Prof. Dr. Gerrit Hornung, LL.M.

Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 G

Telefon Prof. Dr. Gerrit Hornung, LL.M. 0851 509-2380
Telefax 0851 509-2382
e-mail gerrit.hornung @uni-passau.de

Datum 18. April 2015

Stellungnahme

zur öffentlichen Anhörungen des Innenausschusses des Deutschen Bundestages am 20. April 2015

zum Gesetzentwurf der Bundesregierung für Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 25. Februar 2015, BT-Drs. 18/4096

Gliederung

1 Grundsätzliche Einordnung

Der Gesetzentwurf adressiert ein **hochgradig relevantes Problem der Informationsgesellschaft**. In dieser geraten Bürger, Wirtschaft und Staat in erhebliche Abhängigkeit zu der Verfügbarkeit funktionsfähiger, integrer und vertraulicher Informationstechnologie (IT). Die Risiken, die aus unsicherer IT entstehen können, betreffen direkt wichtige Bereiche des gesellschaftlichen und individuellen Lebens. Ursachen können Fehler und Mängel der verwendeten Systeme, aber auch private und staatliche Angreifer sein. Die Bedrohungen für die IT-Sicherheit in Deutschland sind real und konkret.[1]

Aus rechtlicher Sicht ist die Gewährleistung der IT-Sicherheit zum einen **Teil der staatlichen Infrastrukturverantwortung**. Zum anderen hat der Staat auch eine Pflicht, sich schützend und fördernd vor die Grundrechte der Bürgerinnen und Bürger zu stellen. Dies betrifft eine **Vielzahl von Grundrechten**, deren Ausübung heutzutage nicht mehr ohne funktionsfähige IT möglich ist, insbesondere aber das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Bürger, Wirtschaft und Staat sind besonders betroffen, wenn es um Kritische Infrastrukturen geht, deren Ausfall nicht nur einzelnen Individuen und Organisationen, sondern einer Vielzahl von ihnen Nachteile zufügen können. Wie in anderen Bereichen der Regulierung Kritischer Infrastrukturen stellt sich auch für die IT-Sicherheit die **Frage des sinnvollen Maßes an staatlichen Vorgaben einerseits, Selbstverantwortung und Selbstregulierung andererseits**. IT-Sicherheitsmaßnahmen weisen hier Besonderheiten auf: Sie sind typischerweise Vorsorgemaßnahmen, die kostenträchtig und gerade im Erfolgsfall schwer zu rechtfertigen sind, weil die hypothetischen Schadensfälle schwer plausibel gemacht werden können. Kommen IT-Sicherheitsvorfälle vor, so betreffen diese in aller Regel nicht nur einen Akteur, weil dieselben Systeme bei vielen anderen eingesetzt werden. Schließlich haben die Verantwortlichen ein natürliches Interesse, Vorfälle (vor allem, aber nicht nur solche, aus denen sich ein vorwerfbares Verhalten ergibt) nicht publik werden zu lassen, weil der Verlust von Reputation und Kundenvertrauen befürchtet wird.

Wenn die intrinsischen Anreize für kostenträchtige Maßnahmen gering, die potentiellen Auswirkungen von Vorfällen weit verbreitet, die Kommunikation hierüber aber unterentwickelt ist, so ist eine **Kombination aus materiellen Standards mit Meldepflichten für IT-Sicherheitsvorfällen eine grundsätzlich sinnvolle Strategie**. Diese wird in vergleichbaren Fällen bereits verfolgt, etwa im Datenschutzrecht (§ 42a BDSG, § 15a TMG, § 109a TKG, § 83a SGB X). Die Übernahme dieser Regelungsstrategie ist ein zu unterstützender

---

[1] S. nur *BSI*, Die Lage der IT-Sicherheit in Deutschland 2014.

Schritt zur Verrechtlichung der IT-Sicherheit, der durch den **kooperativen Ansatz einer Zusammenarbeit zwischen Behörden und Wirtschaft** auch Chancen für die Verbesserung der Widerstandsfähigkeit der zugrundeliegenden Infrastrukturen bietet.

Die **Abstufung zwischen erheblichen und nicht erheblichen Störungen** (nur erstere sind meldepflichtig) sowie zwischen Störungen **mit und ohne tatsächlichen Auswirkungen** (nur bei ersteren muss der konkrete Betreiber genannt werden, dessen System tatsächlich ausgefallen oder beeinträchtigt wurde) ist **sinnvoll** und berücksichtigt die berechtigten Interessen der Betreiber, nicht mit aufwändigen Meldungen zu unwesentlichen Vorfällen überfrachtet zu werden sowie pseudonym agieren zu können, sofern es nicht zu tatsächlichen Ausfällen oder Beeinträchtigungen gekommen ist.

Gerade weil der Gesetzentwurf ein sinnvolles Anliegen verfolgt, ist darauf hinzuweisen, dass **wesentliche, gleichfalls sinnvolle Inhalte einer umfassenden IT-Sicherheitsstrategie nicht adressiert werden**. So sind beispielsweise IT-Sicherheitsvorfälle bei Unternehmen, die nicht Betreiber Kritischer Infrastrukturen sind, nicht erfasst. Dies betrifft insbesondere die gezielte Wirtschaftsspionage oder sonstige Angriffe auf Unternehmen, die keine Kritische Infrastruktur nach § 2 Abs. 10 BSIG-E betreiben. Ein Handeln des Staates erscheint daneben insbesondere dort wichtig, wo die Betreiber von IT-Systemen keine eigenen Anreize zur Verbesserung der IT-Sicherheit haben (diese sind beim Betrieb Kritischer Infrastrukturen grundsätzlich vorhanden, weil bei Ausfällen direkt Kundeninteressen verletzt werden), nämlich in den Bereichen der Forschung und Entwicklung, der Verfügbarkeit von Technologien zur Selbsthilfe der Bürger (vor allem Verschlüsselungsverfahren) und der unabhängigen Prüfung unter Verwendung von Open Source-Technologien.

2 Europarechtliche Aspekte

Da derzeit mit dem Entwurf der Europäischen Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-RL-E)[2] ein **paralleles Gesetzgebungsverfahren** betrieben wird, stellt sich Frage der Vereinbarkeit des Vorschlags mit den absehbaren europäischen Regelungen. Im Grundsatz verfolgen beide Vorschläge dabei das **identische Ziel** der Verbesserung der IT-Sicherheit bei Kritischen Infrastrukturen und sehen weitgehend kongruente Mittel vor, nämlich zum einen die Vorgabe von IT-Sicherheitsstandards, zum anderen Meldepflichten bei IT-Sicherheitsvorfällen. **Dennoch gibt es Unterschiede**, von denen hier

[2] KOM(2013) 48.

einige anhand der Zusammenstellung in der letzten Position des Rates vom 5. März 2015[3] erläutert werden sollen:

- Noch nicht absehbar ist, wie groß die Unterschiede hinsichtlich des **Adressatenkreises** sein werden. Die Kommission wollte die öffentliche Verwaltung explizit in die Pflicht nach Art. 14 Abs. 1 NIS-RL-E einbeziehen, scheint sich damit aber nicht durchsetzen zu können. In der letzten Position des Rates werden nunmehr aber „operator" erfasst, die nach der Definition in Art. 3 Abs. 8 NIS-RL-E „**public or private entities**" sein können. Hieraus könnten sich Unterschiede zum Gesetzentwurf ergeben. In den meisten anderen Bereichen dürfte es wegen der offenbar beabsichtigten Befugnis der Mitgliedsstaaten zur Definition der betroffenen Betreiber möglich sein, im Rahmen der Verordnung nach § 10 Abs. 1 BSIG-E richtlinienkonform zu agieren.

- Nach Art. 6 NIS-RL-E müssen die Mitgliedsstaaten **nationale Anlaufstellen** einrichten. Dem genügt der Gesetzentwurf in seiner vorliegenden Form. Weiterer gesetzgeberischer Bedarf könnte sich je nach dem endgültigen Inhalt der Vorgaben in Art. 8a und Art. 8b NIS-RL-E hinsichtlich der Zusammenarbeit mit anderen nationalen Behörden und der ENISA ergeben.

- In allen bisher bekannten Positionen beschränken sich die europäischen Entwürfe hinsichtlich der Meldepflichten auf Sicherheitsvorfälle („**incidents**"). Diese werden in Art. 3 NIS-RL-E definiert als „alle Umstände oder Ereignisse, die tatsächlich negative Auswirkungen auf die Sicherheit haben". Der vorliegende **Gesetzentwurf geht an mehreren Stellen hierüber hinaus**, wenn er in § 8b Abs. 4 BSIG-E auch Störungen umfasst, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen führen „können".

- Hinsichtlich einer **Veröffentlichung der gewonnenen Erkenntnisse** enthält Art. 14 Abs. 4 NIS-RL-E eine Befugnis der Behörde. Diese ist **zugleich weiter und enger als die Regelung in § 8d Abs. 1 BSIG-E**. Sie ist weitergehend, weil sie sich explizit auf „individual incidents" beziehen wird und die Interessen der Öffentlichkeit an der gewonnenen Information berücksichtigt. Demgegenüber enthält sie anders als der nationale Vorschlag eine Pflicht zur Anhörung des betroffenen Unternehmens.

- Art. 15 Abs. 2 lit. a NIS-RL-E wird vermutlich vorsehen, dass die nationalen Behörden die **Befugnis** erhalten müssen, von den Betreibern Kritischer Infrastrukturen

---

[3] Abrufbar unter http://statewatch.org/news/2015/mar/eu-council-NIS-consolidated-multi-col-6788-15.pdf.

die **Durchführung eines Sicherheitsaudits zu verlangen**. Dies geht **deutlich über die Regelung in § 8a Abs. 3 BSIG-E hinaus**, der solche Audits gleichberechtigt neben Zertifizierungen und Prüfungen stellt und alle drei lediglich fakultativ nennt.

- In Art. 15 Abs. 3 NIS-RL-E ist vorgesehen, dass die zuständige Behörde „**verbindliche Anweisungen**“ an die Betreiber Kritischer Infrastrukturen zu richten. Auch dies ergibt sich **nicht aus dem Gesetzentwurf**.
- Art. 17 NIS-RL-E sieht die Pflicht für die Mitgliedsstaaten vor, **Sanktionen für eine Verletzung** der Pflichten aus Art. 14 und Art. 15 NIS-RL-E vorzusehen. Dies betrifft sowohl die Einhaltung der IT-Sicherheitsstandards selbst, als auch eine Verletzung der entsprechenden Meldepflichten. Beides enthält der **vorliegende Gesetzentwurf nur sehr rudimentär** (s.u. 4.3 und 5.4).

Insgesamt ergeben sich die größten Unterschiede zu dem geplanten europäischen Vorhaben auf der Ebene der Verpflichteten sowie hinsichtlich der Sanktionsbefugnisse des BSI. Zumindest letzteres ließe sich mutmaßlich nach Abschluss des europäischen Gesetzgebungsvorhabens relativ leicht in das Gesetz integrieren. Sollten sich auf europäischer Ebene hingegen erweiterte **Auswirkungen hinsichtlich der betrieblichen Prozesse** ergeben, sollte zunächst der europäische Gesetzgebungsprozess **abgewartet werden**, um einen nachträglichen Änderungsaufwand bei den Betroffenen Anbietern zu vermeiden.

3 Anwendungsbereich

Angesichts der Pflicht zur Implementierung potenziell kostenträchtige IT-Sicherheitsmaßnahmen und mehr oder weniger aufwändiger Meldeverfahren ist es für die betroffenen Unternehmen von erheblicher Bedeutung zu wissen, ob sie von dem Gesetzentwurf erfasst sind.

3.1 Begriff der Kritischen Infrastrukturen

Die Begriffsbestimmung in § 2 Abs. 10 BSIG-E ist mit Blick auf ihren **Bestimmtheitsgrad vielfach kritisiert** worden.[4]

In der Tat ist der personelle Anwendungsbereich auf Basis des Entwurfs in vielen Fällen nicht ermittelbar. Viele Unternehmen sind in den „Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie

[4] Z.B. *Roos*, K&R 2013, 769, 770; *Heinickel/Feiler*, CR 2014, 708, 713 f.; *Leisterer/Schneider*, CR 2014, 574; 577; *Bräutigam/Wilmer*, ZRP 2015, 38, 40 sowie zahlreiche Stellungnahmen der betroffenen Wirtschaftsverbände.

Finanz- und Versicherungswesen“ tätig (§ 3 Abs. 10 Nr. 1 des Entwurfs). Auch die Präzisierung in Nr. 2 (Einrichtungen, Anlagen oder Teile von diesen, die für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden) führt in vielen Fällen nicht dazu, dass Unternehmen die Anwendbarkeit des Entwurfs auf sich selbst dem Gesetz entnehmen können.

Für die Verordnungsermächtigung in § 10 Abs. 1 BSIG-E gilt **Art. 80 Abs. 1 Satz 2 GG**, wonach Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetze bestimmt werden müssen. Unter Wesentlichkeitsgesichtspunkten ist der **personale Anwendungsbereich** eines Gesetzes in jedem Fall eine **wichtige Frage**. Insoweit gibt die Vorgabe in Nr. 2 dem Verordnungsgeber Leitlinien für die nähere Bestimmung in die Hand. Es wird danach maßgeblich auf die Auswirkungen eines Versagens der jeweiligen Infrastruktur ankommen, nicht auf die Größe des Unternehmens, seine Leistungsfähigkeit oder die Komplexität der betriebenen Infrastruktur. Unter Berücksichtigung dieser Kriterien erscheint die **Übertragung an den Verordnungsgeber als vertretbar**.

Rechtspolitisch und mit Blick auf den Wesentlichkeitsgrundsatz wäre eine **präzisere Bestimmung dennoch wünschenswert**. Wenn in der Gesetzesbegründung bereits die relativ konkrete Zahl von maximal 2.000 Unternehmen genannt wird, die von den Regelungen betroffen sein werden,[5] sind offenbar ja bereits Kriterien verfügbar, nach denen diese Zahl ermittelt wurde. Der durch den Gesetzgeber für den Prozess der Verabschiedung der Rechtsverordnung vorgesehene „Arbeitsprozess mit Vertretern der möglicherweise betroffenen Betreiber Kritischer Infrastrukturen und unter Einbeziehung der Expertise von externen Fachleuten“[6] kann zumindest hinsichtlich der allgemeineren Kriterien auch **im Rahmen des Gesetzgebungsverfahrens** erfolgen. Die an derselben Stelle genannten Kriterien der Quantität und Qualität sind sicher zutreffend. Sie könnten aber im Gesetz selbst (das sie bisher nicht erwähnt) genannt und weiter ausdifferenziert werden. Einige der insoweit genannten differenzierenden Maßstäbe[7] ließen sich in den Gesetzentwurf selbst integrieren und würden so einen deutlichen Gewinn an Rechtssicherheit in dem durch den parlamentarischen Gesetzgeber beschlossenen Normtext bedeuten.

Auch nach einer solchen Präzisierung wäre eine **weitere Konkretisierung** in der Rechtsverordnung nach § 2 Abs. 10 BSIG-E erforderlich. Hier sind unter rechtsstaatlichen Ge-

---

5 BT-Drs. 18/4096, 21; ein BDI Gutachten geht von wesentlich mehr Unternehmen aus eher 20.000 mit wesentlich mehr Vorfällen (http://www.bdi.eu/download_content/KPMG_IT-Sicherheit_in_Deutschland.pdf, 31).

6 BT-Drs. 18/4096, 23.

7 S. den Begründungsentwurf, BT-Drs. 18/4096, 30 f.

sichtspunkten unbedingt konkrete und handhabbare Schwellwerte anzugeben. Es wäre nicht zu rechtfertigen, wenn die Betreiber nicht erkennen könnten, ob sie von dem Gesetz überhaupt erfasst werden. Sollten insoweit Unklarheiten bleiben, wäre es erforderlich, ein **behördliches Feststellungsverfahren** vorzusehen.

3.2 Nicht von der Meldepflicht erfasste Institutionen

Anders als noch der Referentenentwurf vom 18. August 2014 nimmt die Definition der Kritischen Infrastrukturen in § 2 Abs. 10 BSIG-E nicht mehr pauschal Kommunikationstechnik des Bundes (§ 2 Abs. 3 Satz 1 und 2 BSIG) aus. Dennoch geht die Begründung davon aus, dass die **Verwaltung von Regierung und Parlament sowie die öffentliche Bundesverwaltung** und die von ihr eingesetzte Technik **nicht erfasst sind**.[8] Aus dem Gesetzentwurf ergibt sich dies an sich nicht.

In der Sache ist diese Ungleichbehandlung jedoch auch **nicht zu rechtfertigen**. Es stimmt zwar, dass insoweit die Spezialregelungen der §§ 4, 5 und 8 BSIG greifen. Wieso allerdings für die Standards der IT-Sicherheit und die Meldeverfahren unterschiedliche Maßstäbe gelten sollen, ist nicht ersichtlich. Auch Art. 3 Abs. 8 NIS-RL-E erfasst „public or private entities".

Der Gesetzentwurf gibt zutreffend an, dass der Bund für entsprechende Vorgaben für die Behörden und sonstige **Stellen der Länder** keine Kompetenz hätte. Dennoch entsteht insoweit eine **Lücke hinsichtlich der Vollständigkeit der durch das BSI gesammelten Informationen**. Sollte es bei dem vorliegenden Entwurf der europäischen Richtlinie bleiben, müssten die Länder entsprechende Vorgaben machen.

Schließlich weist die Begründung zutreffend darauf hin, dass der Bereich der **Kultur und Medien** aus Kompetenzgründen nicht erfasst sein kann.[9] Bestimmte Angebote und Systeme aus diesen Bereichen können allerdings **durchaus als Kritische Infrastrukturen** verstanden werden, wie sich an dem groß angelegten Angriff auf die französische Fernsehsendergruppe TV5Monde Anfang April 2015 gezeigt hat. Genau dieser Bereich der Massenmedien wird freilich vom Gesetzentwurf gerade nicht erfasst.

4 Vorgaben für IT-Sicherheitsstandards

Der Entwurf enthält eine Reihe inhaltlicher Vorgaben für IT-Sicherheitsstandards. Hierzu ist zu bemerken:

---

[8] BT-Drs. 18/4096, 24.
[9] BT-Drs. 18/4096, 24.

4.1 Inhaltliche Vorgaben

Nach § 8a Abs. 1 BSIG-E sind die Betreiber verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“. Dabei ist der **Stand der Technik** „zu berücksichtigen“.

„**Berücksichtigen**“ ist weniger, als den Stand der Technik „**einzuhalten**“ oder „**zu befolgen**“. Dies erscheint aus zwei Gründen misslich. Zum einen wird so das gesetzgeberische Ziel eines gleichmäßig hohen IT-Sicherheitsstandards **gerade nicht erreicht**. Zum anderen besteht für die betroffenen Unternehmen sogar dann Unklarheit über das konkret geforderte Sicherheitsniveau, wenn ein entsprechender Standard beschlossen wurde. Mit Blick auf die bereits geregelten und weiteren wünschenswerten Sanktionen (s.u. 4.3) ist dies schwer zu rechtfertigen.[10]

Eine **Präzisierung kann durch die branchenspezifischen Sicherheitsstandards** nach § 8a Abs. 2 BSIG-E erfolgen. Dies ist grundsätzlich sinnvoll, wirft aber die folgenden **Probleme** auf:

- In der Diskussion ist bereits auf das Problem hingewiesen worden, dass mehrere, **inhaltlich abweichende Standards für dieselbe Branche** vorgeschlagen werden;[11] dies wird im Entwurf nicht adressiert.
- Noch grundsätzlicher dürfte das Problem sein, dass das **BSI nicht von sich aus tätig werden kann**, sondern auf einen Vorschlag von Betreibern und Verbänden angewiesen ist. Unterbreiten diese keinen Vorschlag, verbleibt der Behörde nur die individuelle Beratung.
- Inhaltlich bezieht sich die Bestätigung des BSI auf die Anforderungen nach Abs. 1, also ebenfalls auf das „Berücksichtigen“ des Stands der Technik. Folglich kann die **Behörde Sicherheitsstandards anerkennen**, die **unterhalb des Stands der Technik** angesiedelt sind.
- Im Gesetz ist **nicht vorgesehen**, die erarbeiteten Standards zu pflegen und zu **aktualisieren**.

---

[10] Die europäischen Vorschläge sehen zwar eine vergleichbare Formulierung vor („having regard to the state of the art“), wegen der in Art. 2 NIS-RL-E explizit vorgesehenen Beschränkung auf eine Mindestharmonisierung besteht insoweit jedoch ein Spielraum für den deutschen Gesetzgeber.

[11] Z.B. *Eckardt*, ZD 2014, 599, 600 f.

- Die Einbeziehung der zuständigen Aufsichtsbehörden nach § 8a Abs. 2 Satz 3 Nr. 2 BSIG-E kann in bestimmten Fällen relativ komplex werden. Insbesondere muss die Vorschrift so verstanden werden, dass die **Datenschutz-Aufsichtsbehörden** zu beteiligen sind, soweit (wie regelmäßig) es zumindest auch um die Verarbeitung personenbezogener Daten geht.

4.2 Nachweis der Einhaltung

Nach § 8a Abs. 3 BSIG-E ist die Erfüllung alle zwei Jahre nachzuweisen. Mittel hierzu sind **Sicherheitsaudits, Prüfungen oder Zertifizierungen**. Von diesen drei Begriffen wird lediglich die Zertifizierung in § 2 Abs. 7 BSIG definiert.

Welcher Art die drei Prozesse sein sollen, wird auch in der Begründung nicht wirklich aussagekräftig beschrieben. Insgesamt **fehlen deshalb detaillierte Aussagen** zu den durchführenden Stellen (einschließlich ihrer Qualifikation und einer etwaigen Akkreditierung), Verfahrensanforderungen, materiellen Standards (etwa die wichtige Frage von Prüfungen vor Ort oder von aussagekräftigen Angriffstests) und Rechtsfolgen. Der Entwurf der Europäischen Kommission für eine Datenschutz-Grundverordnung ist genau für eine solche Nichtregelung erheblich kritisiert worden; es zeichnet sich ab, dass dies im laufenden Verfahren nachgebessert wird.

Diese Punkte sollten entweder im Gesetz oder **zumindest in der Verordnung** geregelt werden; im zweiten Fall wäre **§ 10 BSIG-E entsprechend zu ergänzen**. Insbesondere sollte sichergestellt werden, dass **tatsächlich effektive Tests durchgeführt** werden und nicht lediglich auf Hersteller- oder Betreibererklärungen vertraut wird.

4.3 Fehlen von Sanktionen

Art. 17 NIS-RL-E enthält die **Verpflichtung der Mitgliedsstaaten**, Sanktionen für die Verletzung der in Art. 14 und Art. 15 NIS-RL-E genannten Pflichten einzuführen. Dies bezieht sich auch auf die Implementierung angemessener technische und organisatorische Maßnahmen. Eine solche allgemeine Sanktionsregelung **fehlt im Gesetzentwurf**. Im Falle der Verabschiedung der Richtlinie wäre deshalb eine Ergänzung des vorliegenden Gesetzes erforderlich. Der Gesetzgeber **sollte dies jedoch nicht abwarten**, sondern die Anbieter Kritischer Infrastrukturen insoweit **in die Pflicht nehmen**. Hierzu bietet sich die Einführung entsprechender Bußgeldtatbestände an.

Unabhängig davon enthält der vorliegende Gesetzentwurf in Bezug auf die Sanktionen eine **Ungleichbehandlung, deren Grund nicht ersichtlich ist**. Von allen im Entwurf adressierten Anbietern machen sich ausschließlich die Anbieter nach dem Telemediengesetz (§ 16 Abs. 2 Nr. 2 TMG-E; diese werden regelmäßig noch nicht einmal Kritische Infra-

strukturen betreiben) und Telekommunikationsgesetz (§ 149 Nr. 21a TKG-E) bußgeldpflichtig, wenn sie Sicherheitsmechanismen einsetzen, die nicht dem Stand der Technik entsprechen. Diese Ungleichbehandlung wird auch in der Begründung nicht erklärt. Es ist überdies nicht ersichtlich, wie sie gerechtfertigt werden könnte. Sie sollte zugunsten einer gleichmäßigen Regelung von Ordnungswidrigkeitentatbeständen **für alle Verpflichteten** bereinigt werden.

4.4 Haftungsfragen

Das Gesetz adressiert die wichtige Frage einer zivilrechtlichen Haftung für eine Verletzung der Pflichten aus § 8a BSIG-E nicht. Dies bedeutet allerdings nicht, dass die Anbieter von Kritischen Infrastrukturen nicht auch insoweit durch das Gesetz betroffen wären. Hierzu gibt es **mehrere Ansatzpunkte**:

- Da das Gesetz spezifische Verhaltenspflichten für die Anbieter regelt, werden sich mutmaßlich **Auswirkungen auf allgemeine Fahrlässigkeitsmaßstäbe** ergeben, die sowohl im Rahmen von Verträgen der Anbieter mit ihren Endkunden als auch für allgemeine Haftungsnormen wie § 823 Abs. 1 BGB eine Rolle spielen können. Soweit diese Haftungsfragen durch AGB geregelt werden, könnten die neuen technischen Pflichten eine **Auswirkung auf die gerichtliche AGB-Kontrolle** haben und dazu führen, dass sich die Anbieter insoweit nicht von der Haftung befreien können.
- Demgegenüber dürfte das weitgehende Fehlen einer Bezugnahme auf Dritte, die ebenfalls ein Interesse an den gemeldeten Informationen haben können, dazu führen, dass (anders als etwa bei § 42a BDSG, § 15a TMG, § 109a TKG, § 83a SGB X)[12] die **Meldepflichten keine Schutzgesetze im Sinne von § 823 Abs. 2 Satz 1 BGB** sein dürften. Dies wird aus europarechtlicher Sicht künftig vermutlich sogar vorgegeben werden weil in Art. 14 Abs. 2 NIS-RL-E eine Bestimmung vorgesehen ist, wonach die Meldungen die Anbieter nicht dem Risiko einer verschärften Haftung aussetzen dürfen.
- Für **TK-Anbieter** könnten die neuen Pflichten allerdings im Rahmen der allgemeinen **Haftungsregeln nach §§ 44, 44a TKG** relevant werden. Dies dürfte insbesondere bei der spezifisch auf den Kunden gerichteten neuen Informationspflicht nach § 109a Abs. 4 TKG der Fall sein.

Unklar ist demgegenüber, ob sich auch **Auswirkungen auf die Haftung von Verbraucherinnen und Verbraucher** ergeben. Einen Ansatzpunkt hierfür könnte ebenfalls § 109

[12] S. *Hornung*, in: Roßnagel, Recht der Telemediendienste, 2013, § 15a TMG Rn. 51 m.w.N.

Abs. 4 TKG-E darstellen, wenn nach einer Information durch den TK-Anbieter das Sicherheitsproblem eines privaten Computers nicht behoben wird. Ob sich durch diese Information im Zusammenspiel mit anderen allgemeinen Regeln eine Verkehrssicherungspflicht der Privatnutzer ergibt, ist allerdings völlig offen.

Schließlich kann sich aus allgemeinen Regeln **auch eine Haftung des Bundes für das Handeln des BSI** ergeben. Zumindest gegenüber den Betreibern Kritischer Infrastrukturen wird für die Pflicht in § 8b Abs. 2 Nr. 4 BSIG-E **wohl eine drittgerichtete Amtspflicht zu bejahen** sein, sodass eine Haftung nach § 839 BGB i.V.m. Art. 34 GG möglich ist.

5 Meldepflichten für IT-Sicherheitsvorfälle

Die in § 8b BSIG-E und den weiteren Regelungen vorgesehenen Meldepflichten sind ein **grundsätzlich sinnvolles Instrument**, an einer zentralen Stelle einen umfassenden Überblick über den Stand der IT-Sicherheit in Deutschland zu gewinnen. Für die Umsetzung ergibt sich an einigen Stellen noch ein **Bedarf nach Konkretisierung**, der im Rahmen der **Rechtsverordnung** nach § 10 Abs. 1 BSIG-E erfolgen kann. Dies betrifft insbesondere die Frage, was eine „erhebliche" Störung und eine „Beeinträchtigung" nach § 8a Abs. 4 BSIG-E ist.[13]

5.1 Spezielle Meldepflichten

§ 8c Abs. 3 BSIG-E nimmt TK-Anbieter, Betreiber von Energieversorgungsnetzen und Energieanlagen, Inhaber atomrechtlicher Genehmigungen sowie Betreiber Kritischer Infrastrukturen mit vergleichbaren Vorgaben von den Meldepflichten aus. Für diese gelten **separate Regelungen**, die jedoch **teilweise unzureichend** mit den Bestimmungen im BSIG-E **abgestimmt** erscheinen.

Auf der Ebene des **Anlasses der Meldung** offenbaren sich erhebliche **terminologische Abweichungen**. Während nach § 8b Abs. 4 BSIG-E Betreiber „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse" zu melden haben, „die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben" werden von § 109 Abs. 5 TKG-E „Beeinträchtigungen" von Telekommunikationsnetzen und -diensten erfasst, „die zu beträchtlichen Sicherheitsverletzungen führen oder führen können". Ob mit dieser unterschiedlichen Wortwahl auch unterschiedliche Anforderungen gemeint sind, **wird nicht deutlich**. In der Diskussion ist der Begriff der „Beeinträchtigung" teilweise als umfassender

[13] Z.B. *Bräutigam/Wilmer*, ZRP 2015, 38, 40 f.

aufgefasst worden. Der Begriff der „Sicherheitsverletzung“ ist im TKG an keiner Stelle definiert. Lediglich mittelbar folgt aus § 109 Abs. 5 Satz 1 TKG, dass – unter anderem – „Störungen von Telekommunikationsnetzen oder -diensten" gemeint sind.

Nach § 44b AtomG-E sind „Beeinträchtigungen“ der informationstechnischen Systeme, Komponenten oder Prozesse zu melden, „die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben“. Die begriffliche Struktur ist also ähnlich wie in § 109 Abs. 5 TKG-E, aber erneut anders als in § 8b Abs. 4 BSIG-E. **Besonders auffällig ist**, dass in § 44b AtomG-E offenbar Beeinträchtigungen zu Störungen führen, während in § 8b Abs. 4 BSIG-E genau umgekehrt Störungen Beeinträchtigungen zur Folge haben.

Wieso für die durch § 8c Abs. 3 BSIG-E ausgenommenen Anbieter **die pseudonyme Meldung nicht eröffnet wird, ist nicht recht ersichtlich**. Für den Bereich des Atomrechts mag dies keine Rolle spielen, weil es dort ohnehin nur um wenige Anbieter geht. Für den Bereich des TKG gegen sollte das abgestufte Verfahren des § 8b Abs. 4 BSIG-E entsprechend Anwendung finden. Soweit dies in § 11 Abs. 1c Satz 3 EnWG-E vorgesehen ist, bedarf der Gesetzentwurf eine Ergänzung, weil dort gar keine gemeinsame übergeordnete Ansprechstelle vorgesehen ist, sodass diese Option nach aktuellem Stand nicht wirksam werden kann.

5.2 Datenschutz- und Vertraulichkeitsaspekte

Meldungen über IT-Sicherheitsvorfälle können sensible Informationen umfassen. Dies betrifft vor allem **personenbezogene Daten**, die in Kritischen Infrastrukturen anfallen und von den Betreibern erhoben und verwendet werden. Diese Daten können in drei Fällen betroffen sein:

- Soweit der IT-Sicherheitsvorfall direkt personenbezogene Daten betrifft, können auch die **Meldepflichten nach § 42a BDSG, § 15a TMG, § 109a TKG und § 83a SGB X** einschlägig sein. Insoweit erscheint eine gegenseitige Information oder Zusammenarbeit der Behörden sinnvoll.
- Wichtiger für den Gesetzentwurf ist, dass es je nach Art des Vorfalls erforderlich sein kann, **solche Daten im Rahmen der Meldepflicht an das BSI** zu übermitteln. Hierfür enthält § 8b BSIG-E **keine explizite Ermächtigungsgrundlage**. Lediglich mittelbar lässt sich aus der – zu begrüßenden – Zweckbindung in § 8b Abs. 6 BSIG-E entnehmen, dass der Gesetzgeber davon ausgeht, die Meldungen könnten auch personenbezogene Daten enthalten. Dies sollte im Sinne von Rechtsklarheit und Transparenz **präzisiert werden**. Da die Tätigkeit des BSI im Rahmen von § 8b BSIG-E nicht unter § 14 Abs. 2 und § 15 Abs. 5 Satz 3 TMG fällt, besteht wegen

der Regelung in § 12 Abs. 1 TMG nach dem derzeitigen Gesetzentwurf insbesondere keine Befugnis zur Übermittlung von Bestands und Nutzungsdaten nach dem TMG.

- Denkbar erscheint, dass im Rahmen der Möglichkeiten und Pflichten des BSI zur **Information der Betreiber Kritischer Infrastrukturen und Dritter** ebenfalls personenbezogene Daten übermittelt oder öffentlich gemacht werden. Dies wird jedoch **durch § 8b Abs. 6 BSIG ausgeschlossen**, der sich explizit nur auf die vorstehenden Absätze der Norm bezieht. Insoweit besteht also kein Risiko für die Betroffenen.

Neben den personenbezogenen Daten natürlicher Personen können die Meldungen über IT-Sicherheitsvorfälle auch die **Interessen der betroffenen Unternehmen** beeinträchtigen, wenn entweder Betriebs- und Geschäftsgeheimnisse betroffen sind oder ihre Reputation gefährdet wird. Dem zweiten Problem wird durch das abgestufte Meldesystem in § 8b Abs. 4 BSIG-E Rechnung getragen. Wenn es tatsächlich zu einer Störung kommt, so ist die Offenlegung des konkreten Betreibers gegenüber dem BSI wegen des übergeordneten Interesses gerechtfertigt.

Nicht übersehen werden darf, dass das **BSI nicht nur ein allgemeines Lagebild** zu IT-Sicherheit in Deutschland, sondern auch sehr **konkrete Informationen** über die Anfälligkeit bestimmter Branchen in Deutschland und sogar insoweit bestehenden Probleme einzelner Unternehmen erhalten wird. Dieser Informationen sind hochgradig sensibel, weil sie etwa im Rahmen von Industriespionage verwendet werden können. Es ist deshalb **sicherzustellen, dass das BSI im Rahmen seiner Zusammenarbeit** mit anderen Behörden – insbesondere solcher **Behörden anderer Staaten**, für die eine explizite Aufgabe in § 3 Abs. 1 Satz 2 Nr. 16 BSIG-E vorgesehen ist – **keine derartigen Informationen weitergibt**. Es ist nicht recht einsichtig, wieso der Gesetzentwurf **eine explizite Pflicht insoweit nur nach § 11 Abs. 1c Satz 5 EnWG-E** vorsieht, wonach das BSI und die Bundesnetzagentur sicherzustellen haben, „dass die unbefugte Offenbarung, der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird.“ Eine solche Pflicht sollte für die nach den übrigen Meldepflichten übermittelten Angaben ebenfalls aufgenommen werden.

5.3 Informations- und Veröffentlichungspflichten des BSI

Der Gesetzentwurf wird nach der weiteren Präzisierung in der Rechtsverordnung sehr präzise regeln, welche Informationspflichten die Betreiber Kritischer Infrastrukturen haben. Demgegenüber ist der weitere **Umgang des BSI mit den erlangten Informationen** weniger durchreguliert und in Bezug auf die Information anderer Stellen nur **fragmentarisch** ausgestaltet.

Der Entwurf betont, dass der **verstärkte Schutz der Bürgerinnen und Bürger im Internet** ein wesentliches Ziel ist. Nach dem aktuellen Stand wird dieses Ziel jedoch **nur mittelbar** bewirkt, nämlich über die Verbesserung der IT-Sicherheit in den Kritischen Infrastrukturen; eine Einbindung der Bürgerinnen und Bürger selbst ist nicht vorgesehen. Auch die Gesetzesbegründung z.B. zu § 3 Abs. 1 Satz 2 Nr. 2 des Entwurfs nennt für „Dritte", die auf Antrag informiert werden können, nur Einrichtungen und Unternehmen.[14] Insgesamt sollten die Pflichten und Befugnisse des BSI zur Information Dritter und der Öffentlichkeit **erweitert werden**; dies kann jedoch nur unter Berücksichtigung der legitimen Interessen der Betreiber und der Risiken für die IT-Sicherheit erfolgen.

5.3.1 Interessen der Betreiber und übergeordneter Geheimhaltungsinteressen

Gegen eine Weitergabe der durch die Meldungen erlangten Informationen an Dritte oder die Öffentlichkeit lassen sich die Interessen der Betreiber und das Risiko einer Ausnutzung der auf diesem Wege möglicherweise offenbarten IT-Sicherheitslücken anführen.

Der **Reputationsverlust der Unternehmen** ist insoweit durchaus eine realistische Gefahr. Dieses Interesse ist aber gegen die Interessen derjenigen abzuwägen, die von einer Meldung profitieren würden (weil sie etwa konkrete Abwehrmaßnahmen ergreifen, ihre allgemeinen IT-Sicherheitsbestrebungen präzisieren oder auch Forschung- und Entwicklungsanstrengungen konkreter durchführen können). Auf diesem Wege profitiert auch die Gesellschaft insgesamt davon, dass das Wissen über die Risiken für die IT-Sicherheit nicht nur im Geheimen verbleibt. Hinsichtlich eines drohenden Reputationsverlustes sind **mehrere Fälle zu unterscheiden**. Für die Störung nicht zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit, ist ein solcher nicht zu besorgen; die erfolgreiche Abwehr einer solchen Bedrohung wird die Reputation umgekehrt sogar steigern. Kommt es dagegen zu einem Ausfall oder einer Beeinträchtigung, so kann es in der vorzunehmenden Abwägung zulasten der meldenden Unternehmen sprechen, wenn sie ein vorwerfbares Verhalten trifft; hier dürfte das Risiko einer Veröffentlichung zusätzlich dazu anhalten, IT-Sicherheitsstandards einzuhalten. Im Bereich der nach § 8b Abs. 4 BSIG-E vorgesehenen pseudonymen Meldung besteht (solange auch aus den Umständen nicht auf den betreiberzurückgeschlossen werden kann) von vornherein kein Risiko eines Reputationsverlusts, sodass dieses Argument hier überhaupt nicht greift.

Eine Information der Öffentlichkeit kann auch dann gefährlich sein, **wenn das zugrundeliegende IT-Sicherheitsproblem noch nicht gelöst ist**, die Lücke deshalb weiterhin „offen" ist und deshalb das Risiko besteht, dass Nachahmungstäter erst auf sie aufmerksam

---

[14] BT-Drs. 18/4096, 24.

gemacht werden. In diesen Fällen ist es sinnvoll, **zunächst in Zusammenarbeit mit Herstellern und Anwendern Lösungen zu erarbeiten**. Für eine komplette Geheimhaltung kann aus dieser Notwendigkeit jedoch kein Argument abgeleitet werden. Zum einen wird es für Wissenschaftler und Anbieter vielfach sinnvoll sein, nach dem Schließen einer Lücke von deren Charakteristika zu erfahren, um Erkenntnisse für die Zukunft zu gewinnen. Überdies ist eine Veröffentlichung geboten, wenn Selbsthilfemaßnahmen der institutionellen oder privaten Anwender erforderlich sind. Dass der **zugrundeliegende Konflikt lösbar ist**, zeigt § 42a Satz 2 BDSG. Danach muss im Falle einer unrechtmäßigen Kenntniserlangung von personenbezogenen Daten die Benachrichtigung des Betroffenen „unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird“. Eine solche vorläufige Zurückhaltung der Informationen ist auch im hier vorliegenden Fall möglich.

Soweit im weiteren Gesetzgebungsverfahren entsprechend den Vorschlägen unter 4.3 und 5.4 weitere Sanktionen aufgenommen werden, könnte sich überdies ein **Konflikt mit dem Verbot der Selbstbezichtigung** ergeben. Deshalb sollte erwogen werden, zum Schutz der meldepflichtigen eine § 42a Satz 6 BDSG[15] entsprechende Beschränkung der Verwendung der erlangten Informationen in einem Straf- und Ordnungswidrigkeitenverfahren aufzunehmen.

5.3.2 Schlussfolgerungen

Unter Berücksichtigung dieser Überlegungen erscheinen die **Kommunikationswege zu den Betreibern Kritischer Infrastrukturen** im Wesentlichen **hinreichend**. § 3 Abs. 3 BSIG-E eröffnet dem BSI insoweit die ermessensabhängige Möglichkeit der Beratung bei der Sicherung der Informationstechnik; nach allgemeinen Regeln kann sich dieses Ermessen auf Null reduzieren, wenn beispielsweise ein Betreiber auf die rasche Unterstützung gerade des BSI angewiesen ist. In Umsetzung der neuen Aufgabe zur Zurverfügungstellung von Informationen nach § 3 Abs. 1 Satz 2 Nr. 2 BSIG-E auch an Dritte regelt § 8b Abs. 2 Nr. 4 lit. a BSIG-E eine Pflicht der Behörde zur Information der Betreiber Kritischer Infrastrukturen über sie betreffende Informationen, die aus den mittels der Meldepflicht gesammelten Daten synthetisiert werden.

---

[15] Danach darf eine Benachrichtigung über eine unrechtmäßige Kenntniserlangung personenbezogener Daten, die der Benachrichtigungspflichtige erteilt hat, in einem Strafverfahren oder in einem Verfahren nach dem OWiG gegen ihn oder einen in § 52 Abs. 1 StPO bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

In **Bezug auf konkrete Dritte** ist eine solche **proaktive Informationspflicht** des BSI dagegen nicht nur nicht als Pflicht, sondern **noch nicht einmal als Möglichkeit** ausgestaltet worden. § 8d BSIG-E lässt eine Information Dritter nur auf Antrag zu und stellt sie in das Ermessen der Behörde. Als ermessenslenkende Maßstäbe werden ausschließlich Gründe für den Ausschluss der Auskunft genannt, sodass die Regelung insgesamt restriktiv ausgestaltet ist. Dies ist eine übermäßige Einschränkung der legitimen Interessen Dritter an den durch das BSI gesammelten Informationen. Umgekehrt ist nicht erkennbar, wieso der konkrete Betreiber nicht an der Entscheidung beteiligt oder zumindest informiert werden soll. Die Vorschrift sollte deshalb **in dreifacher Hinsicht geändert** werden:

- Statt die Übermittlung der Informationen per se auszuschließen, wenn schutzwürdige Interessen des Betroffenenbetreibers entgegenstehen, ist **eine Abwägung** zwischen diesen legitimen Interessen und den gleichfalls legitimen Interessen des Dritten vorzunehmen. Andernfalls käme es auch zu einer übermäßigen Einschränkung gegenüber den Regelungen im IFG.
- Soweit das BSI erkennen kann, dass ein berechtigtes Interesse Dritter an den Informationen besteht, um sich vor erheblichen Gefahren der IT-Sicherheit zu schützen, sollte die Behörde eine **proaktive Pflicht treffen, selbst in den entsprechenden Abwägungsprozesse einzutreten**. Andernfalls besteht die Gefahr, dass die dritten keine Kenntnis davon erhalten, dass das BSI über entsprechende Informationen verfügt, und dementsprechend keinerlei Anlass haben, ein Auskunftsverlangen zu stellen.
- Entsprechend den europäischen Entwürfen (§ 14 Abs. 4 NIS-RL-E) sollte eine **Pflicht zur Anhörung des betroffenen Betreibers** vorgesehen werden.

Auch hinsichtlich einer **Pflicht zur Information der Öffentlichkeit** erscheint der Entwurf **überarbeitungsbedürftig**. In der Begründung zu § 8b BSIG-E heißt es zwar, die Öffentlichkeit werde benachrichtigt, wenn das öffentliche Interesse dies erfordere; auch insoweit dürften schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen nicht entgegenstehen.[16] **Auf welcher Basis** diese Information der Öffentlichkeit erfolgen soll, wird jedoch nicht angegeben und ist auch **nicht erkennbar**. § 8b BSIG-E enthält jedenfalls weder eine Befugnis, geschweige denn eine Pflicht zu einer solchen Benachrichtigung. Auch das als Antragsverfahren eines konkreten Dritten ausgestaltete Procedere nach § 8d BSIG-E kann kaum gemeint sein. Somit bleibt lediglich die allgemeine Befugnis zur Warnung der Öffentlichkeit nach § 7 BSIG. Diese bezieht sich jedoch explizit auf die Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nr. 14 BSIG, also gerade nicht auf die neuen Aufgaben nach Nr.

[16] BT-Drs. 18/4096, 27.

17. Regelungssystematisch besteht insoweit also **überhaupt keine Befugnis zur Information der Öffentlichkeit** über die aus den Meldepflichten gewonnenen Informationen.

Dies widerspricht nicht nur den europäischen Plänen (Art. 14 Abs. 4 NIS-RL-E) und stellt eine **nicht begründete Diskrepanz zu der Bestimmung in § 109 Abs. 5 Satz 7 TKG-E** dar,[17] sondern ist auch aus nationaler Sicht eine Lücke, die geschlossen werden sollte. Soweit eine Information der Öffentlichkeit geboten ist, um Sicherheitsvorfälle abzuwenden oder zu lindern, sollte – unter Abwägung mit den legitimen Vertraulichkeitsinteressen der betroffenen Anbieter[18] – eine solche **Pflicht oder zumindest Befugnis des BSI zur Information der Öffentlichkeit** eingeführt werden.

5.4 Fehlen von Sanktionen

Auffällig ist, dass der Gesetzentwurf **ausschließlich für den Bereich des TKG** Sanktionen für Verstöße gegen die geregelten Meldepflichten enthält.[19] Gemäß § 149 Nr. 21a TKG-E begeht eine Ordnungswidrigkeit, wer eine Beeinträchtigung von Telekommunikationsnetzen oder -diensten, die zu einer „beträchtlichen Sicherheitsverletzung“ führt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitteilt. Wieso der Gesetzgeber ausschließlich für diese Anbieter die Notwendigkeit einer entsprechenden Bußgeldbewehrung gesehen hat, wird nicht erläutert. Die Ungleichbehandlung ist nicht nur **verfassungsrechtlich kaum zu rechtfertigen**, sondern auch **sachlich unangemessen**. Ohne eine entsprechende Norm müsste das BSI vollständig darauf vertrauen, dass die Betreiber Kritischer Infrastrukturen ihrer Pflicht aus § 8b Abs. 4 BSIG-E freiwillig nachkommen.

Dementsprechend sollte ein entsprechender Tatbestand aufgenommen werden. Dies entspricht im Übrigen **auch dem geplanten Art. 17 NIS-RL-E**, der nicht nur Sanktionen für die Verletzung von IT-Sicherheitsstandards, sondern auch für die Nichterfüllung der Meldepflichten vorgibt.

6 Verfassungsrechtliche Probleme von § 100 Abs. 1 TKG-E

§ 100 Abs. 1 TKG enthält **bereits heute** die Befugnis der Diensteanbieter, die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen erforderlich ist. Dies entspricht § 100 Abs. 1 Satz 1 TKG-E. Demgegenüber ist **§ 100 Abs. 1 Satz 2 TKG-E** vom Wortlaut her **eine Erweiterung**, weil der Begriff

---

[17] Danach kann die Bundesnetzagentur die Öffentlichkeit unterrichten oder die Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt.

[18] S.o. 5.3.1.

[19] Kritisch z.B. *Bräutigam/Wilmer*, ZRP 2015, 38, 41.

der Störungen auf solche Fälle erstreckt wird, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer „führen können“.

Die Erstreckung auf lediglich potentielle Einschränkungen der Verfügbarkeit **entspricht der Auslegung des Bundesgerichtshofs** zum geltenden § 100 Abs. 1 TKG.[20] Neu ist demgegenüber die Erstreckung auf Systeme der Nutzer (hierbei wird es sich regelmäßig nicht um Kritische Infrastrukturen handeln). Hiermit hatte sich die Rechtsprechung bislang noch nicht zu beschäftigen.

Mit Blick auf den Eingriff in das Fernmeldegeheimnis nach Art. 10 GG, der in der Vorschrift liegt, begegnet § 100 Abs. 1 TKG-E verfassungsrechtlichen Bedenken.[21] Da der Entwurf ebenso wie die geltende Vorschrift als einziges Kriterium für die Erhebung und Verwendung der Daten die Erforderlichkeit nennt, enthält er de facto **keinerlei präzise Regelungen**. Dies ist mit Blick darauf, dass die Norm potenziell eine **umfassende Analyse der Verkehrsdaten aller Teilnehmer und Nutzer in Deutschland** ermöglicht, nicht zu rechtfertigen. Zwar gelten insoweit die durch das Bundesverfassungsgericht und den europäischen Gerichtshof aufgestellten Anforderungen an die Vorratsspeicherung von Telekommunikations-Verkehrsdaten[22] nicht direkt. Die durch die Gerichte beschriebenen Risiken für die unbeobachtete Kommunikation der Bürgerinnen und Bürger sind jedoch auch hier betroffen.

Die in der Diskussion mitunter vorgeschlagene Alternative des **Verzichts auf eine präventive Datenerhebung** und der Beschränkung auf die Erhebung und Verwendung der Daten im Falle eines Sicherheitsvorfalls ist sicher weniger eingriffsintensiv. Inwieweit hierdurch wesentliche Sicherheitsrisiken nicht identifiziert werden könnten, **müssen die technischen Sachverständigen bewerten**.

Wenn es bei dem vorgeschlagenen Verwendungszweck für die nach § 100 Abs. 1 TKG-E erhobenen Daten bleibt, so sind jedenfalls **ergänzende Regelungen zur Sicherung der Persönlichkeitsrechte der Betroffenen** vorzusehen. Dies betrifft insbesondere Erheblichkeitsschwellen (der Entwurf erfasst sämtliche, das heißt auch einfach gelagerte Störungen und Fehler), Maßnahmen zum Schutz gegen Zweckentfremdung, Dokumentationspflichten, Ausnahmen für besonders sensible Kommunikationsvorgänge, Vorgaben zur Information der Betroffenen und zeitlich konkretisierte **Löschpflichten**. Letzteres betrifft insbesondere Daten, die keinen Anlass für einen entsprechenden Verdacht auf Störungen

---

[20] BGH, NJW 2014, 2500; NJW 2011, 1509.
[21] Diese gelten der Sache nach auch für die aktuelle Regelung.
[22] BVerfGE 125, 260; EuGH, NJW 2014, 2169.

oder Fehler ergeben haben.[23] Dass entsprechende Vorgaben zur Zweckbindung, Transparenz und Löschung möglich sind, zeigt die Regelung in § 5 BSIG.

Durch die **Streichung von § 15 Abs. 9 TMG-E** (Referentenentwurf) bleibt es weiterhin bei der grundsätzlichen Unzulässigkeit der Erhebung und Verwendung von Nutzungsdaten durch Webseitenbetreiber zur Störungserkennung. Auf die **damit verbundenen Probleme und Lösungsmöglichkeiten** haben u.a. der FIfF e.V.[24] und das ULD[25] hingewiesen; dies soll deshalb hier nicht vertieft werde.

[23] Das Kriterium der Erforderlichkeit im geltenden § 100 Abs. 1 TKG hat zu einer erheblichen Rechtsunsicherheit hinsichtlich der Frage geführt, wie lange die insoweit erhobenen Daten gespeichert werden dürfen. Die inzwischen erfolgte höchstrichterliche Klärung dieser Frage (BGH, NJW 2014, 2500; NJW 2011, 1509) gilt im Wesentlichen nur für IP-Adressen, für die eine Speicherung von sieben Tagen akzeptiert wurde.

[24] FIfF e.V., Stellungnahme zum IT-Sicherheitsgesetz der Bundesregierung vom 17.12.2014, 4 ff.

[25] Stellungnahme vom 13.2.2015, https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html.