**Deutscher Bundestag**
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 E

Rheinische Friedrich-Wilhelms-Universität Bonn
Rechts- und Staatswissenschaftliche Fakultät

An den Ausschuss für Inneres und Heimat
des Deutschen Bundestags
z. Hd. der Vorsitzenden

**Prof. Dr. Klaus F. Gärditz**
Institut für Öffentliches Recht
Postanschrift:
Adenauerallee 24-42
53113 Bonn
Tel.: 0228/73-9176
Email: gaerditz@jura.uni-bonn.de

Bonn, den 28. Februar 2021

***Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme***

Der Regierungsentwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (BT-Drs. 19/26106) zielt auf eine Fortentwicklung des 2015 geschaffenen IT-Sicherheitsgesetzes.[1] Das Gesetz trägt insgesamt den gewachsenen Gefährdungen digitaler Infrastrukturen Rechnung und versucht, die digitale Infrastrukturgewährleistungsverantwortung des Bundes und das BSI als insoweit operativ zuständige Behörde zu stärken. Die neuen §§ 4a, 4b, 7a-7d, 9a BSIG-E zentralisieren im Einklang mit Art. 87 Abs. 3 Satz 1 GG Zuständigkeiten und Verantwortung beim BSI, dessen Charakter als technik- und infrastrukturbezogene Sicherheitsbehörde insoweit ausgeschärft wird. Dies ist grundsätzlich zu begrüßen, zumal die hier thematischen Gefährdungen in besonderem Maße komplexes Fachwissen erfordern, das sinnvollerweise zentral generiert, gebündelt und operationalisiert werden muss. Die hierbei eingeschlossene Regelung des § 5c BSIG-E über die Bestandsdatenauskunft genügt namentlich den jüngsten[2] Anforderungen des BVerfG.[3]

Da ich mich nur als wissenschaftlicher Sachverständiger für Verfassungs- und Sicherheitsrecht, nicht aber für Technik- und Informationsrecht aus eigener Fachkompetenz äußern kann, möchte ich meine Stellungnahme auf eine Regelung konzentrieren, die im Zusammenhang mit dem 5G-Ausbau steht und politisch besonders sensibel ist: die Untersagung des Einsatzes kritischer Komponenten nach § 9b BSIG-E. Diese Regelung reagiert auf die kontroversen Diskussionen auch in anderen Ländern, inwiefern es mit der „digitalen Souveränität“ und dem Bedarf an Sicherheit sowie Vertraulichkeit der auszubauenden TK-

[1] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 17.7.2015 (BGBl. I 2015 S. 1324).

[2] BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13, CR 2020, 607 (Bestandsdatenauskunft II).

[3] Vgl. auch BVerfGE 154, 152 Rn. 148 ff.; BT-Drs. 19/26106, S. 64.

Netze vereinbar ist, „Kritische Komponenten“ (§ 2 Abs. 13 BSIG-E) von Anbietern einzusetzen, die unter dem Einfluss fremder Staaten stehen, die Sicherheitslücken ausnutzen bzw. technische Infrastruktur-Mitbeherrschung (etwa zu Spionage oder Sicherheitsgefährdung) missbrauchen könnten. Dies ist zwar nach dem Regelungsziel sachgerecht und für einen demokratischen Rechtsstaat zwingend notwendig. Das gilt namentlich für den Ausschluss von Komponenten, die über technische Eigenschaften verfügen, „die geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können“ (§ 9b Abs. 2 Satz 4 BSIG-E). Jedoch erweist sich der konkrete Regelungsinhalt sowohl als verfassungsrechtlich angreifbar als auch als dysfunktional. Die Regelung des § 9b BSIG-E ist kein Beitrag, sicherheitsrechtliche Befugnisse des Bundes zu stärken; die verfassungswidrig unbestimmte Regelung ist vielmehr darauf ausgerichtet, die Wahrung der inneren und äußeren Sicherheit in Bezug auf den TK-Netzausbau weitgehend dem politischen Ermessen der Regierung zu überlassen, insoweit aber eine Intervention bei der Verwendung bedenklicher Komponenten weitestgehend zu erschweren.

Hierzu darf ich im Einzelnen wie folgt Stellung nehmen:

## I. Vorbehalt des Gesetzes

Verfassungsrechtliche Zweifel an der Regelung des § 9b BSIG-E ergeben sich vor allem im Hinblick auf den demokratischen und grundrechtlichen Vorbehalt des Gesetzes.

Der Vorbehalt des Gesetzes beruht auf der Prämisse, dass Gemeinwohl im demokratischen Rechtsstaat fortwährend erst durch politische Entscheidungen in normsetzenden Verfahren hergestellt werden muss.[4] Der rechtsstaatliche Vorbehalt des Gesetzes (verwurzelt in Art. 20 Abs. 3 GG[5]) soll die Berechenbarkeit, Normgeleitetheit und Kontrollierbarkeit der Rechtsanwendung sicherstellen. Er sichert die Berechenbarkeit sowie Kontrollierbarkeit der Rechtsanwendung und wirkt damit der Gefahr von Entscheidungen entgegen, die auf unsachlichen Erwägungen gründen, mithin willkürlich sind.[6] Er dient sowohl der objektiven Rechtssicherheit als auch dem Schutz der Bürgerinnen und Bürger. Der demokratische Vorbehalt des Gesetzes sichert die hinreichende Legitimation und ist im Demokratiegebot (Art. 20 Abs. 2 GG) verankert.

Der Vorbehalt des Gesetzes trifft insoweit nicht nur Aussagen darüber, ob ein bestimmter Regelungsgegenstand *überhaupt* gesetzlich zu regeln ist. Er ist vielmehr auch maßgeblich für die Frage der jeweils gebotenen Regelungsdichte.[7] Die Anforderungen an die Bestimmtheit einer Ermächtigung sind umso höher, je empfindlicher grundrechtlich geschützte Freiheitsentfaltung beschränkt wird.[8] Der Gesetzgeber hat bei der Verwendung unbestimmter Rechtsbegriffe die Grundsätze der Normenklarheit und Justiziabilität zu beachten.[9] Die Reichweite des Vorbehalts des Gesetzes hängt nach der Rechtsprechung zudem von der jeweiligen „Eigenart des zu regelnden Sachverhalts“[10] bzw. von der konkreten und kontextbezogenen Funktion des Gesetzes im

---

[4] *Gärditz*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Stand: 2020, Art. 20 Abs. 3 (Rechtsstaat) Rn. 131.

[5] BVerfGE 40, 237 (248); 49, 89 (126); 48, 210 (221); 107, 59 (102); BVerwGE 109, 29 (37).

[6] Vgl. BVerfGE 33, 125 (158).

[7] BVerfGE 8, 274 (325); 49, 89 (129); 56, 1 (13); 57, 295 (327); 83, 130 (152); 95, 267 (307 f.); 101, 1 (34).

[8] BVerfGE 48, 210 (222); 56, 1 (13); BVerwGE 90, 359 (363); 96, 189 (195).

[9] BVerfGE 8, 274 (325); 13, 153 (160 f.); 21, 73 (79); 34, 165 (192); 63, 312 (324); 78, 214 (226).

[10] BVerfGE 101, 1 (35).

Lichte der Gewaltengliederung[11] ab. Der Gesetzgeber ist verpflichtet, seine Regelungen so bestimmt zu halten, wie dies „nach der Eigenart der zu ordnenden Lebenssachverhalte und mit Rücksicht auf den Normzweck möglich ist“[12]. Dies hängt auch davon ab, „in welchem Umfang der zu regelnde Sachbereich einer genaueren begrifflichen Umschreibung überhaupt zugänglich ist“.[13] Die funktionelle Differenzierung der Staatsgewalt (Art. 20 Abs. 2 Satz 2 GG) zielt zudem auch darauf, dass „staatliche Entscheidungen möglichst richtig, das heißt von Organen getroffen werden, die dafür nach ihrer Organisation, Zusammensetzung, Funktion und Verfahrensweise über die besten Voraussetzungen verfügen“.[14] Hieraus ergeben sich auch Grenzen der Regelbarkeit, die wiederum den Vorbehalt des Gesetzes unter funktionalen Gesichtspunkten begrenzen.

Gemessen hieran ergibt sich für die Regelung des § 9b BSIG-E Folgendes:

## 1. Demokratische Wesentlichkeitsdoktrin

Nach ständiger Rechtsprechung hat der parlamentarische Gesetzgeber in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung alle wesentlichen Entscheidungen selbst zu treffen und darf diese nicht der Verwaltung überlassen.[15] Wesentlich sind vor allem Entscheidungen, die die Grundrechte betreffen (Grundrechtswesentlichkeit)[16]. Entscheidungen über die Grenzen der Freiheit des Bürgers dürfen nicht einseitig in das Ermessen der Verwaltung gelegt werden.

## 2. Folgerung 1: Wesentlich?

Ist die Verwendung von Kritischen Komponenten in TK-Netzen gemessen hieran eine wesentliche Entscheidung?

Auf den ersten Blick mag dies wie Anforderungen an die technische Sicherheit wirken, die gerade im Technikrecht eher durch Rechtsverordnungen, oft sogar nur in Verwaltungsvorschriften geregelt sind. Tatsächlich geht es jedoch vorliegend um die fundamentale Frage, auf welcher freiheitsermöglichenden Infrastruktur die elektronische Kommunikation innerhalb der Bundesrepublik Deutschland künftig stattfinden soll. Die TK-Netze sind unter den heutigen gesellschaftlichen Rahmenbedingungen das Rückgrat des öffentlichen Lebens und der individuellen Freiheit. Von Sicherheitsrisiken innerhalb der Netze betroffen wären insbesondere folgende Kernbereiche des gesellschaftlich-politischen Lebens:

- Alle *Kommunikationsgrundrechte* (insbesondere Art. 5 Abs. 1, Abs. 3, 10 Abs. 1 GG) sind beeinträchtigt, wenn individuelle Kommunikation entweder gestört oder insbesondere über abhängige Technikanbieter einem autoritären Regime zugänglich gemacht wird. Wer potentiell mit Nachteilen rechnen muss, wird sein Kommunikationsverhalten anpassen, was eine erhebliche Beeinträchtigung von Freiheit darstellt.[17] Dies gilt insbesondere dann, wenn ein mächtiger Akteur über seinen technischen Einfluss auf die Kommunikationsnetze eine hinreichend substantielle Wissensherrschaft erlangt, die er etwa gegen politische Opposition oder unliebsame Außenwahrnehmung einsetzen kann. Insoweit greifen

---

[11] BVerfGE 58, 257 (271); 68, 1 (98).

[12] BVerfGE 49, 168 (181); 59, 104 (114).

[13] BVerfGE 56, 1 (13).

[14] BVerfGE 68, 1 (86 f.); 95, 1(15); 98, 218 (252).

[15] BVerfGE 49, 89 (126 f.); 80, 124 (132); 83, 130 (142, 151 f.); 84, 212 (226); 88, 103 (116); 98, 218 (251); 101, 1 (34).

[16] BVerfGE 40, 237 (249); 47, 46 (79); 49, 89 (126 f.); 80, 124 (132); 95, 267 (307 f.); 101, 1 (34); 108, 282 (311); 116, 24 (58); 128, 282 (317); 134, 141 (184); 141, 143 (170 f.); 147, 253 (309 ff.).

[17] Vgl. BVerfGE 100, 313 (359); 120, 274 (323).

grundrechtliche Schutzpflichten für eine hinreichende Kommunikationssicherheit ein,[18] die auch den Gesetzgeber binden (Art. 1 Abs. 3 GG).

- Risiken für die Vertraulichkeit von Interaktionen berühren zudem das *Allgemeine Persönlichkeitsrecht* (Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG).
- Möglichkeiten der Wirtschaftsspionage berühren die *Berufsfreiheit* und das *Eigentum* (Art. 12 Abs. 1, 14 Abs. 1 GG).
- Bei *Kritischen Infrastrukturen* hängen auch vitale Grundrechte (Art. 2 Abs. 2 Satz 1 GG), die sozialstaatliche Sicherheit (Art. 20 Abs. 1 GG) und die Vertrauenswürdigkeit des Staates von funktionierenden und hinreichend manipulationssicheren Kommunikationsinfrastrukturen ab.
- Mindestens ebenso betroffen ist die durch Art. 20 Abs. 2-3 GG gewährleistete und für einen demokratischen Rechtsstaat indisponible *Funktionstüchtigkeit demokratischer und rechtsstaatlicher Institutionen*, die untergraben wird, wenn über Kritische Komponenten des TK-Netzes Angriffe auf die demokratische Willensbildung, die innere und äußere Sicherheit oder die Vertraulichkeit von Staatsgeheimnissen erfolgen.
- Hinzu kommt, dass es überhaupt nicht zu einem tatsächlichen Angriff kommen muss. Schon die *hinreichende Möglichkeit*, technische Komponenten, die in die TK-Netze eingebaut werden, zu Manipulation zu missbrauchen, beeinträchtigt individuelle Freiheit und demokratische Institutionen. So wird bei vertraulichen Inhalten nicht nur das Kommunikationsverhalten dem nicht beherrschbaren Risiko angepasst. Demokratische Willensbildung wird vielmehr auch dadurch ganz allgemein beeinträchtigt, dass jederzeit die plausible Möglichkeit besteht (und öffentlich politisiert werden kann), etwas sei manipuliert worden. Unsicherheiten belasten so die Vertrauenswürdigkeit und Verlässlichkeit sowohl der Volks- als auch der Staatswillensbildung. Die außenpolitische Willensbildung kann im Extremfall sogar zu inadäquater Rücksichtnahme gezwungen sein, wenn (nicht beweisbarer, aber faktisch ausübbarer) Einfluss auf die TK-Netze schlicht erpressbar macht.

Zudem greift auch hier die abwehrgrundrechtliche Wesentlichkeit: § 9b Abs. 1-2 BSIG-E legt Unternehmen Handlungspflichten auf, die ihre Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) beschränken und ggf. dazu führen, auf die technische leistungsstärkste und/oder günstigste Technologie verzichten zu müssen, wenn diese nicht vertrauenswürdig einsetzbar ist. § 9b Abs. 3 BSIG-E enthält zudem eine Verbotsmöglichkeit, die gegenüber den Unternehmen, die die Infrastruktur betreiben, ebenfalls unmittelbar grundrechtsrelevant ist.

*Die grundlegenden Entscheidungen, welche basalen Anforderungen an die technische Sicherheit von TK-Netzen zu stellen sind, sind daher wesentlich im Sinne der bundesverfassungsgerichtlichen Rechtsprechung.* Delegationsfähig wären nur akzessorische Fragen der schlichten technischen Umsetzung, die einer gesetzlichen Regelung praktisch ohnehin kaum zugänglich sind.

## 3. Folgerung 2: Angemessene Regelungsdichte?

Enthält gemessen hieran der Regelungsentwurf des § 9b BSIG-E eine hinreichend dichte Regelung?

Das Bundesministerium des Innern, für Bau und Heimat (im Folgenden: BMI) legt nach § 9b Abs. 2 Satz 5 BSIG-E die Mindestanforderungen für die Garantieerklärung im Einvernehmen mit den betroffenen Ressorts unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung (also Verwaltungsakt nach § 35 Satz 2 VwVfG) fest, die im Bundesanzeiger bekannt zu machen ist. Das Verwendungsverbot

[18] S. nur *Hoffmann-Riem*, AöR 134 (2009), 513 ff.; *ders.*, AöR 137 (2012), 509 ff.; *ders.*, JZ 2014, 53 ff.

bei fehlender oder unvollständiger Garantieerklärung nach Satz 1 gilt erst ab der Bekanntmachung dieser Allgemeinverfügung (§ 9b Abs. 2 Satz 6 BSIG).

Dies genügt aus den folgenden Gründen nicht den dargestellten Anforderungen an den Vorbehalt des Gesetzes:

- Die Regelung sieht ein Outsourcing wesentlicher Festlegungen in eine schlichte Allgemeinverfügung vor (§ 9b Abs. 2 Satz 5 BSIG): Wesentliche Fragen, welche Anforderungen Netzkomponenten grundsätzlich zu genügen haben, dürfen aber nicht *erstmals* in einem Verwaltungsakt festgelegt werden. Das Gesetz müsste zumindest die grundlegenden Parameter fixieren, was durch technische Standards zu gewährleisten ist, welchen Sicherheitszielen die Regelung dienen soll (z. B. „nur" technische Sicherheit oder auch politische Unabhängigkeit/Wehrhaftigkeit). Das Gesetz müsste auch in irgendeiner Form den normativen Grad der Erwartung an die Leistungsfähigkeit umschreiben. Jede Technik ist anfällig für Manipulation, absolute Sicherheit kann es natürlich auch hier nicht geben. Die Frage, welches Maß an Manipulationssicherheit für Kritische Infrastrukturen und Kritisch Komponenten gelten soll, müsste aber normativ auf abstrakt-genereller Ebene zumindest rahmenartig festgelegt werden. Hierzu enthält das gesamte Gesetz keine konkreten Aussagen, die über das vage Ziel des § 9b Abs. 2 Satz 4 BSIG-E hinausgehen. Das Gesetz lässt auch nicht klar erkennen, inwiefern Komponenten ausgeschlossen sein sollen, die zwar für sich den Anforderungen des Satzes 4 genügen, aber im komplexen Zusammenspiel zu Risiken führen.
- Die normativen Parameter, welche Inhalte die maßgebliche Allgemeinverfügung haben soll, bleiben völlig unklar und legen die Prioritätensetzung letztlich vollständig in die Hand der Bundesregierung. Diese gestaltet den Verwaltungsakt „unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange" (§ 9b Abs. 2 Satz 5 BSIG-E). Die Regelung lässt der Regierung völlige Freiheit, die Infrastrukturpolitik zu beliebigen Zwecken einzusetzen. Es fehlt nicht nur eine gesetzliche Gewichtung der ggf. konkurrierenden Interessen. Das Gesetz legt nicht einmal fest, um welche öffentlichen Interessen es konkret gehen darf bzw. soll, was aber Mindestbedingung wäre, damit eine pflichtgemäße Ermessenausübung entsprechend dem Normzweck nach § 40 VwVfG normativ determiniert und kontrollierbar möglich ist. Die konstitutive Einbindung aller Ressorts („Einvernehmen") legt es letztlich nahe, dass *sämtliche* Ressortinteressen berücksichtigungsfähig sind und sich ggf. durchsetzen. Das sind dann völlig disparate und mitunter offen konkurrierende Ziele jenseits der Regelungsstrukturen des vorliegenden Gesetzes; Anhaltspunkte, wie das BMI sein Ermessen auszuüben hat, lassen sich daher der vorliegenden Regelung nicht entnehmen. Dies unterläuft aber elementare rechtsstaatliche wie demokratische Anforderungen an die Programmierung der Verwaltung.
- Insbesondere entscheidet die Regierung nach Belieben, ob und inwieweit sie die öffentlichen Sicherheitsinteressen (und damit zugleich die Freiheit der demokratischen Willensbildung sowie praktische Grundrechtsvoraussetzungen) zu Gunsten (ggf. kurzfristiger) wirtschaftlicher Interessen zurückstellt. Etwa der außenpolitische Wunsch, mit dem Staat, in dem das die fragliche Komponente herstellende Unternehmen angesiedelt ist oder von dem es beherrscht wird, ein Wirtschaftsabkommen zu schließen, eine große Investition eines deutschen Unternehmens zu begünstigen oder einen globalpolitischen Deal einzufädeln, kann willkürlich als Argument missbraucht werden, die innere und äußere Sicherheit zurückzustellen.
- Die gleiche – völlig unbestimmte – Formulierung der Ermessenziele taucht erneut in der Untersagungsermächtigung in § 9b Abs. 3 BSIG-E auf. Ob sie hier das Gleiche bedeutet, ist nicht erkennbar. Die Systematik von Zulassung (Abs. 2) einerseits und Verbot (Abs. 3) andererseits legt es jedenfalls nahe, dass darunter auch ganz unterschiedliche öffentliche

> Interessen gemeint sein können. Die ohnehin verfassungswidrige Unbestimmtheit potenziert sich, weil sich die Regierung bei einem Verbot ggf. von ganz anderen politischen Erwägungen leiten lassen kann als bei der Definition der Sicherheitsstandards.

Die zentrale Aufgabe des Gesetzgebers, politische Wertungskonflikte aufzulösen und in normativ verbindliche sowie demokratisch verantwortbare Regeln zu übersetzen, wird durch die Regelung des § 9b Abs. 2-3 BSIG-E daher im Ergebnis unterlaufen. Folgen davon sind

- ein eklatanter Verlust parlamentarischer Verantwortlichkeit der Regierung, die hier durch konturenloses Blankett ermächtigt wird, ggf. nach tagespolitischer Opportunität außerhalb politischer Verfahren der Rechtsetzung Verwaltungsentscheidungen zu treffen, und
- ein vollständiger Verlust der rechtsstaatlichen Kontrollierbarkeit, weil das Gesetz keinerlei Maßstäbe konkretisiert, nach denen Sicherheit zu gewährleisten ist.

Der Regelungsentwurf ist folglich verfassungswidrig.

## II. Effektiver Rechtsschutz

Die Unbestimmtheit der materiellen Maßstäbe des § 9b BSIG-E wirft zudem die Frage auf, ob hierdurch nicht zugleich betroffenen Unternehmen (seien es die Anbieter oder Wettbewerber) effektiver Rechtsschutz abgeschnitten wird.

Art. 19 Abs. 4 GG garantiert nicht nur, dass überhaupt Rechtsschutz eröffnet ist, sondern dass dieser auch effektiv ist.[19] Das Gebot effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG schließt es zwar nicht aus, „dass durch den Gesetzgeber eröffnete Gestaltungs-, Ermessens- und Beurteilungsspielräume sowie die Tatbestandswirkung von Exekutivakten die Durchführung der Rechtskontrolle durch die Gerichte einschränken."[20] Der Gesetzgeber ist bei der Einräumung von Letztentscheidungsrechten der Exekutive durch die Grundrechte sowie durch das Rechtsstaats- und das Demokratieprinzip und die hieraus folgenden Grundsätze der Bestimmtheit und Normenklarheit gebunden.

> „Will er im Übrigen gegenüber von ihm anerkannten subjektiven Rechten die gerichtliche Kontrolle zurücknehmen, hat er zu berücksichtigen, dass im gewaltenteilenden Staat grundgesetzlicher Prägung die letztverbindliche Normauslegung und auch die Kontrolle der Rechtsanwendung im Einzelfall grundsätzlich den Gerichten vorbehalten ist. Deren durch Art. 19 Abs. 4 Satz 1 GG garantierte Effektivität darf auch der Gesetzgeber nicht durch zu zahlreiche oder weitgreifende Beurteilungsspielräume für ganze Sachbereiche oder gar Rechtsgebiete aushebeln. Die Freistellung der Rechtsanwendung von gerichtlicher Kontrolle bedarf stets eines hinreichend gewichtigen, am Grundsatz eines wirksamen Rechtsschutzes ausgerichteten Sachgrunds."[21]

Hier werden durch die offene Tatbestands- und Rechtsfolgenstruktur des § 9b BSIG-E jedoch faktisch die Mindestbedingungen einer wirksamen gerichtlichen Kontrolle unterlaufen, weil kein transparenter gesetzlicher Maßstab besteht, der eine wirksame Kontrolle der durch Verwaltungsakt festgesetzten Parameter Kritischer Komponenten oder einer Untersagung im Einzelfall ermöglicht. Der Verweis auf politische Interessen ermöglicht nicht nur Willkür, sondern bezweckt diese sogar, weil bewusst kontrollierbare Maßstäbe vorenthalten werden, um es der Regierung zu

---

[19] BVerfGE 40, 272 (275); 55, 349 (369); 60, 253 (269); 113, 273 (310); 116, 1 (18); 129, 1 (20 ff.).

[20] BVerfGE 129, 1 (21 f.).

[21] BVerfGE 129, 1 (22 f.).

ermöglichen, den Grad der Sicherheit nach tagespolitischer Opportunität im Rahmen eines konturenlosen Gestaltungsermessens selbst zu bestimmen.

Mangels hinreichender Maßstäbe, nach denen das BMI die fraglichen Verwaltungsakte erlässt, wird eine wirksame Kontrolle, ob die an Kritische Komponenten angelegten Kriterien rechtmäßig sind, faktisch unterlaufen. Die Regelung verletzt daher auch Art. 19 Abs. 4 GG.

## III. Inkohärenz

Daneben weist die Regelung erhebliche Kohärenzdefizite auf, die dazu führen, dass eine wirksame Anwendung jedenfalls erheblich erschwert wird. Auf folgende Punkte darf hier stellvertretend für zahlreiche Defizite hingewiesen werden:

- *Anwendungsbereich*. § 9b BSIG-E bezieht sich auf Kritische Komponenten, für die eine gesetzliche Zertifizierungspflicht besteht. Auf den ersten Blick erscheint es, als ob die Norm einen weitreichenden Schutz etabliert. Genauer besehen erweist sich die Vorschrift aber in erheblichen Teilen als erst noch auffüllungsbedürftiges Blankett. Hierzu muss die Definition des § 2 Abs. 13 Satz 2 BSIG-E in den Blick genommen werden. Ob etwas Kritische Komponente ist, hängt hiernach von einer vorherigen gesetzlichen Festlegung ab, die das vorliegende Gesetz überhaupt nicht vornimmt. Für TK-Infrastrukturen ergibt sich eine Teilregelung erst – reichlich versteckt – aus § 109 Abs. 6 TKG,[22] was sich im Übrigen nicht aus dem BSIG-E selbst, sondern erst aus seiner Begründung[23] ergibt. Die Zertifizierungspflicht wiederum ergibt sich erst aus dem mit Verweisungen überladenen und unübersichtlichen Regelungsrahmen des Gesetzes (vgl. § 9a BSIG-E).
- *Ressortübergreifendes Einvernehmen und Frist*: Die maßgebliche Allgemeinverfügung nach § 9a Abs. 2 Satz 5 BSIG-E kann das BMI nur im Einvernehmen mit den anderen Ressorts treffen. Auch ein Verbot der Verwendung von Kritischen Komponenten, die nicht hinreichend sicher sind, kann nach § 9b Abs. 3 BSIG-E nur im Einvernehmen mit allen Ressorts erfolgen. Erfolgt das Verbot nicht innerhalb eines Monats, bleibt die Verwendung zulässig. Dies bedeutet, dass selbst bei positiv festgestellten Sicherheitsrisiken das BMI innerhalb eines Montas eine einvernehmliche Entscheidung der Regierung herbeiführen muss, den Einsatz einer bestimmten Komponente zu verbieten. Damit ist die Untersagungsregelung faktisch unbrauchbar gemacht: Zunächst muss eine technisch höchst komplizierte sowie politisch sensible Frage innerhalb eines Monats entscheidungsreif gemacht werden, was schon eine große Herausforderung ist. Wenn das BMI ein Verbot befürwortet, müssen ebenfalls innerhalb der Frist alle Ressorts zur Zustimmung bewegt werden, was – nicht zuletzt in einer Koalitionsregierung – auch offene Ziel- und Wertungskonflikte einschließen kann. Am Ende kann ein einziges Ressort eine Untersagung verhindern, indem es die Zustimmung verweigert, ohne hierfür Sachgründe zu benötigen oder

[22] „Die Bundesnetzagentur erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absätzen 1 und 2. Sie gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht".

[23] BT-Drs. 19/26106, S. 56.

sich – weil die innere Willensbildung der Regierung einer Ausforschung entzogen bleibt[24] – gegenüber dem Bundestag verantworten zu müssen. Eine solche dysfunktionale Regelung hat keine Vorbilder (namentlich kann auch nicht auf das gegenständlich entfernt verwandte Außenwirtschaftsrecht und die §§ 4, 13 AWG, §§ 55 ff. AWV verwiesen werden[25]) und sollte grundlegend überarbeitet werden. Wenn eine ressortübergreifende Einbindung gewollt sein sollte, würde auch ein einfacher Kabinettsbeschluss genügen, der mit Mehrheit ergeht, zumal sich das Kabinett ohnehin im Rahmen des Art. 65 GG ressortübergreifender Entscheidungen annehmen kann.

- Bei *wiederholter Feststellung nicht vorliegender Vertrauenswürdigkeit* nach § 9b Abs. 5 Nr. 1 bis 3 BSIG-E kann das BMI nach § 9b Abs. 7 BSIG-E im Einvernehmen mit den betroffenen Ressorts den Einsatz aller kritischen Komponenten des Herstellers untersagen. Es ist bizarr, dass es erst zu wiederholten (!) Verstößen gegen elementare Sicherheitsanforderungen kommen muss, damit ein Hersteller generell ausgeschlossen werden kann. Jedes Unternehmen kann es also zumindest einmal versuchen, mit einer falschen Erklärung durchzukommen. Die Sicherheitsgewährleistung bleibt hier in einem kritischen Bereich selbst hinter dem allgemeinen Gewerberecht zurück, nachdem ein unzuverlässiges Unternehmen längst seine Zulassung verloren hätte.

- Sollte überhaupt noch Anwendungsraum für die Regelung verbleiben, wird dieser durch das *inadäquate Beweismaß* endgültig beseitigt. Nach § 9b Abs. 5 Nr. 2 BSIG-E ist ein Hersteller erst dann nicht vertrauenswürdig, wenn die Erklärung *unwahre* „Tatsachen“[26] enthält. Nach allgemeinen Regeln liegt daher zugleich die Beweislast beim Bund; dieser muss also ggf. positiv inadäquate Risiken durch fremde Staaten und deren abhängige Akteure beweisen. Dies ist aus mehrerlei Hinsicht aber praktisch kaum möglich. So werden zahlreiche Erkenntnisse über *politische* Missbrauchsrisiken nicht aus der Technologie selbst allein ableitbar sein, sondern sich zumindest auch auf nachrichtendienstliche Aufklärung (namentlich durch den BND, ggf. auch durch das BfV) stützen. Diese Erkenntnisse sind aber strukturell nicht auf förmliche Beweisführung zugeschnitten. Nachrichtendienstliche Aufklärung führt zudem nur zu probabilistischen Wahrscheinlichkeitsurteilen, die eine vertretbare Prognose erlauben, erreicht aber durchweg keinen Wahrscheinlichkeitsgrad, der eine Überzeugung von der Wahrheit über jeden vernünftigen Zweifel erlaubt. Das ist auch weder die Funktion nachrichtendienstlicher Aufklärung noch von Gefahrenabwehr. Letztlich ist das normative Programm hier nicht als sicherheitspolitische Risikoabwägung

---

[24] Hierzu näher BVerfGE 67, 100 (139); 124, 78 (120 ff.); 124, 161 (189); *Geis*, in: Isensee/Kirchhof (Hrsg.), HStR III, 3. Aufl. (2005) § 55 Rn. 51; *Scholz*, AöR 105 (1980), 564 (598); *Schulte* Jura 2003, 505 (509); *Teubner*, Untersuchungs- und Eingriffsrechte privatgerichteter Untersuchungsausschüsse, 2009, S. 379 f.

[25] Schon dem Gegenstand nach unterscheiden sich unter sicherheitspolitischen Auspizien die bloße Investition in ein Unternehmen als Anteilseigner am Kapital einerseits und die Integration begrenzt transparenter ausländischer Technik in deutsche Infrastrukturen andererseits entscheiden. Die nach § 59 AWV iVm § 14a Abs. 1 Nr. 2 AWG greifende Frist zur Intervention beträgt vier Monate. Das ist schon ein gewaltiger Unterschied, wenn es darum geht, insbesondere entscheidungsunwillige Ressorts einzubinden. Die Anforderung einer Untersagung nach § 59 Abs. 1 AWV, „die öffentliche Sicherheit und Ordnung zu gewährleisten“, ist deutlich niedriger als in § 9b BSIG-E. Die AWV orientiert sich hier am Polizeirecht, verlangt also nicht mehr als eine Gefahrenprognose und verweist sogar auf die öffentliche Ordnung, also eine denkbar offene Auffangkategorie. Man vgl. zudem die Schwelle des § 60 Abs. 1b AWV. Schon der Zweck des § 4 Abs. 2 AWG ist wesentlich offener und sicherheitsfreundlicher ausgestaltet. § 13 Abs. 3 Satz 1 AWG sieht für Untersagungen die Zustimmung der Bundesregierung als Kollegialorgan vor. Diese entscheidet aber grundsätzlich im Einklang mit Art. 65 GG durch Mehrheit. Das ist etwas anderes als ein Einvernehmen mit allen Ressorts. Eine Genehmigungsfiktion der Unbedenklichkeitsbescheinigung (zwei Monate!) wird nach § 58 Abs. 2 AWV bereits dadurch verhindert, dass das BMWi ein Prüfverfahren einleitet. Das ist also eine verfahrensrechtliche Vor-Prüffrist, im BSIG-E ist es eine (halb so lange) Entscheidungsfrist.

[26] Das ist schon terminologisch ungenau, weil eine Tatsache nicht unwahr sein kann, sondern allenfalls eine Behauptung von Tatsachen.

konzipiert, die sie eigentlich ermöglichen sollte, sondern wie eine Bestimmung des Gewerberechts, in dem der Staat den gewerbefreien Bürgerinnen und Bürgern deren Unzuverlässigkeit positiv nachweisen muss.

- Die Notwendigkeit eines positiven Nachweises in § 9b Abs. 5 Nr. 2 BSIG-E birgt zudem beträchtliches *außenpolitisches Eskalationspotential*. Diese Norm verhindert es, eine Komponente einfach zurückzuweisen, weil die Verwendungssicherheit im TK-Netz (negativ) nicht hinreichend gewährleistet ist. Vielmehr muss ggf. (positiv) eine sicherheitsgefährdende Einflussnahme fremder Staaten nachgewiesen und belegt werden. Ein gesichtswahrender Rückzug ist dann nicht mehr möglich, die Anwendung der Norm treibt das BMI (und im Kielwasser die Bundesregierung) in eine direkte außenpolitische Konfrontation. Da das nicht ernsthaft intendiert sein wird, liegt ein anderer Schluss näher: Niemand hat die Absicht, auf der Grundlage des § 9b BSIG-E künftig die Nutzung Kritischer Komponenten zu untersagen.
- Soweit nachträglich *Änderungen der Allgemeinverfügung* nach § 9b Abs. 2 Satz 5 BSIG-E erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich (§ 9b Abs. 2 Satz 7 BSIG). Das bedeutet, dass das BMI, selbst wenn es später zu neuen Erkenntnissen über Sicherheitsrisiken gelangt, die mangelnde Verlässlichkeit einer Komponente erst mit Wirkung für künftige Verfahren verwenden kann. Das ist absurd, zumal wenn später hochgradig sicherheitsgefährdende Risiken einer Komponente positiv festgestellt werden, man deren Verwendung dann aber ggf. sehendes Auges weiter dulden muss, weil bereits vorher (unterstellt: nicht vorsätzlich falsche) Garantierklärungen angegeben worden sind.

*Die Summation dieser gravierenden regulativen Defizite wird absehbar dazu führen, dass der Bestimmung des § 9b BSIG-E keine relevante Bedeutung zukommen wird.* Technologiebasierte Sicherheitsrisiken beim Netzausbau lassen sich jedenfalls auf dieser Grundlage nicht angemessen reduzieren. Es liegt der Verdacht nahe, dass genau das auch intendiert ist, die Regierung mit dem Entwurf des § 9b BSIG-E also nur ein Placebo in den Deutschen Bundestag eingebracht hat, um sicherheitspolitische Handlungsbereitschaft zu suggerieren, die tatsächlich gar nicht besteht, was man aber nicht transparent machen möchte.

## IV. Infrastrukturgewährleistung

Insoweit bestehen auch Zweifel, ob diese bewusste Inkaufnahme von substantiellen Sicherheitslücken in den Telekommunikationsnetzen, die das Nervensystem einer modernen Gesellschaft ausmachen, dem Infrastrukturgewährleistungsauftrag aus Art. 87f Abs. 1 GG gerecht wird.

Art. 87f Abs. 2 Satz 1 GG enthält zwar zunächst eine materielle Systementscheidung für eine Leistungserbringung im Wettbewerb.[27] Das Wettbewerbsprinzip wird aber durch den in Art. 87f Abs. 1 GG niedergelegten[28] staatlichen Infrastrukturgewährleistungsauftrag überlagert.[29] „Eine Auslegung des Art. 87f Abs. 2 GG, die ausnahmslos auf die Schaffung von Wettbewerb hinausläuft, wird vom Grundgesetz unter keinem rechtlichen Gesichtspunkt gestützt.“[30] Insoweit ist

---

[27] BVerwGE 114, 160 (168 f.); *Möstl*, in: Maunz/Dürig (Begr.), GG, Art. 87f Rn. 38; *Remmert*, in: Epping/Hillgruber (Hrsg.), GG, 2. Aufl. (2013), Art. 87f Rn. 7; *Windthorst*, in: Sachs (Hrsg.), GG, 8. Aufl. (2018), Art. 87f Rn. 27a.

[28] BVerfGE 130, 52 (71 f.).

[29] BVerfGE 108, 370 (393).

[30] BVerfGE 108, 370 (393).

eine praktische Konkordanz zwischen den konfligierenden Zielen herzustellen.[31] Diese Bestimmung definiert die Grenzen des Privatwirtschaftlichkeitsgebots,[32] ist also spezifischer Rechtfertigungsgrund für Eingriffe in den Wettbewerb. Namentlich die grundsätzliche unternehmerische Leistungsbereitstellung im Wettbewerb (Infrastrukturwettbewerb eingeschlossen) wird also durch hoheitliche Direktiven dort eingeschränkt, wo anderenfalls der Infrastrukturgewährleistungsauftrag nicht erfüllt würde, etwa weil marktexterne politische Ziele der Netzsicherheit sichergestellt werden sollen.

Art. 87f Abs. 1 GG enthält zwar kein Optimierungsgebot, sondern einen bloßen Grundversorgungsauftrag im Sinne eines Untermaßverbots.[33] Dies verdeutlicht bereits die amtliche Begründung der Grundgesetzänderung, durch die Art. 87f GG eingeführt wurde: Der staatliche Handlungsauftrag sei „nicht auf den Ausbau einer optimalen Infrastruktur ausgerichtet, sondern zielt auf die Gewährleistung einer flächendeckenden Grundversorgung durch Sicherung der aus Sicht der Benutzer angemessenen und ausreichenden Dienstleistungen".[34] Eine „Unterversorgung der Bevölkerung mit den entsprechenden Dienstleistungen"[35] ist aber nicht erst dann gegeben, wenn Gebiete vom TK-Netz abgeschnitten oder Netzleistungen (etwa Bandbreite, Kapazität, kontinuierliche Bereitstellung) unzureichend sind. Der Infrastrukturauftrag wird vielmehr auch dann verletzt, wenn die Infrastrukturen gemessen an ihrer Funktion, kommunikative Freiheit zu ermöglichen, nicht hinreichend sicher sind. Insoweit schließt Art. 87f Abs. 1 GG eine objektiv-rechtliche Schutzverantwortung ein, TK-Netze auch gegen Angriffe, Spionage, Überwachung und Missbrauch durch Akteure zu schützen, die von fremden Staaten gesteuert werden. Ein manipulierbares oder exogenem Zugriff zugängliches Netz ist keine adäquate Infrastruktur im Sinne des Art. 87f Abs. 1 GG.

Indem § 9b BSIG-E auf konkrete und bekannte Risiken im Bereich Kritischer Komponenten mit einem faktischen Verzicht auf wirksame Abwehrmaßnahmen reagiert, unterläuft der Bund seinen aus Art. 87f Abs. 1 GG folgenden Auftrag, für sichere und verlässliche Netzstrukturen zu sorgen.

## V. Notifikation

Sollte es im parlamentarischen Verfahren zu einer Änderung des Entwurfs kommen, könnte eine Notifikation gemäß Art. 5 der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1) auch noch nachträglich erfolgen. Eine solche Nach-Notifikation sollte allerdings jedenfalls rein vorsorglich erfolgen. Es bestehen allerdings erhebliche Zweifel, ob eine bloße Änderung des Untersagungsverfahrens nach § 9b BSIG-E tatsächlich der Notifikation bedürfte. Denn diese Regelung betrifft nicht die anzuwenden technischen Spezifikationen oder Vorschriften, die ein auf dem TK-Binnenmarkt tätiger Hersteller einzuhalten hat, sondern lediglich die Rechtsfolgen einer Nichteinhaltung. Diese sind aber nicht unmittelbarer Gegenstand des Regelausschussverfahrens nach Art. 2 f. der Richtlinie.

---

[31] *Gersdorf*, WiVerw 2010, 150 (160); *Mayen*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Art. 87f Rn. 207; *Möstl*, in: Maunz/Dürig (Begr.), GG, Art. 87f Rn. 38-40.

[32] *Mayen*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Stand: 2016, Art. 87f Rn. 206.

[33] *Mayen*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar zum GG, Stand: 2016, Art. 87f Rn. 139 ff.; *Möstl*, in: Maunz/Dürig (Begr.), GG, Art. 87f Rn. 65.

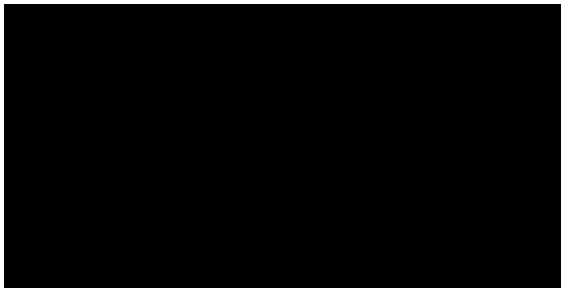
[34] BT-Drs. 12/7269, S. 5.

[35] BVerfGE 130, 52 (72).

## VI. Gesamtwürdigung

Der Deutsche Bundestag büßt an Glaubwürdigkeit ein, wenn einerseits – mit Recht – immer wieder der verfassungsrechtlich hohe Rang der inneren und äußeren Sicherheit betont wird und hiermit verbundene Grundrechtseingriffe gerechtfertigt werden (wie zuletzt im Zuge des BNDG-Novelle in diesem Ausschuss), hier aber das Gesetz mit allen Mittel versucht, sicherheitspolitische Belange abzuwehren bzw. auszuhebeln. Bei der Regelung des § 9b BSIG-E handelt es sich letztlich um ein wirtschaftspolitisches Netz-Sicherheitsverhinderungsinstrument.

Die Regelung des § 9b BSIG-E reduziert die Frage der Nutzung Kritischer Komponenten zudem dysfunktional auf ein reines Technikproblem. Es sollen allenfalls technische Risiken eingedämmt werden. Die einer entsprechenden technologiepolitischen Entscheidung inhärente *politische* Komponente wird aber bewusst ausgeblendet. Dabei betreffen weitreichende Zukunftsentscheidungen, die in diesem Fall nachhaltigen Einfluss auf unsere Kommunikationsstrukturen und damit das freiheitliche Miteinander in unserer Gesellschaft haben werden, immer auch Fragen der Wertorientierung innerhalb der Sicherheits- und Außenpolitik. Insoweit ist es eben nicht gleichgültig, wer eine ökonomisch-technisch leistungsstarke Technologie unter welchen Bedingungen, zu welchen Zwecken und unter welchem politischen System herstellt.[36] Technologien verbinden auch Gesellschaften und insoweit lässt sich die Frage der Techniknutzung eben nicht von den Ideologien dienen, die hinter den Herstellern letztlich stehen und die um globalpolitische Macht ringen. Die rein technikbezogene Regelung des § 9b BSIG-E zielt hingegen gerade darauf ab, jedwede wertorientierte Politisierung zu verhindern und Technologiepolitik auf eine reine Marktfrage zu kondensieren. Das mag für die techniknutzenden Unternehmen adäquat sein. Freiheitliche Wertorientierung in der Technologie- und Außenpolitik, die sich natürlich nicht zwingend durchsetzen muss, aber von vornherein eine gesetzliche Absage zu erteilen, ist aber für die den Entwurf tragende Bundesregierung ein kapitulatives Armutszeugnis.



(Professor Dr. Klaus Gärditz)

[36] Der gegenwärtige Regelungsentwurf ließe es beispielsweise sogar zu, dass Komponenten eingesetzt werden, die der Hersteller durch Kinder- oder Sklavenarbeit oder durch internierte Zwangsarbeiter hergestellt hat.