechtsprechung des angerufenen Gerichts einen unantastbaren Kernbereich

234 Vgl. nur BVerfGE 41, 251, 259 f.; 45, 400, 417 f.

privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt.[235]

Dieser Schutz soll hinsichtlich der beschränkten Online-Durchsuchung nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 durch § 3a G 10 sichergestellt werden. Indes genügt diese Regelung in mehrfacher Hinsicht nicht den verfassungsrechtlichen Anforderungen.

Der Gesetzgeber hat schon im Ausgangspunkt übersehen, dass die o.g. Maßnahme, die zum Teil auch „Quellen-TKÜ plus" oder „erweiterte Quellen-TKÜ" genannt wird, tatsächlich eine Online-Durchsuchung darstellt und somit am IT-Grundrecht gem. Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG auszurichten ist. § 3a G 10 nimmt insoweit jedoch hinsichtlich des Schutzes des Kernbereichs privater Lebensgestaltung keinerlei Differenzierung vor. Hierdurch wird verkannt, dass die Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung von der konkreten Maßnahme abhängen. Die vom angerufenen Gericht formulierten Vorgaben für den Kernbereichsschutz bei Online-Durchsuchungen werden in der Folge nicht hinreichend berücksichtigt.

Bei heimlichen Eingriffen in informationstechnische Systeme ist gesetzlich vorzusehen, dass – soweit vorhanden – technische Sicherungen einzusetzen sind, mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden können.[236] Eine entsprechende Regelung findet sich etwa in der Parallelvorschrift in § 100d Abs. 3 Satz 1 StPO. § 3a G 10 enthält eine solche Regelung hingegen nicht. Hierdurch wird das verfassungsrechtlich erforderliche Schutzniveau für den Kernbereich privater Lebensgestaltung unterschritten.

Darüber hinaus ist der Kernbereich privater Lebensgestaltung beim heimlichen Zugriff auf informationstechnische Systeme gesetzlich auch und besonders auf der Aus- und Verwertungsebene zu schützen. Auf dieser sog. zweiten Stufe ist eine gesetzliche Regelung dahingehend erforderlich, dass die erhobenen Daten frühzeitig durch eine unabhängige Stelle gesichtet werden.[237] Eine solche (Vor-)Prüfung ist bei Maßnahmen nach § 11 Abs. 1a Satz 2 i.V.m. § 3 Abs. 1 G 10 nicht – zumindest nicht in allen Fällen – vorgesehen. Auch insoweit entspricht § 3a G 10 den verfassungsrechtlichen Anforderungen nicht.

Bemerkenswert ist, dass der Gesetzgeber die Anforderungen an den Kernbereichsschutz mit Einführung des neuen § 3a Abs. 2 G 10 gegenüber der vorigen Rechtslage sogar verringert hat. Demnach können automatische Aufzeichnungen nach § 3a Abs. 1 Satz 3 G 10 bei Gefahr im Verzug unter

---

235 BVerfGE 120, 274, 335 m.w.N.; vgl. hierzu auch BVerfGE 141, 220, 277 f.

236 Siehe hierzu BVerfGE 141, 220, 307.

237 BVerfGE 109, 279, 333 f.; 120, 274, 339; 141, 220, 307.

Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, gesichtet werden. Hierdurch wird von § 3a Abs. 1 Satz 4 G 10 abgewichen, wonach die Aufzeichnungen unverzüglich einem bestimmten Mitglied der G 10-Kommission oder seinem Stellvertreter zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen sind.

Zu bedenken ist, dass Nachrichtendienste stets im Vorfeld von konkreten Gefahren tätig werden, sodass das Bedürfnis für eine Regelung bei Gefahr im Verzug im hiesigen Zusammenhang wenigstens zweifelhaft erscheint. Jedenfalls entspricht die konkrete Ausgestaltung nicht den verfassungsrechtlichen Anforderungen. Denn nach § 3a Abs. 2 G 10 genügt bereits die bloße Aufsicht eines Bediensteten mit der Befähigung zum Richteramt. Indes ist es – wenn schon die Anforderungen von § 3a Abs. 1 Satz 4 G 10 in Eilfällen gesenkt werden sollen – verfassungsrechtlich geboten, dass der Bedienstete mit der Befähigung zum Richteramt als neutrale Stelle vorab eine eigenverantwortliche und selbständige Durchsicht vornimmt, um den Interessen des Betroffenen gerecht zu werden.

§ 3a G 10 bleibt damit insgesamt hinter den verfassungsrechtlichen Anforderungen zurück.

2. Unzulässige Erstreckung der Überwachung auf weitere Kennungen, § 11 Abs. 1b G 10

Auch die in § 11 Abs. 1b G 10 vorhandene Regelung zur Erstreckung der Überwachung auf weitere Kennungen verstößt sowohl gegen Art. 10 Abs. 1 GG als auch gegen das IT-Grundrecht in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Nach dem neu eingefügten § 11 Abs. 1b Satz 1 G 10 ist die Erstreckung auf weitere Kennungen derjenigen Person möglich, gegen die sich die Anordnung richtet, sofern diese nach der Anordnung bekannt werden. Eine entsprechende Erstreckung soll gem. § 11 Abs. 1b Satz 2 G 10 nur bei solchen Personen nicht möglich sein, gegen die sich die Anordnung richtet, weil auf Grund bestimmter Tatsachen anzunehmen ist, dass der Verdächtige ihren Anschluss benutzt (§ 3 Abs. 2 Satz 2 Variante 3 G 10).

Diese Regelung wird den verfassungsrechtlichen Anforderungen nicht gerecht.

Sie führt zunächst zu einer Aushebelung wesentlicher Verfahrensvorschriften, die dem Schutz des Adressaten der Maßnahme dienen. So ist für die Erstreckung auf weitere Kennungen weder ein Antrag im Sinne des § 9 G 10, noch eine Anordnung nach § 10 G 10, noch die Zustimmung der G 10-Kommission nach § 15 Abs. 6 G 10 erforderlich. Zudem ist darauf hinzuweisen, dass in dem ursprünglichen Gesetzentwurf noch zwei weitere Sätze in § 11 Abs. 1 G 10

vorgesehen waren, die wenigstens gewisse Melde- und Unterrichtungspflichten – die *notabene* auch keinen hinreichenden Schutz boten – vorgesehen haben;[238] indes sind diese im weiteren Verlauf des Gesetzgebungsverfahrens ohne erkennbaren Grund gestrichen worden.[239] § 11 Abs. 1b G 10 erlaubt der verantwortlichen Behörde damit ohne eine entsprechende Kontrollinstanz eine erhebliche Ausweitung der Überwachung der Kommunikation einer Zielperson. Berücksichtigt man, wie weit der Begriff der „Telekommunikation" verstanden werden kann, kann dies erhebliche Auswirkungen haben und auch die Verhältnismäßigkeit einer Maßnahme beeinflussen: Enthielt etwa die ursprüngliche Anordnung nur die Überwachung eines Kontos bei einem bestimmten Messenger-Dienst, könnte der Nachrichtendienst diese Anordnung auf sämtliche Kommunikation ausweiten – einschließlich der Kommunikation mit Cloud-Diensten und des Surfverhaltens im Internet. Sind noch nicht einmal nachträgliche Genehmigungsvorbehalte und Löschungsanordnungen vorgesehen, wie in der Eilfallregelung des § 15a G 10, hebelt dies wesentliche Schutzvorkehrungen noch massiver aus. Mithin ist § 11 Abs. 1b G 10 bereits in verfahrensrechtlicher Hinsicht verfassungsrechtlich defizitär.

Darüber hinaus ist die Regelung in materieller Hinsicht gemessen an den verfassungsrechtlichen Anforderungen zu unbestimmt. Denn angesichts des weiten Begriffs der Telekommunikation ist kaum zu überblicken, was unter „Kennung von Telekommunikationsanschlüssen" in den Anwendungsbereich von § 11 Abs. 1b Satz 1 G 10 fällt. Betroffen sind damit keineswegs nur „klassische" Telefonnummern, E-Mail-Adressen oder Messenger-Profile, sondern letztlich sämtliche Kennungen, die im Internetverkehr eine Zuordnung zu einer Adresse ermöglichen.

Letztlich wird hier eine sehr umfassende Überwachung ohne nennenswerte verfahrensrechtliche Sicherungen ermöglicht. Im Ergebnis ist § 11 Abs. 1b G 10 sowohl bei einem Eingriff in Art. 10 Abs. 1 GG als auch – und besonders – bei einem Eingriff in das IT-Grundrecht gem. Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG unverhältnismäßig.

3. Unzureichende Regelung zur Benachrichtigungspflicht – zu weitreichende Ausnahmen von der Pflicht zur Benachrichtigung des Betroffenen, § 12 Abs. 1 Satz 2, Satz 5 G 10

Die gesetzlich in § 12 Abs. 1 Satz 2 und Satz 5 G 10 vorgesehenen Ausnahmen von der Pflicht zur Benachrichtigung des Betroffenen über Beschränkungsmaßnahmen nach § 3 nach ihrer Einstellung entsprechen nicht

238 BT-Drs. 19/24785, S. 11.
239 BT-Drs. 19/30477, S. 7.

den verfassungsrechtlichen Anforderungen und verstoßen daher gegen Art. 10 Abs. 1 sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Nach § 12 Abs. 1 Satz 1 G 10 sind dem Betroffenen Beschränkungsmaßnahmen gem. § 3 G 10 nach ihrer Einstellung mitzuteilen. Hierunter fallen auch Beschränkungsmaßnahmen nach § 3 Abs. 1 G 10 i.V.m. § 11 Abs. 1a G 10. Von dieser Benachrichtigungspflicht gegenüber dem Betroffenen lassen § 12 Abs. 1 Satz 2, Satz 5 G 10 Ausnahmen in einem Ausmaß zu, das den verfassungsrechtlichen Anforderungen nicht gerecht wird. Dies gilt für sämtliche Maßnahmen, für die in § 12 Abs. 1 Satz 1, Abs. 2 Satz 1 G 10 eine Benachrichtigungspflicht grundsätzlich vorgesehen ist. Daher sind auch aus diesem Grund die Eingriffe in die Grundrechte der Beschwerdeführer aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (durch die beschränkte Online-Durchsuchung gem. § 11 Abs. 1 lit. a Satz 2 i.V.m. § 3 G 10) und Art. 10 Abs. 1 GG (durch alle Übrigen Maßnahmen, für die die Benachrichtigungspflicht vorgesehen ist) unverhältnismäßig.

Zu den Anforderungen an eine verfassungskonforme Regelung heimlicher Überwachungsmaßnahmen gehören – als verfahrensrechtliche Schutzvorkehrungen – die gesetzliche Anordnung von Benachrichtigungspflichten. Verfassungsrechlich folgt dies aus dem Grundrecht, in das die konkrete Überwachungsmaßnahme eingreift. Vorliegend ist dies Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie Art. 10 Abs. 1 GG), ferner Art. 19 Abs. 4 Satz 1 GG.

Ausnahmen von Pflicht zur Benachrichtigung kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen. Ausnahmeregelungen sind jedoch auf das unbedingt Erforderliche zu beschränken. Sie müssen zudem dem Gebot der Normenklarheit und Bestimmtheit genügen.[240]

§ 12 Abs. 1 Satz 2, Satz 5 G 10 enthalten jedoch viel zu weit gefasste Ausschlusstatbestände und verfehlen daher die verfassungsrechtlichen Anforderungen.

Der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 1 G 10 geht bereits sehr weit. Danach unterbliebt die Benachrichtigung zwingend, solange eine Gefährdung des Zwecks der Beschränkung „nicht ausgeschlossen werden kann“. Die Sicherung des Überwachungszwecks ist zwar grundsätzlich ein verfassungsrechtlich legitimer und tragfähiger Grund, die Benachrichtigung zurückzustellen.[241] Dem Wortlaut der Norm zufolge genügen jedoch bereits

240 BVerfGE 141, 220, 282 f.

241 Vgl. etwa BVerfGE 129, 208, 254; 141, 220, 282 f.

entfernte Risiken, um den Ausnahmetatbestand greifen zu lasen. Ausreichend ist, dass eine Gefährdung des Überwachungszwecks lediglich „nicht auszuschließen“ ist. Angesichts des weit gefassten Aufklärungsauftrags der Verfassungsschutzbehörden wird sich kaum je mit Sicherheit ausschließen lassen, dass eine Benachrichtigung keine Risiken birgt. Gerade im Bereich des Nachrichtendienstwesens, wo Geheimhaltungs- und Sicherheitsbelange besonders sensibel von Angehörigen der Nachrichtendienste bewertet werden, führt diese gesetzlich so großzügige Ausnahme in der Praxis faktisch dazu, dass eine Benachrichtigung problemlos nahezu immer zurückgestellt werden kann.

Die Benachrichtigungspflicht wird durch § 12 Abs. 1 Satz 2 Alt. 1 G 10 daher unverhältnismäßig weit beschränkt. Von Verfassungs wegen erforderlich ist zumindest eine verfassungskonforme Auslegung dahingehend, dass die Benachrichtigung nur dann ausgeschlossen wird, wenn konkrete Tatsachen für eine Gefährdung des Überwachungszwecks vorliegen.[242]

Der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 2 G 10, der die Benachrichtigung ausschließt, solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist, ist ebenso unverhältnismäßig. Die hierbei verwendeten Begriffe des Bundes- oder Landeswohls sind ebenso wie der Begriff der übergreifenden Nachteile weitgehend unbestimmt. Sie sind letztlich nicht geeignet, den Grund für eine Zurückstellung der Benachrichtigung einzugrenzen. Ausweislich des Wortlauts der Norm müssen zudem die Nachteile in keinem zwingenden Zusammenhang mit dem Überwachungszweck stehen. In der Folge wird auch hierdurch der der Ausnahmetatbestand nicht konkretisiert. Letztlich lässt sich unter das Wohl des Bundes oder eines Landes der gesamte Aufgabenkreis der Verfassungsschutzbehörden oder auch jeder anderen Behörde subsumieren. Zudem müssen die befürchteten Nachteile nach dem Wortlaut von § 12 Abs. 1 Satz 2 Alt. 2 G 10 in keinem Zusammenhang mit dem Überwachungszweck stehen, so dass der Ausnahmetatbestand auch hierdurch nicht konkretisiert wird.

Bei Licht betrachtet genügen damit annähernd beliebige behördliche Opportunitätserwägungen dafür, um die grundsätzliche Benachrichtigungspflicht zeitweise zurückzustellen oder auch auf der Grundlage von § 12 Abs. 1 Satz 5 G 10 endgültig auszuschließen. Diese Bewertung stellt der betreffende Nachrichtendienst zudem autark an. *In conctreo* hat es der Gesetzgeber in verfassungsrechtlich relevanter Form versäumt, den Ausnahmetatbestand zum Schutz des Staatswohls näher zu spezifizieren und auf

242 Implizit verlangt solche positiven Anhaltspunkte auch BVerfGE 100, 313, 397 f.; vgl. ferner die nochmals einschränkende Auslegung des ohnehin deutlich restriktiver gefassten Ausnahmetatbestands des § 20w Abs. 2 Satz 1 Hs. 2 BKAG a.F. durch BVerfGE 141, 220, 320.

diese Weise auf hinreichend gewichtige Gründe für eine Annahme einer Ausnahme von der grundsätzlichen Benachrichtigungspflicht zu beschränken. Es hätte nahegelegen, hierbei die spezifisch nachrichtendienstlichen Belange wie die Interessen im Zusammenhang mit der *Third Party Rule* und den Schutz von nachrichtendienstlichen Beziehungen mit ausländischen Diensten als Ausnahmetatbestand von der Benachrichtigungspflicht zu formulieren.[243]

Auch die Tatsache, dass der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 2 G 10 weitgehend wörtlich dem Urteil des Bundesverfassungsgerichts vom 14. Juli 1999 entstammt[244] führt zu keiner anderen Bewertung. Insbesondere wird hierdurch nicht seine Verfassungsmäßigkeit konstituiert. Denn das angerufene Gericht ist nicht der Gesetzgeber sondern dazu berufen, grundrechtliche Grenzen der Rechtsetzung zu bestimmen. Dies hat es getan. Es ist originäre Aufgabe des Gesetzgebers, etwaige Regelungsspielräume durch die Schaffung einfachen Rechts hinreichend normenklar auszufüllen und auf diese Weise Verfassungsrecht zu konkretisieren. Dieser Aufgabe kann sich der Gesetzgeber hingegen nicht dadurch entledigen, indem er schlicht Formulierungen aus einer Urteilsbegründung des angerufenen Gerichts in Gesetzesform gießt. Urteilsbegründung und imperativer Normbefehl eines Gesetzes sind bereits ihrem Wesen nach grundlegend unterschiedliche Formen der Artikulation. Ein – zunehmend in der Gesetzgebung des Sicherheitsrechts erkennbares – schlichtes Abschreiben dieser Formulierungen führt nicht nur zu oft schwerlich verständlichen Gesetzesnormen; es genügt auch nicht den Anforderungen daran, hinreichend normenklare Gesetze zu schaffen und gesetzgeberische Regelungsspielräume auszufüllen.

4. Verfassungsrechtliche Mängel der Übermittlungsvorschriften in § 4 Abs. 4 G 10

Die in § 4 Abs. 4 G 10 enthaltenen Übermittlungsvorschriften genügen nicht den verfassungsrechtlichen Anforderungen, sondern verfehlen diese von dem angerufenen Gericht in mehreren Judikaten konstatierten Anforderungen evident. Die Norm in § 4 Abs. 4 G 10 verstößt gegen den Grundsatz der Verhältnismäßigkeit.

a. Inhalt der Übermittlungsvorschriften

§ 4 Abs. 4 Satz 1 G 10 sieht eine Übermittlungsbefugnis zur Verhinderung oder Aufklärung von Straftaten (Nr. 1), zur Verfolgung von Straftaten (Nr. 2) sowie zur Vorbereitung eines Parteiverbotsverfahrens nach Art. 21 Abs. 2 Satz 2 GG (Nr. 3). § 4 Abs. 4 Satz 2 ordnet daneben bei Übermittlung an ausländische

243 Vgl. die beispielhafte Aufzählung bei BVerfGE 100, 313, 398.
244 Vgl. BVerfGE 100, 313, 398.

öffentliche Stellen sowie an über- und zwischenstaatliche Stellen daneben die Anwendbarkeit von § 19 Abs. 3 Satz 2 und 4 BVerfSchG an. Bei dieser Verweisung darf angenommen werden, dass es sich um eine dynamische Verweisung handelt.

b. Verfassungsrechtlicher Maßstab

Das angerufene Gericht hat den verfassungsrechtlichen Maßstab an Übermittlungsvorschriften für die Datenweitergabe von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden ebenso wie für eine Übermittlung an ausländische öffentliche Stellen klar festgelegt.[245]

Im Urteil zum *Antiterrordateigesetz* hat das angerufene Gericht erklärt:

> „(cc) Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, unterliegen angesichts dieser Unterschiede gesteigerten verfassungsrechtlichen Anforderungen. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt insoweit ein informationelles Trennungsprinzip. Danach dürfen Daten zwischen den Nachrichtendiensten und Polizeibehörden **grundsätzlich nicht ausgetauscht** werden. Einschränkungen der Datentrennung sind **nur ausnahmsweise zulässig**. Soweit sie zur operativen Aufgabenwahrnehmung erfolgen, begründen sie einen **besonders schweren Eingriff**. Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss deshalb **grundsätzlich einem herausragenden öffentlichen Interesse** dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt. Dies muss durch **hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein**; auch die Eingriffsschwellen für die Erlangung der Daten dürfen hierbei **nicht unterlaufen werden**.“[246]
>
> (Hervorhebungen diesseits)

Im Urteil zur *Ausland-Ausland-Fernmeldeaufklärung* hat das angerufene Gericht die Grundsätze zur Datenübermittlung jüngst ausführlich dargelegt.[247] Es hat insbesondere festgestellt:

---

245 S. zur Rechtsprechung bis zum Urteil zur Antiterrordatei in BVerfGE 133, 277 eingehend *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 197 ff. *et passim*.

246 BVerfGE 133, 277 ff., Rn. 123.

247 BVerfGE 154, 152 ff., Rn. 211 ff. m.w.N. zur verfassungsgerichtlichen Rechtsprechung.

> „f) Insgesamt genügen die Übermittlungsvorschriften, die überwiegend auf den in ihrer Fassung schon älteren und an die Entwicklung der Rechtsprechung nicht hinreichend angepassten Strukturen des Bundesverfassungsschutzgesetzes und anderer Sicherheitsgesetze beruhen, den verfassungsrechtlichen Anforderungen nicht. In formeller Hinsicht fehlt es überdies für alle Übermittlungstatbestände an einer Pflicht zur Protokollierung der Übermittlung (oben Rn. 229) sowie zur Nennung der für die Übermittlung in Anspruch genommenen Rechtsgrundlage (oben Rn. 229).“[248]

Dieser Schlussfolgerung unterfallen auch die mit dieser Verfassungsbeschwerde angegriffenen Übermittlungsvorschriften.[249]

c. Auswirkungen auf § 4 Abs. 4 G 10

Die durch § 4 Abs. 4 Nr. 1 lit. a und b G 10 in Bezug genommenen Straftatenkataloge ermöglichen eine Übermittlung auch in Fällen, in denen die Straftat nicht derart schwer wiegt, dass diese den mit der Übermittlung verbundenen Grundrechtseingriff rechtfertigen kann. Dies gilt insbesondere für Daten, die im Wege einer eingriffsintensiven Überwachungsmaßnahme nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 1 und 2 G 10 gewonnen wurden. Zudem genügt beim Katalog des § 4 Abs. 4 Nr. 1 lit. a G 10 bereits die niedrige Schwelle der „tatsächlichen Anhaltspunkte“, um eine Übermittlungsbefugnis auszulösen.

Die von § 4 Abs. 4 G 10 sowohl für Übermittlungen zur Verhinderung oder Aufklärung von Straftaten (Nr. 1), als auch zur Verfolgung von Straftaten (Nr. 2) in Bezug genommenen Straftatenkataloge fallen dadurch auf, dass sie nicht durchgängig von dem Gewicht des zu schützenden Rechtsguts bzw. der Schwere einer Straftat dominiert werden.[250] Sie enthalten etwa auch Übermittlungsbefugnis bei Verdacht eines Verstoß gegen das Aufenthaltsgesetz und im Falle einer (auch leichtfertigen) Geldwäsche nach § 261 StGB (§ 7 Abs. 4 Satz 1 G 10). Überprüft man die vorgenannten Katalogtaten des G 10 anhand des bestehenden verfassungsrechtlichen Maßstabs, insbesondere in der Ausprägung, die es im Urteil des angerufenen Gerichts zum *Antiterrordateigesetz* und im Urteil zur *Ausland-Ausland-Fernmeldeüberwachung* erfahren hat, so verstößt die Übermittlungsbefugnis bei Straftaten nach § 20 Abs. 1 Nr. 1-4 VereinsG evident gegen den Grundsatz der Verhältnismäßigkeit. Offensichtlich unverhältnismäßig ist auch die Übermittlungsbefugnis bei

---

248 BVerfGE 154, 152 ff., Rn. 319.

249 S. zur verfassungsrechtlichen Bewertung des § 4 Abs. 4 G 10 bereits vor dem BNDG-Urteil ausführlich *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 424 ff. m.w.N.

250 *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 442.

Straftaten nach § 95 Abs. 1 Nr. 1–4 AufenthaltsG.[251] Danach wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer gegen verschiedene Ausprägungen des Aufenthaltsrechts verstößt. Der Straftatbestand dient der Durchsetzung der sich aus den verwaltungsrechtlichen Vorschriften des Aufenthaltsgesetzes ergebenden Verhaltenspflichten und bezweckt unmittelbar die „Stabilisierung der verwaltungs- rechtlichen Ordnungssysteme" sowie mittelbar die materiellen Interessen des Aufenthaltsgesetzes.[252] Die Verfolgung dieser Straftaten unter Verwendung nachrichtendienstlich mittels Eingriffs in Art. 10 GG bzw. in das IT-Grundrecht erhobener Daten dient ganz offensichtlich keinen herausragenden öffentlichen Interessen.

Gleiches gilt auch für die Übermittlungsbefugnis bei einer Straftat nach § 130 StGB. Zwar handelt es sich hierbei um kein Delikt der einfachen Kriminalität. Auch in den verschiedenen Ausprägungen in den Absätzen 1 bis 4 ist der Straftatbestand jedoch allenfalls dem mittleren Kriminalitätsbereich zuzuschreiben und von seiner Schwere auch mit Blick auf das geschützte Rechtsgut keineswegs geeignet, ein herausragendes Interesse an der Strafverfolgung zu begründen.

Ebenso offensichtlich ist die Unverhältnismäßigkeit bei der vorgesehenen Übermittlungsbefugnis bei den meisten Tatbeständen der Geldäsche nach § 261 StGB. Dies gilt einmal mehr seit der Novellierung des Geldwäschetatbestandes und der erheblichen Ausweitung der Strafbarkeit zum 18. März 2021.[253] Schon das geschützte Rechtsgut dieses Straftatbestandes ist sehr vage und umstritten. Einerlei, wie man dieses bestimmt, wird mit der Verfolgung einer Geldwäsche kein herausragendes öffentliches Interesse verfolgt. Ganz offensichtlich unverhältnismäßig ist eine Übermittlung im Falle einer leichtfertigen Geldwäsche nach Absatz 6.

Soweit §§ 17 Abs. 4 und 5 sowie 18 Abs. 1-6 AWG als Katalogtaten einbezogen werden, ist auch dies unverhältnismäßig.[254] Dem Verdikt der Unverhältnismäßigkeit dürften daneben die Katalogstraftatbestände in den §§ 109a, 109f, 109g, 87, 89, 99 Abs. 1 StGB unterfallen.

Auch die pauschale Ermöglichung der Übermittlung zur präventiv-polizeilichen Zwecken nach § 4 Abs. 1 Nr. 1 G 10 verstößt gemessen an den Maßstäben des angerufenen Gerichts gegen den Grundsatz der Verhältnismäßigkeit. Der

---

251 S. dazu hier und im Folgenden *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 442 f.

252 BVerfG, Urteil v. 30.3.2004 – 2 BvR 1520/01, Rn. 97.

253 BGBl. 2021 I, S. 327, s. dazu etwa *Böhme/Busch*, wistra 2021, 169 ff.; *Gazeas*, NJW 2021, 1041 ff.; *Gercke/Jahn/Paul*, StV 2021, 330;

254 S. auch dazu *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 443.

Straftatenkatalog ist hier in noch weiterem Umfang mit den verfassungsrechtlichen Anforderungen nicht in Einklang zu bringen.

Der Gesetzgeber hat verkannt, welche Eingriffsintensität mit einer Übermittlung von Daten aus heimlichen Überwachungsmaßnahmen an Polizei und Strafverfolgungsbehörden einhergeht.[255] Der damit verbundene Grundrechtseingriff ist wegen der für den Betroffenen drohenden Konsequenzen in der Regel ein weitaus schwerwiegenderer als der ursprüngliche Grundrechtseingriff im Rahmen der Erhebung dieser Daten durch den Nachrichtendienst. Denn anders als bei der Erhebung drohen bei einer Übermittlung unmittelbar Zwangsmaßnahmen für den Betroffenen.

5. Verfassungsrechtliche Mängel in § 15a G 10 (Eilanordnung)

Die vorgesehene Regelung zum Erlass von Eilanordnungen in § 15a G 10 dispensiert in mehrfacher Hinsicht in Fällen von Gefahr im Verzug von der Einhaltung des üblichen Verfahrens und der Zuständigkeiten für die Anordnung von Maßnahmen nach § 3 G 10. Die in § 15a Abs. 1 bis 4 G 10 getroffenen Ausnahmeregeln verletzten hierbei verfassungsrechtlich notwendige Schutzvorkehrungen und verstoßen daher jedenfalls gegen das IT-Grundrecht in seiner Ausgestaltung als Grundrechtschutz durch Verfahren. § 15a G 10 sieht keinerlei Dokumentationspflichten für Anordnungen in Eilfällen vor, insbesondere im Hinblick auf die Annahme von Gefahr im Verzug. Sie sieht im Falle des § 15a Abs. 4 G 10 auch keine verfassungsrechtlich hinreichende kompensatorische Regelung dafür vor, wer im Eilfall statt der G 10-Kommission oder des zuständigen Bundesministeriums die Anordnung im Eilfall treffen kann. Von Verfassungs wegen ist als Mindestmaß zu verlangen, dass ein Bediensteter, der die Befähigung zum Richteramt hat, die Frage des Vorliegens von Gefahr im Verzug prüft und die Eilanordnung bei Vorliegen der Voraussetzungen hierfür erlässt. Es fehlt zudem an einer Regelung eines Beweisverwertungsverbotes von Erkenntnissen für den Fall, dass eine Anordnung nicht bestätigt wird. § 15a Abs. 2 G 10 sieht lediglich eine Löschungspflicht vor. Erforderlich ist eine strukturell vergleichbare Regelung wie in § 3a Satz 8 G 10, die ein Verwertungsverbot enthält.

VI. Verletzung von Art. 12 Abs. 1 GG

Die Ermächtigungsgrundlagen in § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 sowie § 3 Abs. 1 i.V.m. 11 Abs. 1a Satz 1 G 10 sowie § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 verletzen die Beschwerdeführer zu 2), 4), 6), 9),

---

255 Ausführlich dazu *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 244 ff.

13), 26), 27), 29), 34), 41), 42), 47), 48), 58), 59) und 64), die als Rechtsanwälte tätig sind, auch in ihrem Grundrecht auf Berufsfreiheit gem. Art. 12 Abs. 1 GG.

Dies folgt daraus, dass die Gefahr einer Überwachung der Kommunikation mit ihren Mandanten die Kommunikationsmöglichkeiten der Beschwerdeführer zu 2), 4), 6), 9), 13), 26), 27), 29), 34), 41), 42), 47), 48), 58), 59) und 64) erheblich einschränkt, weil sie zu einer nachvollziehbaren Hemmung führt, Telekommunikationsmittel in Anspruch zu nehmen, die bis zu einem Abstandnehmen reichen kann. Damit wird zugleich die Effektivität der Arbeit der genannten Beschwerdeführer als Rechtsanwälte beeinträchtigt.

Die Gefahr einer Überwachung der Kommunikation mit ihren Mandanten ist auch trotz § 3b G 10 tatsächlich gegeben. Zwar ist in § 3b Abs. 1 Satz 1 G 10 geregelt, dass die entsprechenden Maßnahmen u.a. dann unzulässig sind, wenn sie sich gegen Rechtsanwälte richten und voraussichtlich Erkenntnisse erbringen würden, über die diese das Zeugnis verweigern dürften (vgl. § 53 Abs. 1 Satz 1 Nr. 2, Nr. 3 StPO). Auch wird dieses Erhebungsverbot in § 3b Abs. 1 Satz 2 G 10 mit einem Verwertungsverbot flankiert. Allerdings gilt diese Vorschrift, wie sich aus einem Umkehrschluss aus § 3b Abs. 4 G 10 ergibt, nur für den Fall, dass es sich bei dem Berufsgeheimnisträger um einen Nachrichtenmittler handelt, dem seine konkrete Unterstützungsfunktion nicht bewusst ist.[256] Nicht erfasst ist also insbesondere der Fall, dass der Berufsgeheimnisträger lediglich als Kommunikationspartner der Zielperson betroffen ist.[257] Zudem gilt § 3b Abs. 1 bis Abs. 3 G 10 gem. § 3b Abs. 4 G 10 auch dann nicht, wenn die zeugnisverweigerungsberechtigte Person Verdächtiger im Sinne des § 3 Abs. 2 Satz 2 G 10 ist oder tatsächliche Anhaltspunkte den Verdacht begründen, dass sie dessen in § 3 Abs. 1 G 10 bezeichnete Bestrebungen durch Entgegennahme oder Weitergabe von Mitteilungen bewusst unterstützt. Somit ist auch die Kommunikation mit Rechtsanwälten potenziell von den oben genannten Maßnahmen betroffen (vgl. dazu auch § 3b Abs. 4 G 10).

Da angesichts der obigen Ausführungen auch dieser Eingriff nicht gerechtfertigt ist, sind die Beschwerdeführer 2), 4), 6), 9), 13), 26), 27), 29), 34), 41), 42), 47), 48), 58), 59) und 64) in ihrem Grundrecht auf Berufsfreiheit aus Art. 12 Abs. 1 verletzt.

---

256 Siehe dazu nur *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, S. 1203 Rn. 59.

257 Vgl. etwa *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, S. 1203 Rn. 59; zu dem (nachträglichen) Verwendungsverbot siehe aber § 3b Abs. 1 Satz 5 G 10; siehe zudem *Roggan*, in: NOMOS-G 10, 2018, § 3b G 10 Rn. 8 für eine aus dem Verhältnismäßigkeitsgrundsatz folgende Pflicht, die Echtzeituntersuchung unter bestimmten Voraussetzungen zu unterbrechen.

VII. Verletzung von Art. 38 Abs. 1 Satz 2 i.V.m. Art. 47 GG

Die Ermächtigungsgrundlagen nach § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 sowie § 3 Abs. 1 i.V.m. 11 Abs. 1a Satz 1 G 10 sowie § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 verletzen alle Beschwerdeführer, weil sie Abgeordnete des Deutschen Bundestages sind, zusätzlich in ihrem Recht auf eine freie Mandatsausübung aus Art. 38 Abs. 1 Satz 2 i.V.m. Art. 47 GG.[258]

Das Recht zur freien Mandatsausübung aus Art. 38 Abs. 1 Satz 2 GG umfasst auch eine „die freie, von staatlicher Beeinflussung unberührte Kommunikationsbeziehung des Abgeordneten mit den Wählerinnen und Wählern".[259] Bereits die Sammlung öffentlich verfügbarer Informationen begründet einen Eingriff in das freie Mandat.[260] Dies muss erst recht gelten, wenn Inhalte der Kommunikation zwischen einem Abgeordneten und Wählerinnen und Wählern oder anderen Kommunikationspartnern heimlich erhoben werden. Verstärkt wird diese Vertrauensbeziehung durch Art. 47 GG, der dem Abgeordneten für Informationen ein Zeugnisverweigerungsrecht zubilligt, die ihm als Abgeordneter anvertraut worden sind, und überlassene Schriftstücke insoweit einem Beschlagnahmeverbot unterwirft.[261] Diese Vertraulichkeit zwischen einem Abgeordneten und einer Person, die sich ihm anvertraut, wird durch eine tatsächliche oder auch nur vermutete heimliche Überwachung dieser Kommunikation erheblich beeinträchtigt. Auch insoweit gilt, dass Bürgerinnen und Bürger sich abgeschreckt fühlen könnten, einen Abgeordneten zu kontaktieren, wenn sie befürchten müssen, dass die entsprechende Kommunikation überwacht wird.

Für den Umstand, dass die Kommunikation zwischen Abgeordneten einerseits und Wählerinnen und Wählern andererseits trotz § 3b G 10 von den oben genannten Maßnahmen betroffen ist, kann auf die obigen Ausführungen zu Berufsgeheimnisträgern und Art. 12 Abs. 1 GG verwiesen werden.

VIII. Verstoß gegen Art. 19 Abs. 4 GG

Die Beschwerdeführer werden überdies durch § 13 i.V.m. § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 in ihrem Grundrecht auf Gewährleistung effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG verletzt.

---

258 S. zur Möglichkeit, diese Rechtsverletzung mit der Verfassungsbeschwerde zu rügen die Ausführungen oben in der Zulässigkeit hierzu.

259 BVerfGE 134, 141, 178.

260 BVerfGE 134, 141, 178.

261 BVerfGE 108, 251, 286 f.

Zu den Adressaten der Rechtsweggarantie gem. Art. 19 Abs. 4 GG gehört auch – und gerade – der Gesetzgeber.[262]

Nach § 13 G 10 ist der Rechtsschutz u.a. gegen die Anordnung von Beschränkungsmaßnahmen nach § 3 G 10 sowie deren Vollzug vor der Mitteilung an den Betroffenen pauschal und *per se* ausgeschlossen. Für Eingriffe in Art. 10 Abs. 1 GG hat dies seine verfassungsrechtliche Basis in Art. 10 Abs. 2 Satz 2 GG, der auch ausweislich Art. 19 Abs. 4 Satz 3 GG, der hierauf *expressis verbis* verweist, unberührt bleibt. Die nun mit § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 eingeführte beschränkte Online-Durchsuchung stellt indes – wie bereits dargelegt – keinen Eingriff in Art. 10 Abs. 1 GG, sondern einen solchen in das IT-Grundrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Für Eingriffe in dieses Grundrecht fehlt es an einer ausdrücklichen verfassungsrechtlichen Grundlage für eine Ausnahme von der Rechtsweggarantie aus Art. 19 Abs. 4 GG.[263] Daher wäre eine Einschränkung nach allgemeinen Grundsätzen nur dann möglich, wenn sie unmittelbar dem Schutz von Grundrechten Dritter oder anderer Verfassungsrechtsgüter dienen würde.[264] Dies ist indes nicht der Fall.

Wollte man als entgegenstehendes Verfassungsrechtsgut den Schutz der freiheitlichen demokratischen Grundordnung oder den Bestand oder die Sicherung des Bundes oder eines Landes anführen, so wäre damit die – fehlerhafte – Annahme verbunden, dass Art. 10 Abs. 2 Satz 2 GG obsolet wäre bzw. einen rein deklaratorischen Charakter hätte.

Mithin ist die in § 13 G 10 vorgesehene Ausnahme von der Gewährleistung effektiven Rechtsschutzes jedenfalls insoweit verfassungswidrig und verletzt die Beschwerdeführer in ihrem aus Art. 19 Abs. 4 GG folgenden Grundrecht, als hiermit der Rechtsweg bei einer Maßnahme nach § 3 Abs. 1 i.V.m. § 11 Abs. 1a Satz 2 G 10 vor der Mitteilung an den Betroffenen ausgeschlossen wird.

IX. Anregung zum Erlass einer einstweiligen Anordnung in Bezug auf § 11 Abs. 1a Satz 2 G 10-Gesetz

Die Beschwerdeführerinnen und Beschwerdeführer regen gegenüber dem angerufenen Gericht an, zu erwägen, von Amts wegen eine einstweilige Anordnung

> begrenzt auf die Regelung zur Durchführung einer beschränkten Online-Durchsuchung (§ 11 Abs. 1a S. 2 G 10) gemäß § 32 Abs. 1 BVerfGG

---

262 Siehe nur *Enders*, in: BeckOK-GG, 47. Edition 2021, Art. 19 Rn. 72.

263 So auch *Poscher*, Stellungnahme zu dem Entwurf der Bundesregierung eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Mai 2021, S. 9.

264 Siehe nur *Schulze-Fielitz*, in: Dreier, GG, 3. Aufl. 2013, Art. 19 Abs. 4 Rn. 140.

zu erlassen.

Den Beschwerdeführern ist bewusst, dass gerade im Falle eines Parlamentsgesetzes – zurecht – vom Gericht ein noch strengerer Maßstab angewandt wird, als er bereits generell für den Erlass einer einstweiligen Anordnung gilt.[265] Ihnen ist auch bewusst, dass die Erfolgsaussichten des Hauptsacheverfahrens für die Entscheidung über den Erlass einer einstweiligen Anordnung grundsätzlich außer Betracht bleiben, sondern allein eine Folgeabwägung stattfindet.[266] Das angerufene Gericht hat jedoch – wenn auch in seltenen Fällen – angedeutet, nicht nur dann auf eine Folgenabwägung zu verzichten, wenn eine Beschwerde oder ein Antrag offensichtlich unzulässig oder unbegründet ist, sondern auch wenn ein Antrag offensichtlich begründet ist[267] oder aus der offensichtlichen Verfassungswidrigkeit einer besondere Dringlichkeit gefolgert.[268] Ferner berücksichtigte das angerufene Gericht mehrfach die offensichtliche Begründetheit, wenn im Hauptsacheverfahren Rechtsverletzungen nicht mehr rückgängig gemacht werden können.[269]

Aus Sicht der Beschwerdeführer liegt eine solche Konstellation hier vor: Das angerufene Gericht hat in zwei Entscheidungen deutlich entschieden, dass die Quellen-TKÜ eine eng begrenzte Ausnahme bleiben muss, die sich nur auf die Überwachung „laufender Kommunikation“ beziehen darf. Anderenfalls liegt eine Online-Durchsuchung und ein Eingriff in das IT-Grundrecht vor – mit entsprechend höheren Anforderungen.[270] Daher muss die Begrenzung auf laufende Kommunikation sogar technisch abgesichert sein.[271] § 11 Abs. 1a Satz 2 G 10 ignoriert – wie schon § 100a Abs. 1 Satz 3 StPO – diese Grenzziehung und erlaubt auch den Zugriff auf abgeschlossene

---

265 BVerfGE 104, 23, 27; 104, 51, 55; 112, 284, 292; 122, 342, 361; 131, 47, 61; 140, 99, 106 f.; 140, 211, 219.

266 Statt vieler BVerfGE 111, 147, 152 f.

267 Vgl. BVerfGE 104, 24, 28 f.: „Ist der Antrag in der Hauptsache weder unzulässig noch offensichtlich *begründet* oder unbegründet, so wägt das Bundesverfassungsgericht die Nachteile, die einträten, wenn die einstweilige Anordnung nicht erginge, die Maßnahme aber später für verfassungswidrig erklärt würde, gegen diejenigen Nachteile ab, die entstünden, wenn die Maßnahme nicht in Kraft träte, sie sich aber im Hauptsacheverfahren als verfassungsgemäß erwiese (vgl. BVerfGE 88, 173 [179f.]; stRspr).“

268 BVerfGE 7, 175, 179 f.: „Damit ist nicht gesagt, daß die Gründe, die für oder gegen die Verfassungsmäßigkeit einer Gesetzesbestimmung sprechen, in dem Verfahren über den Erlaß einer einstweiligen Anordnung in keinem Fall auch nur erwogen werden dürften. Diese Gründe können dann von Bedeutung sein, wenn entweder eine einstweilige Anordnung wegen Unzulässigkeit oder offensichtlicher Unbegründetheit der Verfassungsbeschwerde nicht in Betracht kommt, oder *wenn bei offensichtlicher Verfassungswidrigkeit der Norm die Dringlichkeit, ihren Vollzug einstweilen auszusetzen, besonders deutlich wird*. Da hier keiner dieser Ausnahmefälle vorliegt, muß die Frage der Verfassungsmäßigkeit der Norm, der Regel entsprechend, im Verfahren über die einstweilige Anordnung ausscheiden.“; siehe auch BVerfGE 20, 363, 364.

269 BVerfGE 111, 147, 153; BVerfGK 8, 195, 198; 10, 1, 2; BVerfG, Beschluss vom 31. Juli 2014 – 1 BvR 1858/14, Rn. 10.

270 BVerfGE 141, 220, 309, 120, 274, 309.

271 Ausführlich dazu BVerfGE 141, 220, 310 f.

Telekommunikationsvorgänge. Diesen Punkt haben in Bezug auf § 100a Abs. 1 Satz 3 StPO eine Reihe der Beschwerdeführer bereits mit Verfassungsbeschwerde vom 17. August 2018 gerügt, die beim Zweiten Senat anhängig ist (Az. 2 BvR 1797/18).

Betrachtet man die Folgen, die bis zu einer Entscheidung in der Hauptsache eintreten können, sind dort vor allem die Grundrechtsverletzungen durch Eingriffe in das IT-Grundrecht zu berücksichtigen – nicht nur der Beschwerdeführer, sondern aller potenziell Betroffenen.[272] Das angerufene Gericht hat dabei schon früher in einer Informationserhebung, die auf einer verfassungswidrigen Grundlage beruht einen schwerwiegenden und nicht wieder rückgängig zu machenden Grundrechtseingriff gesehen.[273] Vorliegend ist dieser Grundrechtseingriff aufgrund des Gewichts des IT-Grundrechts und der potenziellen Reichweite des § 11 Abs. 1a Satz 2 G 10 besonders schwerwiegend. Erschwerend zu berücksichtigen ist hierbei auch, die Pflicht von Telekommunikationsunternehmen, Datenströme aus- und wiedereinzuleiten (§ 2 Abs. 1a Nr. 4 G 10). Dadurch wird es möglich, bei jeder Verbindung mit dem Internet potenziell ein Datenpaket „anzukoppeln", das einen „Staatstrojaner" auf das entsprechende IT-System lädt. Hierdurch wird das Vertrauen in die Integrität des Kommunikationsprozesses erheblich erschüttert; dies ist wiederum von großer Bedeutung, weil die Nutzung von Telekommunikationsangeboten in der modernen Welt alltäglich, unvermeidbar und auch für Freiheitsenthaltung unverzichtbar ist.

Zwar wird vielfach darauf verweisen, dass die Instrumente der Quellen-TKÜ und Online-Durchsuchung nur sehr selten angewendet werden. Dies könnte auch dafür sprechen, dass die Bedeutung nicht so groß ist, wie dies vielfach vorgebracht wird oder Alternativen zur Verfügung stehen. Zu berücksichtigen ist ebenfalls, dass nach Auskünften des BKA der Behörden durchaus Alternativen zur Verfügung stehen, um – ohne Online-Durchsuchung – etwa den verbreiteten Messengerdienst *WhatsApp* trotz Ende-zu-Ende-Verschlüsselung mitzulesen.[274] Schließlich ist nicht absehbar, wie sich die Anwendung der Instrumente zukünftig entwickelt. Anders als der Einsatz durch Polizei- und Strafverfolgungsbehörden wird über die Anwendung von Quellen-TKÜ und Online-Durchsuchung nach § 11 Abs. 1a Satz 2 G 10 keine Statistik veröffentlicht, sondern dem Parlamentarischen Kontrollgremium berichtet (§ 14 Abs. 1 S. 2 G 10). Parlamentarische Anfragen hierzu würden voraussichtlich mit Verweis auf das Staatswohl nicht beantwortet werden.

---

272 BVerfGE 122, 342, 362.

273 BVerfGE 121, 1, 22 zum Abruf von Telekommunikationsverbindungsdaten.

274 *A. Meister*, „Polizei und Geheimdienste können WhatsApp mitlesen", netzpolitik.org, 10. Mai 2021, abrufbar unter https://netzpolitik.org/2021/ohne-staatstrojaner-polizei-und-geheimdienste-koennen-whatsapp-mitlesen/, zuletzt abgerufen am 12. Juli 2021.

Eine einstweilige Anordnung müsste nicht zwangsläufig die Nichtanwendung des § 11 Abs. 1a Satz 2 G 10 zum Inhalt haben. Denkbar wäre auch eine Anwendung mit der einschränkenden Maßgabe,[275] dass die Anforderungen vorliegen müssen, die das Gericht an eine Online-Durchsuchung gestellt hat.[276] Damit wäre zumindest der Einsatz zur Abwehr konkreter terroristischer und staatsgefährdender Gefahren für überragend wichtige Rechtsgüter weiterhin möglich, auch wenn die Gefahrenabwehr aus Sicht der Beschwerdeführerinnen und Beschwerdeführer keine Aufgabe der Nachrichtendienste ist.

(Dr. Nikolaos Gazeas)
Rechtsanwalt

275 Vgl. zu einem ähnlichen Vorgehen BVerfGE 121, 1, 23 ff.
276 Vgl. dazu BVerfGE 120, 274, 328 f.; 141, 220, 304 f.