Ausarbeitung

Verfassungsrechtliche Aspekte des IT-Sicherheitsgesetzes

[redacted]

Verfassungsrechtliche Aspekte des IT-Sicherheitsgesetzes

Verfasser/in: [redacted]
Aktenzeichen: WD 3 - 3000 - 087/15
Abschluss der Arbeit: 17. April 2015
Fachbereich: WD 3: Verfassung und Verwaltung
Telefon: [redacted]

Inhaltsverzeichnis

1. Fragestellung

Am 20. März 2015 wurde der von der Bundesregierung eingebrachte Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)[1] in erster Lesung beraten.[2] Es handelt sich um ein Artikelgesetz, mit dem Änderungen in acht Gesetzen vorgenommen werden, insbesondere im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), im Atomgesetz, im Energiewirtschaftsgesetz, im Telemediengesetz und im Telekommunikationsgesetz.

Wesentliche Elemente des Gesetzes sind die Verpflichtung von Betreibern Kritischer Infrastrukturen zur Einhaltung eines Mindestniveaus an IT-Sicherheitsvorkehrungen nach dem Stand der Technik (Sicherungspflicht) sowie die Verpflichtung dieser Betreiber, IT-Sicherheitsvorfälle den zuständigen Bundesbehörden zu melden (Meldepflicht).

In der öffentlichen Debatte sind – neben rechtspolitischen – auch verfassungsrechtliche Bedenken gegen verschiedene Bestimmungen des Gesetzes artikuliert worden.[3] Gebeten wird nunmehr um eine Untersuchung dieser verfassungsrechtlichen Aspekte.

Die vorgebrachten verfassungsrechtlichen Bedenken beziehen sich im Wesentlichen auf die Fragen,

- ob die Ermächtigung des Bundesministeriums des Innern zur näheren Bestimmung des Begriffs der Kritischen Infrastrukturen durch Rechtsverordnung verfassungswidrig ist (dazu unter 2.),

- ob die den Betreibern Kritischer Infrastrukturen auferlegten Verpflichtungen mit deren Berufsfreiheit nach Art. 12 Abs. 1 GG vereinbar sind (dazu unter 3.),

- ob die dem Bundesamt für Sicherheit in der Informationstechnik eingeräumten Befugnisse zur Erhebung, Speicherung und Verwendung von Daten mit dem Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vereinbar sind (dazu unter 4.),

- ob die Tatsache, dass lediglich Unternehmen, nicht aber Behörden Adressaten der Verpflichtungen sind, gegen die Verfassung verstößt (dazu unter 5.).

---

1 BT-Drs. 18/4096.

2 BT-PlPr. 18/95, S. 9037.

3 Vgl. insbesondere die verfassungsrechtlichen Einwände von Ahlhaus/Holzinger, Verfassungsrechtliche Stellungnahme im Auftrag des Cyber-Sicherheitsrat Deutschland e.V. zum Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015, unveröffentlicht.

2. Verstoß gegen das Wesentlichkeitsgebot bzw. Bestimmtheitsgebot?

2.1. Bestimmungen des Entwurfs

Nach Art. 1 des Entwurfs des IT-Sicherheitsgesetzes wird § 2 BSI-Gesetz folgender Absatz 10 angefügt:

> „(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die
>
> 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
>
> 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
>
> Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt."

§ 10 Abs. 1 BSI-Gesetz soll folgende Fassung erhalten:

> „(1) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt."

2.2. Kritik

Die Delegation der Präzisierung des Begriffs der Kritischen Infrastrukturen auf den Verordnungsgeber wird teilweise – als Verstoß gegen das Wesentlichkeitsgebot bzw. Bestimmtheitsgebot – für

verfassungswidrig gehalten.[4] Auch der Bundesrat hat in seiner Stellungnahme um eine stärkere Präzisierung des Begriffs bereits im Gesetz selbst gebeten, ohne allerdings den Vorwurf der Verfassungswidrigkeit zu erheben.[5]

2.3. Verfassungsrechtliche Würdigung

Das aus dem Rechtsstaats- und Demokratieprinzip abgeleitete sogenannte **Wesentlichkeitsgebot** verpflichtet den parlamentarischen Gesetzgeber, in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, alle wesentlichen Entscheidungen selbst zu treffen und nicht der Verwaltung zu überlassen.[6] Die Abgrenzung des vom Gesetzgeber zu regelnden „Wesentlichen" vom nicht zwingend durch das Parlament zu regelnden „Unwesentlichen" stößt auf praktische Schwierigkeiten und lässt sich nicht generell-abstrakt vornehmen.[7] Allgemein lässt sich jedoch sagen: Je schwerwiegender die Auswirkungen einer Regelung und je wesentlicher eine Angelegenheit für die Allgemeinheit bzw. den einzelnen Bürger ist, desto genauer müssen die Vorgaben des parlamentarischen Gesetzgebers sein.[8]

Zudem begrenzt **Art. 80 Abs. 1 GG** die Delegation der Rechtsetzung auf die Exekutive. Danach bedarf der Erlass einer Rechtsverordnung durch die Bundesregierung, ein Bundesministerium oder eine Landesregierung einer gesetzlichen Ermächtigung, deren Inhalt, Zweck und Ausmaß gesetzlich bestimmt ist. Diese Anforderung wird auch als **verordnungsspezifisches Bestimmtheitsgebot** bezeichnet und dient der parlamentarischen Steuerung und Begrenzung der exekutiven Rechtsetzung.[9] Erforderlich ist danach zunächst, dass die gesetzliche Ermächtigungsgrundlage hinreichend klar ist.[10] Daneben betrifft die Bestimmtheit im Sinne des Art. 80 Abs. 1 GG aber auch das Maß der erforderlichen gesetzlichen Vorprägung von Rechtsverordnungen.[11] Damit bestehen enge Berührungspunkte zum Wesentlichkeitsgebot.

---

4 So etwa Ahlhaus/Holzinger, Verfassungsrechtliche Stellungnahme im Auftrag des Cyber-Sicherheitsrat Deutschland e.V. zum Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015, unveröffentlicht, S. 21 ff.; kritisch auch Roos, Der neue Entwurf eines IT-Sicherheitsgesetzes, MMR 2014, 723 (725); Roth, Neuer Referentenentwurf zum IT-Sicherheitsgesetz, ZD 2015, 17 (19), sowie Leisterer/Schneider, Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz, CR 2014, 574 (577).

5 BR-Drs. 643/14, S. 1 f.

6 BVerfGE 49, 89 (126 f.); 77, 170 (231); 83, 130 (142); BVerfG, Beschluss vom 4.5.1997, NJW 1998, 669 (670); vgl. auch Rachor, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Abschnitt E Rn. 723.

7 Zu den Konkretisierungs- und Anwendungsproblemen des Wesentlichkeitsgebots vgl. Ossenbühl, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band 5, 3. Aufl. 2007, § 101 Rn. 56 ff.

8 BVerfGE 33, 125 (158 ff.); 96, 189 (193).

9 Vgl. Uhle, in: Epping/Hillgruber, BeckOK GG, 23. Edition 2014, Art. 80 Rn. 18.

10 Vgl. Remmert, in: Maunz/Dürig, GG, 72. Ergänzungslieferung 2014, Art. 80 Rn. 67.

11 Vgl. Remmert, in: Maunz/Dürig, GG, 72. Ergänzungslieferung 2014, Art. 80 Rn. 68.

Der **unbestimmte Rechtsbegriff** der **Kritischen Infrastruktur** ist der zentrale Begriff des Gesetzentwurfs. Insbesondere ist er Dreh- und Angelpunkt der Novellierung des BSI-Gesetzes (Art. 1 des Gesetzentwurfs). Denn Adressaten insbesondere der IT-Sicherungspflicht und der Meldepflicht nach den neuen Bestimmungen des BSI-Gesetzes sind Betreiber Kritischer Infrastrukturen im Sinne der Rechtsverordnung nach § 10 Abs. 1 BSI-Gesetz-Entwurfsfassung. Auch die in Art. 3 des Entwurfs enthaltene Änderung des Energiewirtschaftsgesetzes knüpft an Betreiber von Energieanlagen an, die durch die Rechtsverordnung nach § 10 Abs. 1 BSI-Gesetz-Entwurfsfassung „als Kritische Infrastruktur bestimmt wurden". Nicht aus dem Gesetz selbst, sondern erst aus der auf dessen Grundlage erlassenen Rechtsverordnung ergibt sich also, wer **Adressat** der gesetzlichen Verpflichtungen ist.[12]

Fraglich ist, ob der parlamentarische Gesetzgeber mit dieser Delegation den Anforderungen des Wesentlichkeits- und Bestimmtheitsgebots ausreichend Rechnung trägt. Festzuhalten ist zunächst, dass es nach diesen Grundsätzen jedenfalls nicht geboten ist, die einzelnen Unternehmen, für die die Anforderungen gelten sollen, bereits im Gesetz konkret zu benennen. Wesensmerkmal eines Gesetzes sind gerade generell-abstrakte Regelungen, die allerdings den genannten Anforderungen des Wesentlichkeits- und Bestimmtheitsgebotsgenügen müssen. Die gesetzliche Definition der Kritischen Infrastrukturen in § 2 Abs. 10 BSI-Gesetz-Entwurfsfassung macht lediglich **zwei Vorgaben**: Zum einen muss es sich um Einrichtungen, Anlagen oder Teile davon aus bestimmten Sektoren handeln (nämlich Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen). Zum anderen müssen diese Einrichtungen, Anlagen oder Teile davon „von hoher Bedeutung für das Funktionieren des Gemeinwesens [sein], weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

Bei dieser Definition handelt es sich um eine vergleichsweise offene Festlegung des Adressatenkreises, zumal die in der Definition verwandten Begriffe „hohe Bedeutung für das Funktionieren des Gemeinwesens" und „erhebliche Versorgungsengpässe" ihrerseits offen und wertungsabhängig sind. Gleichwohl macht § 2 Abs. 10 BSI-Gesetz-Entwurfsfassung Rahmenvorgaben, die die gesetzgeberische Vorstellung des Umfangs Kritischer Infrastrukturen erkennen lassen. Zu berücksichtigen ist dabei auch, dass sich in der **Entwurfsbegründung** zu der Verordnungsermächtigung in § 10 BSI-Gesetz-Entwurfsfassung detaillierte Vorstellungen zu Inhalt und Struktur der zu erlassenden Rechtsverordnung finden. Dort werden nicht nur die Sektoren in **qualitativer Hinsicht** näher spezifiziert. Das betrifft die Frage, ob eine Dienstleistung oder Branche überhaupt als „kritisch" zu bewerten ist. Vielmehr solle die Rechtsverordnung in **quantitativer Hinsicht** auch den Versorgungsgrad der Bevölkerung durch die jeweiligen Einrichtungen berücksichtigen und diesbezügliche Schwellenwerte festsetzen.[13] Die Erläuterungen in der Begründung binden den Verordnungsgeber zwar nicht unmittelbar, entfalten aber gleichwohl mittelbare Wirkung: Denn sie sind, da sie den gesetzgeberischen Willen zum Ausdruck bringen, bei der Auslegung des § 10 BSI-Gesetz-Entwurfsfassung zu berücksichtigen. Welche Maßstäbe und Kriterien für die Bemessung von Schwellenwerten anzulegen sind, folgt wiederum aus dem Gesetz selbst, das eine *hohe* Bedeutung für das Funktionieren des Gemeinwesens und *erhebliche* Versorgungsengpässe fordert. Mit diesen in § 2

12 Zur Bedeutung einer hinreichend präzisen Definition des Adressatenkreises auch BR-Drs. 643/14, S. 1 f.

13 Vertiefend Roth, Neuer Referentenentwurf zum IT-Sicherheitsgesetz, ZD 2015, 17 (19).

Abs. 10 BSI-Gesetz-Entwurfsfassung getroffenen Attributen wird nicht nur der Kreis möglicher Adressaten der Verpflichtungen, sondern auch die Verordnungsermächtigung als solche begrenzt.

Im vorliegenden Kontext der IT-Sicherheit ist ferner zu berücksichtigen, dass es sich um einen nicht nur technisch komplexen, sondern auch ständiger Veränderung unterliegenden Sachbereich handelt. Technische Entwicklungen können hier flexible und rasche Anpassungen der normativen Vorgaben erforderlich machen. Wie das Bundesverfassungsgericht festgestellt hat, ist es dem parlamentarischen Gesetzgeber in Bereichen des technischen Sicherheitsrechts schon aufgrund der **Komplexität der technischen Fragen** in der Regel nicht möglich, sämtliche sicherheitstechnischen Anforderungen bis ins Einzelne festzulegen.[14] Hinzu kommt, dass der parlamentarische Gesetzgeber, hätte er einmal eine detaillierte Regelung getroffen, diese auf Gebieten, bei denen durch die **rasche technische Entwicklung** ständig mit Neuerungen zu rechnen ist, laufend auf den neuesten Stand bringen müsste.[15] Hier ist es dem Gesetzgeber nicht nur erlaubt, unbestimmte Rechtsbegriffe zu verwenden und damit eine laufende Anpassung der Regelung an die wissenschaftliche und technische Entwicklung durch die die administrative und judikative Ebene zu ermöglichen.[16] Er darf gerade in derartigen Fällen, die einerseits technischen Sachverstand und andererseits laufende Anpassungen erfordern, die Konkretisierung der normativen Vorgaben auch der Verordnungsgebung durch die Exekutive überlassen.

Der Entwurf des IT-Sicherheitsgesetzes verfolgt insoweit eine ähnliche Regelungstechnik, wie sie auch dem **Immissionsschutzrecht** zugrunde liegt: Das Bundes-Immissionsschutzgesetz (BImSchG) regelt in den §§ 4 ff. Pflichten der Betreiber genehmigungsbedürftiger Anlagen sowie Einzelheiten des Genehmigungsverfahrens. Was aber genehmigungsbedürftige Anlagen sind, an die der gesamte Abschnitt des Gesetzes anknüpft, wird nicht durch das Gesetz selbst bestimmt, sondern gemäß § 4 Abs. 3 BImSchG der Bestimmung durch Rechtsverordnung überantwortet. § 4 Abs. 1 S. 1 BImSchG setzt hierzu – insoweit dem § 2 Abs. 10 BSI-Gesetz-Entwurfsfassung ähnlich[17] – lediglich einen allgemeinen Rahmen. Die eigentliche Festlegung erfolgt im technisch komplexen Anhang der 4. Durchführungsverordnung (4. BImSchV). Verfassungsrechtlich ist dies zulässig.

Die Delegation der Präzisierung des Begriffs der Kritischen Infrastrukturen auf den Verordnungsgeber durch § 10 BSI-Gesetz-Entwurfsfassung erscheint nach den dargestellten Maßstäben auch hier vereinbar mit dem Wesentlichkeitsgebot und dem Bestimmtheitsgebot.[18] Das gesetzgeberische Ziel wird deutlich, die Ermächtigung ist hinreichend begrenzt, und der Inhalt der zu erlassenden Rechtsverordnung wird – zumal angesichts des genannten Spielraums bei technisch komplexen Rechtsbereichen – ausreichend gesetzlich vorgeprägt.

---

14 BVerfGE 49, 89 (134).

15 BVerfGE 49, 89 (134 f.).

16 BVerfGE 49, 89 (135).

17 Diesen Vergleich stellt auch Roßnagel, Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), S. 4, an.

18 Ebenso Roßnagel, Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), S. 4.

Ob und inwieweit im Verlauf des Gesetzgebungsverfahrens bereits im Gesetz selbst (und nicht nur in der Entwurfsbegründung) weitere Präzisierungen vorgenommen werden sollten, wie es unter anderem der Bundesrat fordert, ist daher eine rechtspolitische Frage. Die Grenze der Verfassungswidrigkeit erscheint hier jedenfalls nicht erreicht.

3. Verletzung der Berufsfreiheit (Art. 12 Abs. 1 GG)?

3.1. Bestimmungen des Entwurfs

Art. 1 des Entwurfs sieht Änderungen des BSI-Gesetzes vor. §§ 8a und 8b BSI-Gesetz-Entwurfsfassung verpflichten die Betreiber Kritischer Infrastrukturen (im Folgenden: Betreiber) zum einen zur Einhaltung eines Mindestniveaus an IT-Sicherheit (**Sicherungspflicht**) und zum anderen zur Meldung erheblicher IT-Sicherheitsvorfälle (**Meldepflicht**) an das BSI.

Im Hinblick auf die **Sicherungspflicht** sieht § 8a Abs. 1 S. 1 BSI-Gesetz-Entwurfsfassung vor, dass die Betreiber angemessene organisatorische und technische Vorkehrungen zur Absicherung der von ihnen betriebenen Kritischen Infrastruktur treffen müssen. Die organisatorischen und technischen Vorkehrungen sind gemäß § 8a Abs. 1 S. 2 BSI-Gesetz-Entwurfsfassung dann angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht. Die Betreiber müssen die Erfüllung der Sicherungspflicht mindestens alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen.

Im Hinblick auf die **Meldepflicht** sieht § 8b Abs. 4 BSI-Gesetz-Entwurfsfassung vor, dass die Betreiber erhebliche Störungen, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastruktur führen können oder bereits geführt haben, über eine von ihnen einzurichtende Kontaktstelle an das BSI zu melden haben.

3.2. Kritik

Die durch §§ 8a und 8b BSI-Gesetz-Entwurfsfassung begründeten Sicherungs- und Meldepflichten werden teilweise als Verletzung von Art. 12 Abs. 1 GG erachtet.[19] Die Auferlegung von Sicherungs- und Meldepflichten stelle eine „Indienstnahme Privater für öffentliche Aufgaben“ dar, durch die den Betreibern unzumutbare Mehrkosten entständen und nicht ausgeglichen würden.

3.3. Verfassungsrechtliche Würdigung

Art. 12 Abs. 1 GG ist ein einheitliches Grundrecht, das – abweichend von seinem Wortlaut – die **Freiheit des Einzelnen, einen Beruf zu wählen und einen Beruf auszuüben**, gleichermaßen schützt. Unter einem Beruf wird jede auf Dauer angelegte Tätigkeit verstanden, die der Schaffung

19 Vgl. Ahlhaus/Holzinger, Verfassungsrechtliche Stellungnahme im Auftrag des Cyber-Sicherheitsrat Deutschland e.V. zum Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015, unveröffentlicht, S. 26 ff.

und Erhaltung einer Lebensgrundlage dient.[20] Das Grundrecht ist jedoch nicht vorbehaltlos gewährleistet. Der Gesetzgeber hat die Befugnis, die Berufsfreiheit durch Gesetz weiter auszugestalten und zu konturieren. Diese Befugnis, die sich aus Art. 12 Abs. 1 S. 2 GG ergibt, erstreckt sich dem Grunde nach auf beide „Phasen" der Berufstätigkeit. Das heißt jedoch nicht, dass die Gestaltungsbefugnisse hinsichtlich jeder dieser „Phasen" inhaltlich gleich weit gehen.[21] Je stärker der Gesetzgeber in die Berufsfreiheit eingreift, umso gewichtiger müssen die Rechtfertigungsgründe sein.[22] Das Bundesverfassungsgericht hat in diesem Zusammenhang die Drei-Stufen-Theorie entwickelt und darin die Eingriffsintensität und die Anforderungen an die verfassungsrechtliche Rechtfertigung schematisch zueinander ins Verhältnis gesetzt: Schafft der Gesetzgeber eine Regelung der Berufsausübung, schafft er also Bedingungen und Modalitäten, unter denen bzw. in denen sich die berufliche Tätigkeit vollzieht, so muss er diese durch vernünftige Erwägungen des Gemeinwohls legitimieren (1. Stufe).[23] Stellt der Gesetzgeber Regeln auf, die die Berufswahl des Einzelnen von persönlichen Eigenschaften oder Fähigkeiten abhängig machen (sog. subjektive Berufswahlregelungen), so muss dadurch der Schutz besonders wichtiger Gemeinschaftsgüter bezweckt werden (2. Stufe).[24] Schließlich sind objektive Berufswahlregelungen, die sich nicht an der persönlichen Qualifikation, sondern an allgemeinen Kriterien orientieren, nur dann zulässig, wenn sie der Abwehr schwerer und nachweisbarer Gefahren für überragend wichtige Gemeinschaftsgüter dienen (3. Stufe).[25] Ein Eingriff des Gesetzgebers muss außerdem im Übrigen verhältnismäßig sein.

Neben natürlichen Personen können nach Art. 19 Abs. 3 GG auch **juristische Personen** den Schutz von Art. 12 Abs. 1 GG genießen. Schutzgut des Art. 12 Abs. 1 GG ist bei juristischen Personen die Freiheit, eine Erwerbszwecken dienende Tätigkeit, insbesondere ein Gewerbe, zu betreiben, soweit diese Erwerbstätigkeit ihrem Wesen und ihrer Art nach in gleicher Weise von einer juristischen wie von einer natürlichen Person ausgeübt werden kann.[26]

Die durch den Entwurf begründeten Sicherungs- und Meldepflichten stellen einen **Eingriff in die Berufsausübungsfreiheit** der Betreiber dar, die nach den vorgenannten Grundsätzen auch den Schutz von Art. 12 Abs. 1 GG als juristische Personen genießen. Der Regelung müssen somit **vernünftige Erwägungen des Gemeinwohls** zugrunde liegen und sie muss sich im Übrigen als **verhältnismäßig** erweisen.

Ausweislich der Begründung des Entwurfs ist „Ziel des Gesetzes […] eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger im Internet und

---

20 BVerfGE 50, 290 (362); 54, 301 (313); 105, 252 (265).

21 BVerfGE 7, 377 (401).

22 BVerfGE 7, 377 (401); vgl. Mann, in: Sachs, Grundgesetz Kommentar, 7. Auflage 2014, Art. 12 Rn. 125.

23 BVerfGE 7, 377 (405 f.); 16, 286 (297); 65, 116 (125).

24 BVerfGE 13, 97 (107); 19, 330 (337); 25, 236 (247).

25 BVerfGE 7, 377 (408); 11, 168 (183); 25, 1 (11).

26 Vgl. BVerfGE 21, 261 (266).

in diesem Zusammenhang auch eine Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamts (BKA).“[27] Auch aus der Definition der „Kritischen Infrastruktur“ in § 2 Abs. 10 BSI-Gesetz-Entwurfsfassung als Einrichtungen oder Anlagen näher umschriebener Sektoren, die „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“, kann man ableiten, dass das Gesetz darauf abzielt, die Grundbedürfnisse der Bevölkerung zu sichern. Dieses Ziel stellt fraglos eine **vernünftige Erwägung des Gemeinwohls** dar, die verfassungsrechtlich nicht zu beanstanden ist.

Die Maßnahme muss sich auch im Übrigen als **verhältnismäßig** darstellen. Das vom Gesetzgeber eingesetzte Mittel muss **geeignet** und **erforderlich** sein, den angestrebten Zweck zu erreichen und sich bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht und der Dringlichkeit der ihn rechtfertigenden Gründe als **angemessen** darstellen.[28]

Gegen die **Geeignetheit** und **Erforderlichkeit** der Regelungen bestehen jedenfalls im Hinblick auf die insoweit bestehende gesetzgeberische Einschätzungsprärogative keine Bedenken.

Im Rahmen der Prüfung der **Angemessenheit** ist die Schwere des Grundrechtseingriffs in Relation zu dem verfassungsrechtlichen Gewicht des verfolgten Zwecks zu setzen. Die Angemessenheit einer staatlichen Maßnahme ist dann gewahrt, wenn der Grundrechtseingriff nicht außer Verhältnis zum verfolgten Zweck steht.

Der durch den Entwurf **verfolgte Zweck**, der Schutz informationstechnischer Systeme, nimmt im Wirtschafts- und Sozialleben des 21. Jahrhunderts eine immer wichtigere Rolle ein. „Die Nutzung informationstechnischer Systeme (IT-Systeme) und des Internets mit seinen vielfältigen Angeboten durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße“, heißt es in der Entwurfsbegründung.[29] Mit dem verfolgten Zweck kommt der Staat auch bestehenden Schutzpflichten im Hinblick auf verschiedene grundrechtlich geschützte Sphären nach, wie insbesondere solchen aus Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG, Art. 10 Abs. 1 GG, Art. 12 Abs. 1 GG und Art. 14 GG.

Dem gegenüber steht der Grundrechtseingriff: Im Hinblick auf die **Sicherungspflicht** werden die Betreiber verpflichtet, lediglich **angemessene** technische und organisatorische **Vorkehrungen** zum Schutze der IT zu treffen. Damit ist bereits auf einfachgesetzlich-tatbestandlicher Ebene der Aufwand, den die Betreiber erbringen müssen, auf solche Vorkehrungen begrenzt, die nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur stehen. Die Vorkehrungen sollen lediglich „branchenspezifische Mindestanforderungen an die IT-Sicherheit“[30] erfüllen. Auch bezüglich der Nachweispflicht der Betreiber formuliert der Entwurf keine überzogenen Anforderungen. Laut Entwurfsbegründung soll die Ausgestaltung der Sicherheitsaudits, Prüfungen und Zertifizierungen nicht im Detail gesetzlich vorgegeben werden,

27 BT-Drs. 18/4096, S. 1.

28 BVerfGE 11, 30 (42 f.); BVerfGE 13, 97 (104 f.).

29 BT-Drs. 18/4096, S. 1.

30 Vgl. BT-Drs. 18/4096, S. 42.

da die Ausgestaltung von den gegebenenfalls erarbeiteten branchenspezifischen Sicherheitsstandards, den in den Branchen vorhandenen technischen Gegebenheiten und bereits bestehenden Auditierungs- und Zertifizierungssystemen abhänge.[31] Anknüpfungspunkt der Nachweispflicht ist also der branchenspezifische technische Status quo.

Im Hinblick auf die **Meldepflicht** ist zu beachten, dass die Betreiber nur **erhebliche Störungen**, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastruktur führen, unverzüglich melden müssen. Die Betreiber müssen also nicht tagtäglich vorkommende Ereignisse wie Spam, übliche Schadsoftware oder Hardwareausfälle im üblichen Rahmen melden, sondern nur solche Störungen, die eine Erheblichkeitsschwelle überschreiten.[32] Eine erhebliche Störung liegt nach der Entwurfsbegründung vor, wenn durch sie die Funktionsfähigkeit der kritischen Dienstleistung bedroht ist.[33] Es wird geschätzt, dass pro Betreiber pro Jahr maximal sieben erhebliche Störungen auftreten.[34] Da relevante IT-Sicherheitsvorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen, fällt nur insofern ein Mehraufwand an, als die relevanten Informationen an das BSI weitergegeben müssen.[35]

Durch die Sicherungs- und Meldepflicht entstehen den Betreibern **Kosten**. Im Rahmen der Fragestellung, inwiefern den Betreibern solche Kosten zugemutet werden können, muss bedacht werden, dass die den Betreibern auferlegten Sicherungs- und Meldepflichten jedenfalls auch der Allgemeinheit zugutekommen und so auch der Erfüllung staatlicher Aufgaben dienen. Denn die Verbesserung der IT-Sicherheit kritischer Unternehmen ist auch in einer marktwirtschaftlich geordneten Wirtschaft eine legitime Aufgabe der staatlichen Wirtschaftspolitik, da durch das Gesetz sichergestellt werden soll, dass gerade die IT-Sicherheit derjenigen Infrastrukturen gewährleistet ist, die für das Funktionieren des Gemeinwesens zentral sind.[36] Eine solche „Indienstnahme Privater für öffentliche Aufgaben“ als solche ist durch die Verfassung nicht ausgeschlossen.[37] Sie begründet an sich, ohne Rücksicht auf ihre Ausgestaltung im Einzelnen, auch keinen Anspruch auf Entschädigung oder Aufwendungsersatz der betroffenen Unternehmen. Die Grenzen der Belastbarkeit der in Anspruch genommenen Unternehmen müssen viel mehr im Wege einer Gesamtabwägung ermittelt werden.[38] Hierbei ist zu berücksichtigen, dass die im Zuge der Sicherungspflichten anfallenden Kosten zunächst auch unmittelbar dem jeweiligen Betreiber selbst zugutekommen, da sie ihn vor Schäden bewahrt. Der im Zuge der Meldepflicht entstehende Aufwand ist zudem gruppennützig,

31 Vgl. BT-Drs. 18/4096, S. 42.

32 Vgl. BT-Drs. 18/4096, S. 47.

33 Vgl. BT-Drs. 18/4096, S. 46.

34 Vgl. BT-Drs. 18/4096, S. 5.

35 Vgl. BT-Drs. 18/4096, S. 5.

36 Zum Aspekt des Funktionieren des Gemeinwesens BT-Drs. 18/4096, S. 2.

37 Vgl. BVerfGE 30, 292 (311); 30, 292 (311).

38 Vgl. BVerfGE 30, 292 (316).

weil mittelbar alle Betreiber von dem gewonnenen Wissen profitieren und Angriffe auf ihre IT-Systeme damit besser abwehren können.[39]

Der **Umfang der Kostenlast**, der durch die Sicherungs- und Meldepflicht bei den Betreibern entsteht, wird unterschiedlich eingeschätzt. In der Entwurfsbegründung heißt es, der Kostenaufwand könne zum jetzigen Zeitpunkt nicht quantifiziert werden. Zum einen sei die Zahl der Betreiber vor Erlass der konkretisierenden Verordnung noch nicht klar, zum anderen müsse differenziert werden, welche Sicherheitsstandards derzeit bestünden und noch erforderlich seien.[40] Aus Kreisen der Wirtschaft werden die geschätzten Bürokratiekosten für die zu erwartende Anzahl an Meldungen der Betreiber an das BSI mit 600 Mio. EUR beziffert.[41] Für die aufgrund der Sicherungspflicht anfallenden Personal- und Infrastrukturkosten liegen keine Zahlen vor. Das Bundesverfassungsgericht erachtet die Indienstnahme von privaten Unternehmen zugunsten öffentlicher Aufgaben im Hinblick auf die Kostenlast dann als unzumutbar, wenn die Rentabilität des betroffenen Unternehmens nicht nur „geringfügig gemindert" wird, wenn „eine maßgebliche Beeinflussung des gewerblichen Gesamtgewinns" droht und wenn die Bindung der betrieblichen Mittel des betroffenen Unternehmens „für die Betriebsführungen von ausschlaggebendem Gewicht" ist.[42]

Der Umfang der tatsächlich anfallende Kostenlast kann derzeit – bevor bekannt ist, wie viele und welche Betreiber Adressaten des Gesetzes sind und welcher organisatorische wie technische Aufwand zu erbringen ist – nicht abgeschätzt werden. Inwiefern sich die tatsächlich anfallende Kostenlast als rechtswidrige unzumutbare Indienstnahme darstellt, wird somit eine Frage der **Rechtmäßigkeit der konkretisierenden Verordnung**, nicht der Verfassungsmäßigkeit der BSI-Gesetz-Entwurfsfassung sein. Zu unterstreichen ist insoweit nochmals, dass § 8a Abs. 1 BSI-Gesetz-Entwurfsfassung die Betreiber lediglich zu „angemessenen" organisatorischen und technischen Vorkehrungen verpflichtet.

3.4. Zwischenergebnis

Der Eingriff in die Berufsausübungsfreiheit der Betreiber durch die Sicherungs- und Meldepflichten ist durch das Ziel der Erhöhung der IT-Sicherheit legitimiert. Im Hinblick auf die Verhältnismäßigkeit der Maßnahme erweist sich diese als geeignet und erforderlich. Im Rahmen der Angemessenheit ist festzuhalten, dass der Grundrechtseingriff aufgrund seiner tatbestandlichen Beschränkungen in seiner Intensität nicht außer Verhältnis zum verfolgten Zweck steht. Die Bewertung der Zumutbarkeit der Kostenlast hängt entscheidend von der Konkretisierung des Adressatenkreises und der zu erfüllenden Standards durch die zu erlassende Rechtsverordnung ab.

---

39 Vgl. auch Hornung, Selbstanzeigepflicht zum Wohle der IT-Sicherheit?, NJW-Editorial, Heft 40/2014.

40 Vgl. BT-Drs. 18/4096, S. 5.

41 KPMG, IT-Sicherheit in Deutschland, online verfügbar unter: http://www.bdi.eu/download_content/KPMG_IT-Sicherheit_in_Deutschland.pdf (zuletzt abgerufen am 14. April 2015).

42 Vgl. BVerfGE 7, 377 (405); vgl. zu allem Scholz, in: Maunz/Dürig, Grundgesetz-Kommentar, 72. Ergänzungslieferung 2014, Art. 12 Rn. 163.

4. Verletzung des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)?

4.1. Bestimmungen des Entwurfs

Der Entwurf verpflichtet die Betreiber in § 8b Abs. 4 BSI-Gesetz-Entwurfsfassung im Rahmen der bereits angesprochenen Meldepflicht, **erhebliche Störungen unverzüglich an das BSI zu melden**. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist hingegen nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. § 8b Abs. 2 BSI-Gesetz-Entwurfsfassung sieht vor, dass das BSI die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik **wesentlichen Informationen sammelt und auswertet**. Dies sind insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise.

4.2. Kritik

Die durch den Entwurf begründete Meldepflicht (**Erhebung von Daten**) und die Befugnis des BSI, die Daten zu sammeln und auszuwerten (**Speicherung und Verwendung von Daten**), werden teilweise als Verletzung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG erachtet. Durch die umfangreiche Datenerhebung sei es möglich, die Sicherheitsvorfälle bestimmten Betreibern zuzuordnen, was deren Rechte verletze.[43] Darüber hinaus räume der Entwurf dem BSI eine zu umfassende und damit unzulässige Möglichkeit der Datenspeicherung ein.[44]

4.3. Verfassungsrechtliche Würdigung

Das **Grundrecht auf informationelle Selbstbestimmung** schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[45] Auch juristische Personen können sich dem Grunde nach auf das Grundrecht berufen, da es sich nicht nur individuell sondern auch korporativ wahrnehmen lässt (vgl. Art. 19 Abs. 3 GG).[46] Bei der Bestimmung, welche Daten eines Unternehmens dem Schutz der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unterfallen, ist maßgeblich auf die Bedeutung der betroffenen Informationen für den

---

43 Vgl. Ahlhaus/Holzinger, Verfassungsrechtliche Stellungnahme im Auftrag des Cyber-Sicherheitsrat Deutschland e.V. zum Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015, unveröffentlicht, S. 34 ff.

44 Vgl. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Stellungnahme des FIfF zum IT-Sicherheitsgesetz der Bundesregierung vom 17. Dezember 2014, S. 1.

45 BVerfGE 118, 168 (184); 120, 274 (312).

46 Vgl. BVerfGE 118, 168 (203 f.).

grundrechtlich geschützten Tätigkeitskreis der juristischen Person abzustellen.[47] Somit sind nicht sämtliche mit dem Betreiber und dessen Tätigkeit verknüpfte Informationen vom Grundrecht auf informationelle Selbstbestimmung erfasst, sondern nur solche, die mit der wirtschaftlichen Betätigung im jeweiligen Sektor unmittelbar zusammenhängen. So hat das Bundesverfassungsgericht entschieden, dass die staatliche Erfassung von Kontostammdaten bei einem Kreditinstitut dessen wirtschaftliche Verhaltensfreiheit nicht gefährden würde und mithin keinen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.[48] Abgesehen davon gilt das Recht auf informationelle Selbstbestimmung nicht schrankenlos. Durch die sog. Schrankentrias des Art. 2 Abs. 1 GG ist der Gesetzgeber berechtigt, verhältnismäßige Freiheitsbeschränkungen auch des Rechts auf informationelle Selbstbestimmung vorzunehmen.

Zunächst ist zu klären, ob ein **Eingriff** in den Schutzbereich des Grundrechts vorliegt. Im Hinblick auf die **Erhebung von Daten** sieht der Entwurf in § 8b Abs. 4 S. 2 BSI-Gesetz-Entwurfsfassung vor, dass die Meldung der Betreiber **Angaben zu der Störung** sowie zu den **technischen Rahmenbedingungen**, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur **Branche des Betreibers** enthalten muss. Die **Nennung des Betreibers** ist dabei, wie dargestellt, nicht der Regelfall, sondern nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Unterhalb dieser Erforderlichkeitsschwelle kann die Meldung pseudonymisiert erfolgen.[49] Dadurch soll der besonderen Sensibilität der Meldungen im Hinblick auf die wirtschaftlichen Auswirkungen eines möglichen Bekanntwerdens entsprechender Vorfälle Rechnung getragen werden.[50]

Sofern solche Daten erhoben werden, die **Angaben zu der Störung** sowie den **technischen Rahmenbedingungen** enthalten, es sich also um Informationen technischer Natur handelt[51], stellt dies nach den vorgenannten Grundsätzen **keinen Eingriff** in den Schutzbereich des Rechts auf informationelle Selbstbestimmung dar, da diese Daten nicht mit der wirtschaftlichen Betätigung der Betreiber im jeweiligen Sektor unmittelbar zusammenhängen. Dies dürfte im Ergebnis auch für die verpflichtende Meldung der **Branche des Betreibers** gelten. Denn obgleich die Branche näher an der Sphäre der wirtschaftlichen Betätigung des Betreibers zu verorten ist als die vorgenannten Informationen technischer Natur, dürfte die anonymisierte Meldung der Branche ohne weiteren Bezug zum Betreiber nicht dessen wirtschaftliche Verhaltensfreiheit im jeweiligen Sektor gefährden.

Sofern eine Meldung die **Nennung des Betreibers** vorsieht, so stellt dies zwar einen **Eingriff** in das Recht auf informationelle Selbstbestimmung dar. Da das Gesetz jedoch bereits auf tatbestandlicher Ebene anordnet, dass die Nennung des Betreibers nur erforderlich ist, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastruktur geführt hat, wird dieser Eingriff als **verhältnismäßig** und als verfassungsrechtlich gerechtfertigt anzusehen sein. Denn im Szenario des Ausfalls oder einer Beeinträchtigung der Funktionsfähigkeit

47 Vgl. BVerfGE 118, 168 (203 f.).

48 Vgl. BVerfGE 118, 168 (203 f.).

49 Vgl. BT-Drs. 18/4096, S. 47.

50 Vgl. BT-Drs. 18/4096, S. 47.

51 Vgl. BT-Drs. 18/4096, S. 48.

der kritischen Infrastruktur steht dem Eingriff durch die Pflicht zur namentlichen Nennung des Betreibers das kollektive Interesse der Gemeinschaft gegenüber, den konkreten Störungsfall aufzuklären. Denn dieser soll beim betroffenen Betreiber behoben werden, damit die kritische Infrastruktur wieder zur Verfügung steht, und der Informationszugewinn soll zum Schutz der übrigen kritischen Infrastruktur genutzt werden.

Im Hinblick auf die Befugnis des BSI, **Daten zu speichern und zu verwenden,** bezieht sich § 8b Abs. 2 Nr. 1 BSI-Gesetz-Entwurfsfassung nur auf „die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentliche Informationen", „insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise". Die Befugnis des BSI bezieht sich somit primär auf Informationen technischer Natur. Darin ist nach oben genannten Grundsätzen bereits **kein Eingriff** in das Recht auf informationelle Selbstbestimmung zu sehen.

Teilweise wurde die Befürchtung vorgebracht, im Einzelfall könne bei der Erhebung dieser Daten ein Personenbezug auftreten.[52] Durch den Personenbezug könnte die Datenspeicherung dann einen **Eingriff** darstellen. Zu dieser Problematik sieht der Entwurf in § 8b Abs. 6 BSI-Gesetz-Entwurfsfassung vor, dass Informationen mit Personenbezug nur zu den in dieser Vorschrift vorgesehenen Zwecken erhoben, verarbeitet oder genutzt werden dürfen. Eine darüber hinausgehende Verarbeitung und Nutzung zu anderen Zwecken ist unzulässig. Da außerdem die allgemeinen datenschutzrechtlichen Regelungen gelten, ist auch der Grundsatz der Datensparsamkeit nach § 3a BDSG anzuwenden. Daher müssen alle Beteiligten die Möglichkeiten zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten anwenden.[53] Sollte es also im Einzelfall durch die Speicherung und Verwendung von Daten zu einem Eingriff in das Recht auf informationelle Selbstbestimmung kommen, dürfte ein solcher Eingriff angesichts der datenschutzrechtlichen Schutzvorkehrungen als **verhältnismäßig** anzusehen sein.

4.4. Zwischenergebnis

Die durch den Entwurf begründete Befugnis des BSI, **Daten zu erheben, zu speichern und zu nutzen**, bezieht sich im Wesentlichen auf Informationen technischer Natur. Diese unterfallen nicht dem Schutzbereich des Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG, der juristische Personen vor Gefährdungen hinsichtlich ihrer spezifischen Freiheitsausübung, hier also der Berufsausübungsfreiheit, schützt. Somit stellen die Erhebung, Speicherung und Nutzung solcher Daten von Betreibern Kritischer Infrastruktur grundsätzlich keinen Grundrechtseingriff dar. Sofern es im Einzelfall – wie teilweise befürchtet – zur Erhebung, Speicherung oder Nutzung von personenbezogenen Daten kommt, sieht der Entwurf effektive Datenschutzmechanismen vor, die etwaige Eingriffe als verhältnismäßig und damit gerechtfertigt erscheinen lassen. Die Nennung des Betreibers im Rahmen der Meldepflicht ist schließlich nur in Ausnahmefällen erforderlich. Der Entwurf geht vom Grundsatz der anonymen Meldung aus und trägt damit der Sensibilität Rechnung, die

52 Vgl. Roßnagel, Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), S. 20.

53 Vgl. Roßnagel, Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), S. 20.

im Zusammenhang mit dem Bekanntwerden von Störungsfällen für die Betreiber besteht. Die Bestimmungen erscheinen somit verfassungsgemäß.

5. Verletzung des Gebots der Folgerichtigkeit bzw. des allgemeinen Gleichheitssatzes (Art. 3 Abs. 1 GG)?

5.1. Kritik an der Nichteinbeziehung von Bundesbehörden

Schließlich wird teilweise kritisiert, dass **Bundesbehörden von der gesetzlichen Definition der Kritischen Infrastruktur ausgenommen** und deshalb nicht Adressaten der Schutz- und Meldepflichten sind. Dies sei mit dem verfassungsrechtlichen Gebot der Folgerichtigkeit der Gesetzgebung nicht vereinbar und verletze deshalb Art. 3 Abs. 1 GG.[54]

5.2. Verfassungsrechtliche Würdigung

Dem angesprochenen **Gebot der Folgerichtigkeit** (das auch unter den Begriffen der Systembindung, Systemgerechtigkeit oder Rationalität des Gesetzgebers diskutiert wird) liegt der Gedanke zugrunde, dass der Gesetzgeber zwar in weitem Umfang frei entscheiden könne, nach welchen inhaltlichen Grundsätzen er einzelne gesetzliche Regelungen ausgestaltet, er innerhalb des gewählten Systems jedoch verpflichtet sei, an den gewählten Grundsätzen festzuhalten.[55] Das Gebot wird überwiegend im Rahmen des allgemeinen Gleichheitssatzes des Art. 3 Abs. 1 GG diskutiert. Was genau das Gebot der Folgerichtigkeit für die Prüfung des Gleichheitssatzes bedeutet, wird indes unterschiedlich beurteilt, so dass eine genaue Konturierung des Konzepts schwerfällt.[56] Überwiegend – insbesondere seitens des Bundesverfassungsgerichts – wird jedoch angenommen, dass die fehlende Folgerichtigkeit einer Regelung einen Gleichheitsverstoß „allenfalls“[57] indizieren könne. Eine Verfassungswidrigkeit begründet sie nicht.[58] Dies erscheint unausweichlich, muss es dem Gesetzgeber doch gestattet sein, von bisherigen Regelungssystemen auch wieder abzuweichen. Denn ansonsten würde jede sinnvolle und sachgerechte Ausnahme, jede Anwendung entgegenstehender Gesichtspunkte oder Prinzipien einen Systembruch darstellen, der zur Verfassungswidrigkeit der jeweiligen Regelung führen würde.[59] Auch die offensichtliche Inkonsequenz einer Regelung führt nicht automatisch zu deren Verfassungswidrigkeit. Maßgeblich für die Bemessung der Verfassungsmäßigkeit des Entwurfs im Hinblick auf die angebliche Ungleichbehandlung von Betreibern und Bundesbehörden

54 Vgl. Ahlhaus/Holzinger, Verfassungsrechtliche Stellungnahme im Auftrag des Cyber-Sicherheitsrat Deutschland e.V. zum Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015, unveröffentlicht, S. 11 ff.

55 Vgl. Payandeh, Das Gebot der Folgerichtigkeit: Rationalitätsgewinn oder Irrweg der Grundrechtsdogmatik, AöR 136 (2011), 578 (579).

56 Vgl. Kischel, in: Epping/Hillgruber, BeckOK GG, 23. Edition 2014, Art. 3 Rn. 95.

57 BVerfGE 81, 156 (207).

58 Vgl. Kirchhof, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VIII, 3. Auflage, § 181 Rn. 220; Rüfner, in: Bonner Kommentar zum Grundgesetz, 170. Ergänzungslieferung 2014, Art. 3 Rn. 38; BVerfGE 81, 156 (207); 68, 237 (253).

59 Vgl. Kischel, in: Epping/Hillgruber, BeckOK GG, 23. Edition 2014, Art. 3 Rn. 95.

ist, ob eine Verletzung des allgemeinen Gleichheitssatzes des Art. 3 Abs. 1 GG festzustellen ist. Aus der Ausklammerung von Bundesbehörden per se auf eine Verfassungswidrigkeit wegen fehlender Folgerichtigkeit zu schließen, würde die Reichweite des Gebots der Folgerichtigkeit überstrapazieren.

Art. 3 Abs. 1 GG gebietet dem Gesetzgeber, **wesentlich Gleiches gleich und wesentlich Ungleiches ungleich** zu behandeln. Aus ihm ergeben sich je nach Regelungsgegenstand und Differenzierungsmerkmalen unterschiedliche Grenzen für den Gesetzgeber, die vom bloßen Willkürverbot bis zu einer strengen Bindung an Verhältnismäßigkeitserfordernisse reichen.[60] Auch inländische juristische Personen des Privatrechts können sich, wie dargestellt, nach Art. 19 Abs. 3 GG dem Grunde nach auf grundrechtlich gewährleistete Rechtspositionen berufen. Dies gilt auch für den allgemeinen Gleichheitssatz.[61]

Ob zwei Sachverhalte gleich oder ungleich behandelt werden, beurteilt sich anhand eines Vergleichs der Rechtsfolgen.[62] Die Betreiber treffen die Pflichten des IT-Sicherheitsgesetzes, da sie dem Begriff der Kritischen Infrastruktur unterfallen. Bundesbehörden treffen diese Rechtsfolgen indes nicht. Die Sachverhalte werden somit **ungleich behandelt**. Zentral für die Beurteilung der Verfassungsmäßigkeit dieser Ungleichbehandlung ist nun, ob beide Gruppen als „gleich“ im Sinne des allgemeinen Gleichheitssatzes anzusehen sind und sich die Ungleichbehandlung somit als verfassungswidrig darstellt oder aber, ob beide Gruppen als „ungleich“ im Sinne des allgemeinen Gleichheitssatzes anzusehen sind und die Ungleichbehandlung durch den Entwurf deshalb verfassungsrechtlich zulässig ist.

Bei der Bestimmung der Frage, ob die **Sachverhalte gleich oder ungleich** sind, bietet es sich an, diejenigen Eigenschaften zu sammeln, in denen sich die betrachteten Sachverhalte gleichen und unterscheiden.[63] Im Hinblick auf juristische Personen muss insbesondere der jeweilige Lebens- und Sachbereich berücksichtigt werden.[64]

Es liegt nahe, die Betreiber und Bundesbehörden aufgrund ihrer strukturellen Unterschiede als **ungleich** anzusehen. Die Betreiber, als juristische Personen des Privatrechts, und Bundesbehörden, als Organe des Bundes, gehören unterschiedlichen rechtlichen Ordnungsbereichen an. Daraus ergeben sich vielfältige Unterschiede, etwa im Hinblick auf die Möglichkeit des Staates im Rahmen der Staatssteuerung auf die jeweiligen Gruppen einzuwirken. Der Staat darf in die grundrechtliche Freiheitssphäre Privater nur eingreifen, wenn er verfassungsrechtlich dazu ermächtigt ist und die Anforderungen einhält, die die Verfassung an Eingriffe der jeweiligen Art stellt. Demgegenüber kann die Steuerung von Bundesbehörden jederzeit durch schlichte Verwaltungsvorschriften erfolgen. Privatrechtliche Unternehmen, die Grundrechtsträger sind, und Behörden, die als Teile des Staates keine Grundrechtsträger sind, erscheinen daher als strukturell ungleich im Sinne des

60 BVerfGE 110, 274 (291).

61 Vgl. BVerfGE 3, 383 (390).

62 Vgl. Kischel, in: Epping/Hillgruber, BeckOK GG, 23. Edition 2014, Art. 3 Rn. 15.

63 Vgl. Kischel, in: Epping/Hillgruber, BeckOK GG, 23. Edition 2014, Art. 3 Rn. 15.

64 Vgl. BVerfGE 25, 269 (292).

Gleichheitssatzes. Eine Ungleichbehandlung der beiden Gruppen erscheint schon insoweit verfassungsrechtlich unbedenklich.

Teilweise werden die Gruppen hingegen als im Hinblick auf die Zweckrichtung des IT-Sicherheitsgesetzes gleich angesehen, da beide als Kritische Infrastruktur angesehen werden können:

So können in der Sache auch Bundesbehörden die definitorischen Anforderungen, die § 2 Abs. 10 S. 2 BSI-Gesetz-Entwurfsfassung an die Einrichtungen stellt, die den sieben Sektoren angehören, erfüllen: Zweifelsohne können auch Bundesbehörden von hoher Bedeutung für das Funktionieren des Gemeinwohls sein, weil durch ihren Ausfall oder ihre Beeinträchtigung Gefährdungen für die öffentliche Sicherheit eintreten würden.

Darüber hinaus hat auch das Bundesministerium des Innern den Sektor „Staat und Verwaltung" in seine Einteilung der Kritischen Infrastruktur in neun Sektoren aufgenommen.[65] Diese Aufteilung hat die Bundesregierung bei der Aufstellung des „Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit: Selbstbestimmt und sicher in der digitalen Welt 2015 - 2020"[66] aufgegriffen.

Schließlich lässt sich einem Vorschlag der Europäischen Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union entnehmen, dass die Kommission die Systeme der öffentlichen Verwaltung als wesentlich für das Funktionieren des Binnenmarkts erachtet. Denn danach sollen auch diese von den Mitgliedstaaten verpflichtet werden, „geeignete Schritte zur Beherrschung von Sicherheitsrisiken zu unternehmen und den zuständigen nationalen Behörden gravierende Sicherheitsvorfälle zu melden."[67]

Folgt man dieser Ansicht und sieht die privaten Betreiber und Bundesbehörden als im Hinblick auf die IT-Sicherheit gleich an, lässt sich die dann entstehende gesetzliche Ungleichbehandlung von Gleichem allerdings durch sachgerechte Gründe **rechtfertigen**.

Zunächst enthält das **BSI-Gesetz** in den §§ 4, 5 und 8 **bereits Spezialregelungen** für die Bereiche Regierung, Parlament und öffentliche Verwaltung. Insbesondere sind Bundesbehörden in Bezug auf **Meldepflichten** gemäß § 4 Abs. 3 BSI-Gesetz verpflichtet, alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, die ihnen bekannt werden und für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, unverzüglich dem BSI zu melden. § 8 Abs. 1 BSI-Gesetz sieht in Bezug auf die **Sicherungspflicht** vor, dass das BSI Mindeststandards für die Sicherung der Informationstechnik des Bundes festlegen kann. Insofern ist es **sachgerecht**, dass die in der Entwurfsfassung genannten

65 Vgl. BT-Drs. 18/4304, S. 12.

66 Vgl. BT-Drs. 18/4304.

67 KOM (2013), 48: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, online verfügbar unter: http://www.bundesanzeiger-verlag.de/fileadmin/Betrifft-Recht/Dokumente/externe%20dokumente/COM_2013__48_final.pdf (zuletzt abgerufen am 16. April 2015), S. 2.

Melde- und Sicherungspflichten nicht auch die Behörden des Bundes treffen und somit doppelt verpflichten bzw. doppelte Rechtsgrundlagen schaffen.

Darüber hinaus erscheint es auch – bei unterstellter Gleichheit – sachgerecht, dass die Steuerung von juristischen Personen des Privatrechts und von bundeseigenen Organen bereits dem Grunde nach unterschiedlich erfolgt. Dies fußt auf oben angesprochenen strukturellen Unterschieden zwischen Betreibern als juristischen Personen des Privatrechts und Bundesbehörden als Organen des Bundes. Aufgrund der unterschiedlichen staatlichen Steuerungs-, Einwirkungs- und Erkenntnismöglichkeiten erscheint es gerechtfertigt, private Einrichtungen zu Adressaten eines Gesetzes zu machen, während Bundesbehörden vom Anwendungsbereich des Gesetzes nicht umfasst sind.

5.3. Zusammenfassung

Eine verfassungswidrige Ungleichbehandlung ist nach alledem nicht zu erkennen.

6. Ergebnis

Insgesamt begegnet der Entwurf des IT-Sicherheitsgesetzes keinen durchgreifenden verfassungsrechtlichen Bedenken.

[redacted] [redacted]