4. Kapitel: Übertragung in das IT-Sicherheitsrecht

In diesem Teil wird die IT-Sicherheit nach dem RegE BSIG beleuchtet und untersucht, ob der Begriff der „Resilienz" auch hierin übertragen werden könnte.

Dabei beschränkt sich der Untersuchungsgegenstand auf die Anforderungen an die hier gegenständlichen, personalisierten digitalen Dienste nach § 30 i.V.m. § 28 Abs. 2 Nr. 3 i.V.m. Anlage 2, Ziff. 6 RegE BSIG. Im BSIG und der NIS-RL sind digitale Dienste (§ 8c BSIG und Art. 16 NIS-RL) und kritische Infrastrukturen (§ 8a BSIG und Art. 14 NIS-RL) bislang noch in separaten Pflichtennormen adressiert, wobei die Regulierung der kritischen Infrastrukturen als Vorbild und Grundlage für die Regulierung der digitalen Dienste verstanden werden kann. Insbesondere im Rahmen der Bestimmung der Schutzgüter wird daher auch in dieser Arbeit noch einmal auf die kritischen Infrastrukturen (künftig Betreiber kritischer Anlagen, § 28 Abs 6 Nr. 4 RegE BSIG) zurückzukommen sein.

Mit § 30 RegE BSIG besteht dann unter der künftigen Rechtslage eine gemeinsame Pflichtennorm.[638] Die für die Resilienz maßgeblichen IT-Sicherheitspflichten, denen digitale Dienste unterliegen finden sich folglich v.a. in § 30 Abs. 1, 2 RegE BSIG.[639]

Parallel zur Untersuchung in der DSGVO (Kapitel 3., Abschnitt B.) sollen zunächst die Schutzgüter bestimmt werden, die durch diese IT-Sicherheitspflichten gesichert werden (A.). In einem weiteren Schritt (B.) werden sodann die gesetzlichen Sicherheitsvorgaben an digitale Dienste näher untersucht, wobei insbesondere die Begriffe „Risiko" und „Sicherheit", die Schutzobjekte Netz- und Informationssysteme, Dienste und Daten sowie die Schutzziele betrachtet werden. Anschließend werden die so aufbereiteten Vorgaben mit jenen der DSGVO gegenübergestellt (C.), um mögliche

638 Die bisherige Unterteilung zwischen kritischen Infrastrukturen und digitalen Diensten hat sich nach dem europäischen Gesetzgeber „als überholt erwiesen […], da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt" widerspiegle, EG 6 S. 2 NIS2-RL. Für Betreiber kritischer Anlagen gelten zusätzlich die Anforderungen des § 31 RegE BSIG.

639 Weiterhin erlässt die EU-Kommission nach § 30 Abs. 3 RegE BSIG, Art. 21 Abs. 5 UAbs. 1 NIS2-RL bis zum 17.10.2024 einen konkretisierenden Durchführungsrechtsakt für die digitalen Dienste.

Unterschiede zu identifizieren, die einer Übertragung des Resilienzbegriffs aus der DSGVO in den RegE BSIG entgegenstehen könnten. Auf Basis dessen wird schließlich die Möglichkeit der Implementierung der Resilienz in den RegE BSIG geprüft (D.). Am Ende dieses Kapitels wird schließlich unter E. geprüft, ob die Resilienz auch nach dem RegE BSIG als IT-Sicherheitsanforderung für die digitalen Dienste eine rechtspraktische Funktion erfüllen kann und mit Blick auf die plurale Informationsmanipulation ggf. auch etwas andere Maßnahmen als in der DSGVO erfordert.

A. Bestimmung der Schutzgüter

Im Nachfolgenden sollen die Schutzgüter des § 30 RegE BSIG für digitale Dienste herausgearbeitet werden. Als Schutzgüter werden analog zur Untersuchung in der DSGVO[640] die jeweiligen Rechtsgüter bezeichnet, die durch die Anforderungen an die IT-Sicherheit gesichert werden sollen.

Anders als in der DSGVO gestaltet sich die Bestimmung der Schutzgüter im RegE BSIG jedoch deutlich komplexer. Das RegE BSIG dient wie gezeigt werden wird mit seinen Vorgaben zur IT-Sicherheit nicht nur dem Schutz von Individual-, sondern insbesondere auch von Gemeinschaftsrechtsgütern,[641] an denen sich die Schadfolgen von IT-Sicherheitsvorfällen realisieren können.

Um die Schutzgüter im Einzelnen zu bestimmen, wird zunächst die historische Entwicklung des (RegE) BSIG nachgezeichnet und dabei bereits erste Anhaltspunkte für die Bestimmung der Schutzgüter herausgearbeitet (I.). Im Anschluss folgt die Bestimmung der Schutzgüter für die tradierten kritischen Anlagen, wobei insbesondere auf die Begriffe der *Daseinsvorsorge* sowie der *öffentlichen Sicherheit* eingegangen wird (II.). Abschließend folgt eine spezifizierende Bestimmung der Schutzgüter für die digitalen Dienste (III.).

I. Historische Entwicklung des BSIG

Das BSIG wurde ursprünglich 1991 als reines Aufgabenzuweisungsgesetz geschaffen, in welchem dem Bundesamt für Sicherheit in der Informati-

640 S. 105 ff.
641 Zu diesem Begriff siehe: S. 249.

onstechnik (BSI) nach § 3 des BSIG insbesondere die Untersuchung von Sicherheitsrisiken, die Entwicklung von Sicherheitsvorkehrungen sowie Verfahren zur Messung von Sicherheit ebenso wie Produktprüfung und -zulassung zugewiesen wurde. Diese Aufgaben dienten primär der Absicherung der IT-Infrastruktur des Bundes, allerdings war auch damals bereits die Unterstützung des Datenschutzbeauftragten (§ 3 Abs. 1 Nr. 5 BSIG a.F.) sowie die Beratung von IT-Produkt-Herstellern (§ 3 Abs. 1 Nr. 7 BSIG a.F.) vorgesehen.

Einen ersten Impuls im Sinne des heutigen IT-Sicherheitsrechts setzte der nationale Plan zum Schutz kritischer Infrastrukturen 2005. Hier wurden insbesondere auch die kritischen Infrastrukturen definiert als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten."[642]

Die erste Änderung des BSIG 2009 brachte zwar noch keine tiefgreifenden materiellen Änderungen; dem BSI wurden lediglich mehr eigene Befugnisse eingeräumt, insbesondere auch ohne Amtshilfeersuchen von anderen Behörden bei diesen zur Erhöhung der IT-Sicherheit und zur Abwehr von Gefahren tätig zu werden.[643] Allerdings wurde aus der Gesetzesbegründung bereits deutlich, dass der Gesetzgeber die gesteigerte Bedeutung der Informations- und Kommunikationstechnologie (IKT) erkannte. Diese sei „mittlerweile Voraussetzung für das Funktionieren des Gemeinwesens".[644] Und bei Ausfällen könnte etwa die Versorgung mit Energie oder Wasser gefährdet sein, entsprechende Angriffe auf die IKT könnten somit sogar unmittelbare Auswirkungen auf Leben und Gesundheit vieler Menschen haben. Außerdem bedrohe auch die Gefahr von (digitalen) Spionageaktivitäten in Wirtschaft und Forschung den Wohlstand und die innere Sicherheit Deutschlands.[645]

642 BMI, Nationaler Plan zum Schutz der Informationsinfrastrukturen, Juli 2005, S. 21; ebenso später: BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, S. 3.
643 BR-Drs. 62/09, S. 11.
644 BR-Drs. 62/09, S. 1.
645 BT-Drs. 62/09, S. 1.

1. Novelle 2015 – Schutz kritischer Infrastrukturen

Materielle Anforderungen an die IT-Sicherheit von kritischen Infrastrukturen wurden mit dem IT-Sicherheitsgesetz vom 25.07.2015 in das BSIG aufgenommen.[646]

Betreiber kritischer Infrastrukturen wurden gemäß § 8a BSIG 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."

Was eine kritische Infrastruktur ist, wird mittels einer *mehrstufigen Methodik* festgelegt: Ausgangspunkt ist die Definition kritischer Infrastrukturen nach § 2 Abs. 10 BSIG. Demnach sind kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon, die nach Nr. 1 bestimmten Sektoren unterfallen (namentlich: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen) und nach Nr. 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. In der Gesetzesbegründung wird insoweit ergänzt: Diese Sektoren seien für die „Sicherung der Grundbedürfnisse der Bevölkerung" von hoher Bedeutung.[647] Im Kontext der Meldung von Sicherheitsvorfällen (§ 8b BSIG) wird insoweit auch von Gefährdungen der „Versorgungssicherheit" gesprochen.[648]

Welche Dienstleistungen innerhalb des Sektors ab welchem Versorgungsgrad i.S.d. § 2 Abs. 10 Nr. 2 BSIG als kritisch anzusehen sind, wird nach § 10 Abs. 1 BSIG durch eine Rechtsverordnung des BMI, die *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* (BSI-KritisV) bestimmt. Nach der Gesetzesbegründung ist insoweit wiederrum ein zweistufiges Verfahren zugrunde zu legen:

Qualitativ ist zunächst zu ermitteln, „welche Dienstleistungen innerhalb der genannten Sektoren in dem Sinne kritisch sind, dass sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren

646 Vgl. *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 2 BSIG, Rn. 28.
647 BT-Drs. 18/4096, S. 23.
648 BT-Drs. 18/4096, S. 28.

Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kategorie Qualität sollte sich hierbei insbesondere auf die Sicherheit von Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung beziehen, die von einem Ausfall unmittelbar oder mittelbar beeinträchtigt wären."[649]

Bezüglich des Versorgungsgrades folgt sodann die quantitative Festlegung sog. Schwellenwerte, also die Größe einer Einrichtung, insbesondere mit Blick auf die Zahl der versorgten Personen, oberhalb derer eine entsprechende Einrichtung als kritisch zu qualifizieren ist.[650]

2. Novelle 2017 – Schutz digitaler Dienste

In der zweiten Novelle folgte die Umsetzung der europäischen NIS-RL vom 19.07.2016, die neben den bereits auf nationaler Ebene adressierten kritischen Infrastrukturen (hier als „wesentliche Dienste", Art. 4 Nr. 4, Anhang II NIS-RL) auch die hier gegenständlichen digitalen Dienste (Art. 4 Nr. 5, Art. 5 Abs. 2, Anhang III NIS-RL, Art. 1 Abs. 1 lit b) RL 2015/1535) einbezog. Hierunter fallen demnach Online-Suchmaschinen, Online-Marktplätze und Cloud-Computing-Dienste, die in der nationalen Umsetzung als digitale Dienste (§ 2 Abs. 11 BSIG) in § 8c BSIG adressiert werden. Teilweise werden diese Dienste als „besonders wichtiger Kernbereich des Internets" beschrieben.[651]

Die Gesetzesbegründung hingegen erläutert die besondere Bedeutung gerade dieser ausgewählten Dienste nicht. Die Dienste waren auch im ursprünglichen Kommissionsentwurf der NIS-RL nicht enthalten.[652] In EG 48 NIS-RL heißt es nun zumindest, diese Dienste seien „für das reibungslose Funktionieren vieler Unternehmen von wesentlicher Bedeutung. Eine Störung eines solchen digitalen Dienstes könnte die Bereitstellung anderer, von ihnen abhängiger Dienste verhindern und somit wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten in der Union beeinträch-

649 BT-Drs. 18/4096, S. 31 f.
650 Wie zuvor; anders als bei der qualitativen Ermittlung wird somit nicht unmittelbar auf die Schadfolgen bei einem Ausfall, sondern auf die Zahl der versorgten Personen bei Funktionsfähigkeit der kritischen Infrastruktur abgestellt.
651 *Schallbruch*, CR 2016, 663 (665).
652 EU-Kommission, KOM(2013) 48, Vorschlag zur NIS-RL, 5.7.2016.

tigen." Dabei unterscheiden sich die Dienste nach der Einschätzung des europäischen Gesetzgebers in ihrer gesellschaftsrelevanten Bedeutung von „wesentlichen Diensten" (in nationaler Terminologie: kritische Infrastrukturen), da (nur) letztere nach EG 49 S. 2 NIS-RL für die Aufrechterhaltung „kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung" seien. „Daher sollten die an Anbieter digitaler Dienste gestellten Sicherheitsanforderungen geringer sein."[653]

Die NIS-RL fokussierte sich mit der Adressierung der digitalen Dienste somit stärker auf das Funktionieren der Wirtschaft, was sich insbesondere auch mit Blick auf die Online-Marktplätze zeigt. Eine Störung des Amazon Marketplace mag für viele Kund:innen zwar misslich, für die zahlreichen Unternehmen, die hier möglicherweise sogar exklusiv ihre Waren anbieten, hingegen existenzbedrohend sein. Ähnliches erscheint z.B. für Nachrichtenseiten denkbar, die nicht zuletzt über den News-Bereich von *Google* erreichbar sind. Skalierbare Cloud-Computing-Dienste betreffen die zahlreichen Unternehmen, die ihre IT-Leistung dorthin ausgelagert haben. Was der Gesetzgeber jedenfalls damals aber wohl noch nicht im Blick hatte, waren die drohenden Gefahren durch (manipulative) Angriffe auf Online-Suchmaschinen und auch den später mit der NIS2-RL erfassten sozialen Netzwerken mit ihren Folgen u.a. für Informationsgrundrechte und die öffentliche Meinungsbildung, dazu später (S. 256 ff.) ausführlich.

Der Fokus auf die Wirtschaft rechtfertigte aus Sicht des Gesetzgebers wohl eine geringer zu bemessende Kritikalität dieser Dienste. Denn auch wenn die Wirtschaftsförderung Teil des zu schützenden Gemeinwesens ist,[654] so sind wirtschaftliche und damit zumindest primär finanzielle Schäden in ihrer Gewichtung geringer einzuschätzen als etwa die unmittelbar auch humanitären Folgen einer erheblichen Störung in der Strom- oder Trinkwasserversorgung.

Im Ergebnis blieb das abstrakte Schutzgut der Funktionsfähigkeit des Gemeinwesens damit identisch, nur wurde bei digitalen Diensten der Fokus stärker auf die Wirtschaft verlagert. Es wird damit im Rahmen digitaler Dienste in einer besonderen Ausprägung des Gemeinwesens geschützt.

653 EG 49 NIS-RL, S. 3.
654 Dazu später bei den Schutzgütern: S. 238 f.

3. Novelle 2021 – Unternehmen im besonderen öffentlichen Interesse

Im Jahr 2021 folgte die Novellierung des BSIG mit dem IT-Sicherheitsgesetz 2.0. Im Rahmen dessen wurde insbesondere der Adressatenkreis erneut erweitert. Zusätzlich wurden nun sog. „Unternehmen im besonderen öffentlichen Interesse" (UBI) erfasst, zu denen nach § 2 Abs. 14 Nr. 1-3 BSIG drei Gruppen von Unternehmen gehören:

Zunächst nach § 2 Abs. 14 Nr. 1 BSIG Unternehmen, die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln. Diese Güter umfassen insbesondere Kriegswaffen.[655] Zweitens wurden Unternehmen erfasst, die aufgrund ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind. Gleichsam erfasst wurden auch aufgrund von Alleinstellungsmerkmalen nicht austauschbare Zulieferer solcher Unternehmen. Schließlich umschreibt die dritte Gruppe Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung oder solche, die nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind, so dass hier insbesondere Chemieunternehmen[656] adressiert wurden.

Anders als die zuvor genannten Adressaten trafen die UBI keine direkten Pflichten zur Vornahme von technischen und organisatorischen Maßnahmen, sondern lediglich Informationspflichten gegenüber dem BSI.[657] Die entsprechenden Selbsterklärungen zur IT-Sicherheit mussten zeigen, welche Zertifizierungen und sonstigen Audits/Prüfungen in den letzten zwei Jahren durchgeführt wurden. Außerdem muss das Unternehmen darlegen, wie es seine besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen schützt und ob dabei der Stand der Technik eingehalten wird.

655 *Monschke/Copeland*, CCZ 2022, 152 (152).
656 *Monschke/Copeland*, CCZ 2022, 152 (153).
657 Und auch das nur für Unternehmen der ersten und zweiten Gruppe.

4. Novelle 2024 – NIS2-RL

Am 27.12.2022 ist die neue NIS2-RL[658] in Kraft getreten. Diese ist nach Art. 41 Abs. 1 bis zum 17.10.2024 in nationales Recht umzusetzen, was in Deutschland eine weitere Novellierung des BSIG erforderlich macht. Die Novellierung soll nach aktuellem Stand durch das NIS2UmsuCG[659] erfolgen und führt neben inhaltlichen Änderungen insbesondere auch zu einer grundlegenden Änderung der Gesetzesstruktur des BSIG. In dieser Untersuchung wird dieses Gesetz mit dem Regierungsentwurf vom 22.07.2024 als *RegE BSIG* bezeichnet und für den weiteren Verlauf zugrunde gelegt.

Die IT-Sicherheitspflichten für betroffene Unternehmen werden nun wie bereits beschriebenen in der neuen Pflichtennorm des § 30 RegE BSIG festgelegt, was insbesondere auch die digitalen Dienste betrifft. Für Betreiber kritischer Anlagen (§ 2 Nr. 22, 24, § 56 Abs. 4 RegE BSIG) gelten die zusätzlichen Anforderungen des § 31 RegE BSIG. Die selbstständige Kategorie der „Unternehmen im besonderen öffentlichen Interesse" ist wieder entfallen, die entsprechenden Unternehmen werden aber nun ebenfalls von § 30 RegE BSIG adressiert.[660]

Darüber hinaus wurde der Adressatenkreis erweitert. Besonders bemerkenswert ist insoweit, dass entsprechend der NIS2-RL wie auch schon bei den UBIs auch Unternehmen erfasst werden, die anders als kritische Anlagen oder digitale Dienste keine besonders kritischen Dienstleistungen anbieten. Hierzu gehört insbesondere der Sektor „verarbeitendes Gewerbe/Herstellung von Waren" u.a. mit dem Maschinen- und Kraftfahrzeugbau.[661]

Das Adressatenmodell wurde ebenfalls grundlegend geändert, so dass nun primär zwischen *„besonders wichtigen Einrichtungen"* und *„wichtigen Einrichtungen"* unterschieden wird. Weiterhin bestehen nun zwei Kataloge, die zwei verschiedene Sektorengruppen adressieren (Anlage 1, 2 RegE BSIG) und die im Weiteren als „kritische Sektoren" und „weniger kritische Sektoren" bezeichnet werden sollen.

---

658 RL 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

659 Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz).

660 BReg, Entwurf NIS2UmsuCG, 22.07.2024, S. 145

661 § 28 Abs. 2 Nr. 3 i.V.m. Anlage 2, Ziff. 5, 5.4-5.6 RegE BSIG.

Betreiber kritischer Anlagen (bislang: kritische Infrastrukturen) sind zugleich *besonders wichtige Einrichtungen* nach § 28 Abs. 1 Nr. 1 RegE BSIG.[662] Auch Großunternehmen, die aufgrund einer Unterschreitung der Schwellenwerte zwar (noch) keine kritische Anlage betreiben, aber trotzdem einem kritischen Sektor (z.B. Energie- und Wasserversorgung) angehören, werden nach § 28 Abs. 1 Nr. 4 RegE BSIG *als besonders wichtige Einrichtungen* erfasst.[663]

Zu den *wichtigen Einrichtungen* gehören nun Unternehmen mittlerer Unternehmensgröße in kritischen Sektoren sowie mittlere Unternehmen und Großunternehmen in weniger-kritischen Sektoren. Zu den weniger kritischen Sektoren gehören nach Einschätzung des Gesetzgebers neben z.B. dem genannten Maschinen- und Kraftfahrzeugbau insbesondere auch die *Anbieter digitaler Dienste*. Der Kreis der Anbieter digitaler Dienste (Anlage 2, Ziff. 6 RegE BSIG) wird außerdem verändert, hierzu gehören nun auch „Plattformen für Dienste sozialer Netzwerke" (hier nur: „soziale Netzwerke"). Eine solche ist nach § 2 Nr. 30 RegE BSIG definiert als:

> „eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;"

Damit wurde ein weiterer Anbieter eines Dienstes aufgenommen, der sich durch einen hohen Grad an algorithmischer Personalisierung auszeichnet und somit für den Untersuchungsgegenstand dieser Arbeit von besonderer Bedeutung ist. Dafür gehören Cloud-Computing-Dienste (trotz entsprechender Definition, § 2 Nr. 4 RegE BSIG)[664] nicht mehr zu dem Sektor digitaler Dienste, sondern zum (kritischen) Sektor „Informationstechnik und Telekommunikation."[665]

662 Vgl. *Kipker/Dittrich*, MMR 2023, 481 (482).

663 Allerdings mit geringeren Anforderungen als Betreiber kritischer Anlagen, § 31 RegE BSIG. Zusätzlich werden größenunabhängig „qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registry [und] DNS-Diensteanbieter" sowie mittlere Unternehmen im Telekommunikationssektor erfasst (§ 28 Abs. 1 Nr. 2, 3 RegE BSIG).

664 Siehe hierzu später, S. 283, Fn. 859.

665 Anlage 1, Ziff. 6.1.4. RegE BSIG.

5. Fazit

Aus der historischen Betrachtung des (RegE) BSIG kann als erste Erkenntnis eine stetige Erweiterung des Adressatenkreises festgestellt werden. Waren die Adressaten ursprünglich nur Kritische Infrastrukturen (später: kritische Anlagen), die essenzielle Dienstleistungen der Daseinsvorsorge (dazu sogleich) anboten, wurde der Adressatenkreis im Laufe der Zeit kontinuierlich auch um immer weniger kritische Einrichtungen (zunächst etwa digitale Dienste, dann z.B. auch Unternehmen im Maschinen- und Kraftfahrzeugbau) erweitert und so das IT-Sicherheitsrecht von einem spezifischen Recht kritischer Infrastrukturen in die Breite der Unternehmenslandschaft gebracht.

Diese historische Entwicklung weist bereits auf die möglichen Herausforderungen bei der Frage der Schutzgüter hin. Diesem Hinweis folgend soll nun die Frage der Schutzgüter zunächst anhand der klassischen kritischen Infrastrukturen bzw. Anlagen beleuchtet (II.) und davon ausgehend die Schutzgüter der digitalen Dienste als „neue Adressaten" in den Blick genommen werden (III.).

II. Schutzgüter kritischer Anlagen

Im Rahmen der historischen Entwicklung wurde die Erweiterung des Adressatenkreises dargestellt. Je nach Adressatenkreis und damit auch je nach Sektor könnten auch unterschiedliche Schutzgüter betroffen sein. Dieser Frage soll nun vertieft nachgegangen werden, indem zunächst die Schutzgüter für die historisch zuerst adressierten kritischen Anlagen (früher: kritische Infrastrukturen) beschrieben werden.

1. Begriff der Daseinsvorsorge

Bereits in der früheren Entwicklung des BSIG (Novelle 2015) wurden die kritischen Infrastrukturen anhand ihrer Bedeutung für die „Sicherung der Grundbedürfnisse"[666] sowie das „Funktionieren des Gemeinwesens" definiert, da ein Ausfall oder eine Beeinträchtigung ihrer Dienstleistungen „erhebliche Versorgungsengpässe" befürchten ließe (§ 2 Abs. 10 BSIG) und hat

666 BT-Drs. 18/4096, S. 23.

sich in ähnlicher Form bis heute gehalten bzw. wird auch noch erweitert: So wird § 2 Nr. 24 RegE BSIG die von kritischen Anlagen zu erbringende kritische Dienstleistung definiert als „eine Dienstleistung zur *Versorgung der Allgemeinheit* in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu *erheblichen Versorgungsengpässen* oder zu Gefährdungen der öffentlichen Sicherheit führen würde".[667]

Viele dieser Begriffe und auch die dabei adressierten Sektoren wie z.B. Energie, Wasser, Siedlungsabfallentsorgung und Gesundheit weisen bereits dem ersten Anschein nach starke Parallelen zum Begriff der *Daseinsvorsorge* auf, der im nachfolgenden deshalb genauer beleuchtet werden soll, um damit die Schutzgüter genauer zu bestimmen.

Auf Basis des in Deutschland von *Ernst Forsthoff*[668] etablierten Begriffs der Daseinsvorsorge kann mit diesem heute die Versorgung der Bevölkerung mit den nach dem jeweiligen Stand der Zivilisation für eine normale Lebensführung notwendigen Gütern und Dienstleistungen beschrieben werden.[669] Sie werden deshalb im Weiteren als „Daseinsvorsorgeleistungen" bezeichnet. In Deutschland kann hierunter insbesondere gezählt werden: Die Strom- und Wasserversorgung, die Entsorgung von Abfall und

667 Eine sehr ähnliche Formulierung findet sich auch für „wesentliche Dienste" in Art. 2 Nr. 5 RKE-RL; diese wesentlichen Dienste werden zwar in der NIS2-RL nicht mehr explizit aufgegriffen, aber „kritische Einrichtungen" (die wesentliche Dienste erbringen, Art. 6 Abs. 2 lit a) RKE-RL) sollen nach EG 30 NIS2-RL zugleich als „wichtige Einrichtungen" gelten. Insoweit wirken diese (ähnlichen) Vorgaben also auch in der NIS2-RL.

668 *Forsthoff*, Rechtsfragen der leistenden Verwaltung, S. 9 ff..; zu der kritischen Verquickung der forsthoffschen Idee der Daseinsvorsorge mit völkischem Gedankengut in *Forsthoff*, Die Verwaltung als Leistungsträger (1938) siehe: *Püttner*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 32 (33); *Schiller*, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, S. 74 ff.;

669 *Forsthoff* seinerzeit mit der engen Definition: „Leistungen, auf welche der in die modernen massentümlichen Lebensformen verwiesene Mensch lebensnotwendig angewiesen ist", *Forsthoff*, Rechtsfragen der leistenden Verwaltung, S. 27; *Bull*, Der Staat 2008, 1 (3); *Henneke*, in: Krautscheid/Waiz/Münch, Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, 17 (18); zur Kritik an der begrifflichen Weite des Begriffs, aber gleichwohl zur Anerkennung als *„deskriptiver Sammelbegriff"* im hier verwendeten Sinn: *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, S. 46 f.

Abwasser, die Post, die Telekommunikation, der Rundfunk, die Gesundheitsversorgung, der ÖPNV sowie die Bildung.[670] Mit der Kopplung an den Stand der Zivilisation unterliegt dieser Katalog einer *dynamischen Veränderung*, d.h. mit steigendem Wohlstand und fortschreitender technologischer Entwicklung erweitert sich auch der Umfang der zur normalen Lebensführung, auch unter Berücksichtigung der Möglichkeit zur Teilnahme am Sozialleben, erforderlichen Leistungen.[671] So muss inzwischen zur Daseinsvorsorgeleistung im Bereich der Telekommunikation insbesondere der Internetzugang[672] sowohl über das Festnetz[673] als auch via Mobilfunk in entsprechender Bandbreite gezählt werden. Stellt man diese Daseinsvorsorgeleistungen mit den Sektoren kritischer Dienstleistungen nach § 2 Nr. 24 RegE BSIG gegenüber, fällt eine deutliche Überschneidung auf, insbesondere bezüglich der Strom-, Wasser, und Abwasserversorgung, Siedlungsabfallentsorgung, Informationstechnik und Telekommunikation, des Gesundheitswesens, des Finanz- und Versicherungswesens sowie des Transports und Verkehrs.

Insoweit lässt sich attestieren, dass der RegE BSIG mit dem Begriff der kritischen Dienstleistungen und damit auch den diese erbringenden kritischen Anlagen (§ 2 Nr. 22, 24 RegE BSIG)in einem weiten Verständnis[674] die der Daseinsvorsorge entsprechenden Sektoren adressiert. Genauer begrifflich ausdifferenziert lässt sich sagen, dass die Daseinsvorsorge und parallel dazu die kritische Dienstleistung als Beschreibung der (jeweiligen)

670 *Henneke*, in: Krautscheid/Waiz/Münch, Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, 17 (18); ähnlich auch: *Ronellenfitsch*, in: Magiera/Sommermann, Daseinsvorsorge und Infrastrukturgewährleistung, 27 (33); *Spannowsky*, in: Spannowsky/Runkel/Goppel, Raumordnungsgesetz (ROG), 2. Auflage 2018, § 2, Rn. 80.

671 *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 63 f.; *Pfannkuch*, KommJur 2023, 245 (245, 247 f.), der nun auch die Bereitstellung einer Ladeinfrastruktur für E-Autos zur Daseinsvorsorge zählt.

672 *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 63; *Luch/S. E. Schulz*, MMR 2009, 19 (23).

673 Der Anspruch auf einen solchen „Universaldienst" ist inzwischen in § 156 Abs. 1 i.V.m. § 157 Abs. 2 TKG niedergelegt; zu dessen Bedeutung für die „soziale und wirtschaftliche Teilhabe an der Gesellschaft" siehe: BT-Drs. 19/26108, S. 348.

674 Zusätzlich nicht typischerweise zur Daseinsvorsorge gezählt werden die in § 2 Nr. 24 RegE BSIG ebenfalls genannten Sektoren Ernährung und Weltraum.

Aufgabe bzw. Leistung verstanden werden kann[675] und die zugehörige Anlage das Instrument zur Bereitstellung derselben verkörpert.[676]

Auf europäischer Ebene (Art. 106 Abs. 2 AEUV) wird statt dem Begriff der Daseinsvorsorge der Begriff der „Dienstleistungen von allgemeinem (wirtschaftlichem) Interesse" (DA(W)I) verwendet.[677] Dieser auf dem französischen „service public" aufbauende Begriff[678] ist zwar zur Daseinsvorsorge nicht deckungsgleich, folgt aber im Wesentlichen derselben Idee[679]. Insoweit stellt die EU-Kommission die Bedeutung dieser Dienstleistungen für die „Befriedigung der Grundbedürfnisse der Bürger und die Erhaltung von Kollektivgütern" heraus.[680] Ersteres auslegend kann man mithin auch hier sagen, dass es sich um Leistungen handelt, auf die der Einzelne „für seine Lebensführung typischerweise angewiesen ist."[681] Der Begriff der Kollektivgüter dürfte dem hier schon in Abgrenzung zu Individualrechtsgütern geprägten Begriff der Gemeinschaftsrechtsgüter entsprechen.

Auch in der konkreten inhaltlichen Erfassung stimmt dieser europäische Begriff überwiegend mit der Daseinsvorsorge überein; die Kommission fasst unter die Dienstleistungen im allgemeinen wirtschaftlichen Interesse insbesondere die großen „netzgebundenen Wirtschaftszweige […] wie Telekommunikations-, Strom-, Gas-, Verkehrs- und Postdienste" sowie den Rundfunk, die Abfallwirtschaft und die Wasserversorgung bzw. die Abwas-

675 In diese Richtung auch: *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 32.

676 Vgl. *Wolff*, in: Gusy/Kugelmann/Würtenberger, Rechtshandbuch Zivile Sicherheit, 657 (662).

677 Ohne das Merkmal der Wirtschaftlichkeit erfassen „Dienstleistungen von allgemeinem Interesse" auch nicht-marktbezogene Dienstleistungen, EU-Kommission, KOM(2004) 375 endgültig, 12.5.2004, Anhang I, S. 27, wie etwa Polizei und Justiz, EU-Kommission, KOM(2007) 725 endgültig, 20.11.2007, S. 4 f. sowie „Pflichtschulwesen und soziale Sicherheit", EU-Kommission, Leistungen der Daseinsvorsorge in Europa, ABl. 1996 Nr. C 281/3, Rn. 18 und die Wahrnehmung anderer „kultureller, sozialer oder karitativer Belange", *C. Jung*, in: Calliess/Ruffert, EUV/AEUV, 6. Auflage 2022, Art. 106 AEUV, Rn. 39, m.w.N.

678 *Ronellenfitsch*, in: Magiera/Sommermann, Daseinsvorsorge und Infrastrukturgewährleistung, 27 (36).

679 *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 85; *Püttner*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 32 (36).

680 EU-Kommission, KOM(2003) 270 endgültig, 21.5.2003, S. 3.

681 *W. Weiß*, EuR 2013, 669–687 (672).

serentsorgung.[682] Jenseits der NIS2-RL gelten für diese Dienstleistungen bzw. die Anbieter derselben europarechtlich insbesondere Einschränkungen des Wettbewerbsrechts nach Art. 106 Abs. 2 AEUV. Ihre grundrechtliche Bedeutung wird auch durch Art. 36 GRC unterstrichen.[683]

Der Begriff der Daseinsvorsorge erschöpft sich zunächst in seiner rechtlichen Bedeutung in der *deskriptiven Zusammenfassung*[684] der Leistungen, die für die Versorgung der Bevölkerung zum jeweiligen Zivilisationsstand von besonderer Bedeutung sind.[685]

Die Frage, ob und in welchem Umfang der Staat für diese Daseinsvorsorgeleistungen einzustehen hat und die (Gewährleistung der) Erbringung derselben gleichsam zur Staatsaufgabe wird, ist somit noch nicht beantwortet.[686] Eine Antwort auf diese Frage ist aber erforderlich, um zu bestimmen ob und inwieweit die Leistungserbringungen im Bereich der Daseinsvor-

682 EU-Kommission, KOM(2007) 725 endgültig, 20.11.2007, S. 3 f.

683 Dabei gewährt Art. 36 GRC aber weder ein subjektives (Grund)recht noch ein objektives Recht, das die Mitgliedsstaaten zur Bereitstellung verpflichten würde. Die Gegenansicht für ein objektives Recht: *M. Jung*, Die Europäisierung des Gemeinwohls am Beispiel des Art. 106 Abs. 2 AEUV, S. 62; uneindeutig: sowohl als „soziales bzw. wirtschaftliches" Grundrecht, aber ohne eigenständiges, „individuell einklagbares Leistungsrecht" *Krajewski*, in: Pechstein/Nowak/Häde, Frankfurter Kommentar zu EUV, GRC und AEUV, 2. Auflage 2023, Art. 36 GRC, Rn. 4 ff. bzw. als subjektives Recht, sich gegen Einschränkungen der DAWI durch die Europäische Union zur Wehr zu setzen: *Krajewski*, in: Wagner/Wedl, Bilanz und Perspektiven zum europäischen Recht, 433 (441). Vielmehr handelt es sich nach wohl überwiegender Auffassung um einen Grundsatz im Sinne des Art. 52 Abs. 5 GRC, der somit nur bei der Auslegung und bei Entscheidungen über die Rechtmäßigkeit europäischer Rechtsakte (auch Sekundärrecht sowie in Umsetzung europäischen Rechts erlassenes nationales Recht) berücksichtigt werden muss, *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 36, Rn. 3; *Pielow*, in: Stern/Sachs, Europäische Grundrechte-Charta 2016, Art. 36, Rn 37; *Rohleder*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage 2019, Art. 36, Rn. 14 m.w.N.

684 *Schiller*, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, S. 79; *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 48; *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, S. 47; a.A. wohl *Ronellenfitsch*, in: Magiera/Sommermann, Daseinsvorsorge und Infrastrukturgewährleistung, 27 (31 ff.).

685 Anders bei den europäischen „Dienstleistungen vom allgemeinem wirtschaftlichem Interesse", die von den Mitgliedsstaaten durch Hoheitsakt explizit als solche bestimmt werden müssen, um die entsprechenden Privilegierungen nach Art. 14, 106 AEUV zu erhalten: *C. Jung*, in: Calliess/Ruffert, EUV/AEUV, 6. Auflage 2022, Art. 14 AEUV, Rn 12 f.; *EuG*, Urt. v. 12.02.2008 – T-289/03, BeckRS, 70248, Rn. 172.

686 So wies auch bereits *Forsthoff* darauf hin, dass allein aus der Zuordnung zur Daseinsvorsorge noch keine Rechtsfolgen im Sinne von Verpflichtungen der Ver-

sorge als rechtliche Schutzgüter zu qualifizieren sind. Eine staatliche Einstandspflicht ist jedenfalls nicht selbstverständlich, denn in einer sozialen Marktwirtschaft erfolgt die Versorgung mit Gütern und Dienstleistungen, -auch jenen, die (lebens)notwendig sind- grundsätzlich nicht durch den Staat, sondern durch private Akteure und der Staat kann sich grundsätzlich darauf beschränken, die entsprechenden Rahmenbedingungen zu schaffen.[687]

a. Verfassungsrechtliche Pflichten zur Leistungsbereitstellung

Im nächsten Schritt wird deshalb untersucht, inwieweit sich die Pflicht zur Bereitstellung i.S. einer Verfügbarmachung von Daseinsvorsorgeleistungen als Teil der öffentlichen Leistungsverwaltung[688] verfassungsrechtlich herleiten lässt.[689] Hierbei wird auf Leistungsansprüche aus Grundrechten (i.), grundrechtliche Schutzpflichten (ii.), Gemeinwohlziele (iii.) sowie das Sozialstaatsprinzip (iv.) eingegangen. Abschließend wird ein Fazit gezogen (v.).

i. Leistungsansprüche aus Grundrechten

Im Grundsatz wird die Ableitung originärer Leistungsansprüche („status positivus“) aus den Grundrechten kritisch gesehen.[690] Teilweise wird aber

---

waltung zur Schaffung oder Verbesserung entsprechender Leistungen resultieren, *Forsthoff*, Rechtsfragen der leistenden Verwaltung, S. 12 f.

687 *Henneke*, in: Krautscheid/Waiz/Münch, Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, 17 (17).

688 *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 36; *H. Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, S. 7, Rn 16 f.

689 Für eine Herleitung aus grundrechtlichen Schutzpflichten und dem Sozialstaatsprinzip bereits: *Luch/S. E. Schulz*, MMR 2009, 19 (20); *Haack*, VerwArch 2009, 197 (203).

690 Ausnahmen bestehen aber, wenn der Verfassungstext dies wie etwa beim Mutterschutz (Art. 6 Abs. 4 GG) ausdrücklich vorsieht: *Di Fabio*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 2, Rn. 57. Außerdem i.V.m. dem Sozialstaatsprinzip: *Grzeszick*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20, VII. Sozialstaat, Rn. 31; *BVerfG*, Beschluss v. 29.05.1990 – 1 BvL 20/84, 1 BvL 26/84, 1 BvL 4/86 (erhältlich in juris), Rn. 88. Zu einer Leistungspflicht bei der Informationsfreiheit (Art. 5 Abs. 1 Alt. 2 GG): *Paulus*, in: Huber/Voßkuhle, Grundgesetz, 8. Auflage 2024, Art. 5, Rn. 69 m.w.N.

zumindest vertreten, dass die Verfügbarkeit der Daseinsvorsorgeleistungen aufgrund dessen, dass sie erst eine normale Lebensführung ermöglichen, Voraussetzung für den Grundrechtsgebrauch sei und der Staat insoweit eine vorgelagerte „Grundrechtsermöglichungspflicht" habe.[691] Eine andere Argumentationslinie stützt sich direkt auf die Würde des Menschen nach Art. 1 Abs. 1 GG, die (ggf. i.V.m. dem Sozialstaatsprinzip) die Bereitstellung der Leistungen für ein „menschenwürdiges Existenzminimum" verlange.[692] Das BVerfG zählt zu letzterem insbesondere „Nahrung, Kleidung, Hausrat, Unterkunft, Heizung, Hygiene und Gesundheit."[693]

Für die Ableitung von Ansprüchen auf die Bereitstellung von Daseinsvorsorgeleistungen ist indes bei beiden Argumentationslinien Zurückhaltung geboten. In der Tat ist zwar aus Art. 1 Abs. 1 GG i.V.m. Art. 20 Abs. 1 GG mit dem BVerfG ein Anspruch auf die Versorgung mit Daseinsvorsorgeleistungen anzuerkennen, aber nur soweit es tatsächlich das Existenzminium im o.g. Sinne betrifft.[694] Würden diese Bedürfnisse durch den freien Markt nicht (mehr) erfüllt, z.B. im Falle von Katastrophen, so wäre der Staat grundrechtlich verpflichtet die entsprechenden Leistungen selbst zu erbringen. Weitergehende Ansprüche auch im Sinne einer „Grundrechtsermöglichungspflicht" drohen hingegen die Grundrechte in ihrem Gehalt schnell zu überdehnen, da es kaum objektiv bestimmbar erscheint, welche Leistungen über das Existenzminimum hinaus für die konkrete Grundrechtsausübung des Einzelnen nach dem jeweiligen zivilisatorischen Stand der Gesellschaft erforderlich wären.

691 *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, S. 186; ähnlich auch i.V.m. dem Sozialstaatsprinzip: *Friauf*, DVBl 1971, 674 (676 f.); *Haack*, VerwArch 2009, 197 (203); EU-Kommission, KOM(2004) 375 endgültig, 12.5.2004, S. 5.

692 *BVerfG*, Urt. v. 09.02.2010 – 1 BvL 1/09, 1 BvL 3/09, 1 BvL 4/09 (erhältlich in juris), Rn. 133.

693 *BVerfG*, Urt. v. 09.02.2010 – 1 BvL 1/09, 1 BvL 3/09, 1 BvL 4/09 (erhältlich in juris), Rn. 135.

694 D.h. soweit sie zur „Aufrechterhaltung eines menschenwürdigen Daseins unbedingt erforderlich" sind: *BVerfG*, Urt. v. 09.02.2010 – 1 BvL 1/09, 1 BvL 3/09, 1 BvL 4/09 (erhältlich in juris), Rn. 133, 135; siehe auch: *BVerfG*, Beschluss v. 08.06.2004 – 2 BvL 5/00 (erhältlich in juris), Rn. 96; *BVerfG*, Beschluss v. 29.05.1990 – 1 BvL 20/84, 1 BvL 26/84, 1 BvL 4/86 (erhältlich in juris), Rn. 83, 99; mit Blick auf die Daseinsvorsorge ebenso *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 96.

ii. Grundrechtliche Schutzpflichten

Weiterhin könnten staatliche Schutzpflichten zur Begründung herangezogen werden. Im Rahmen der Schutzpflichten hat der Staat die Pflicht, den Bürger vor der Verletzung seiner Grundrechte durch Dritte zu schützen.[695] Sie sind in ihrem Umfang allerdings weit weniger konkret als die Abwehr- oder die o.g. Leistungsdimension; insbesondere folgen aus ihnen keine subjektiven Ansprüche auf die Gewährleistung eines bestimmten Zustands",[696] also etwa das staatliche, initiale Angebot neuer Leistungen."[697] Vielmehr hat der Gesetzgeber bei der Ausgestaltung der Schutzpflichten einen *weiten Einschätzungsspielraum*, bei der er insbesondere auch widerstreitende Interessen und Rechtsgüter berücksichtigen kann und muss.[698]

In der Folge können die Schutzpflichten jedenfalls keinen Anspruch auf die initiale Bereitstellung von Daseinsvorsorgeleistungen begründen. Gut begründbar erscheint es dagegen, zumindest eine Verpflichtung des Staates anzunehmen, die *Kontinuität der häufig auch von Dritten, d.h. von privaten Akteuren, erbrachten Daseinsvorsorgeleistungen sicherzustellen*. So können bei einigen Infrastrukturleistungen wie insbesondere der Strom-, Wasser- oder der Gesundheitsversorgung plötzliche Ausfälle schnell sogar Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 S. 1 GG, Art. 2 Abs. 1, 3 Abs. 1 GRC) der betroffenen Personen bedrohen.[699] Der Grund dafür liegt v.a. auch in der sog. *symbolischen Kritikalität*, mit der das Vertrauen der Bürger:innen in die kontinuierliche Erbringung der Daseinsvorsorgeleistungen beschrieben wird.[700] Würde dieses Vertrauen nicht bestehen, müssten sie ihr Leben grundlegend anders strukturieren, etwa durch eine ausgeprägte Vorratshaltung an Wasser oder auch Strom. Umgekehrt resultiert ihre besondere Verletzlichkeit gerade daraus, dass sie aufgrund ihres bestehenden Vertrauens keine solche Vorratshaltung betreiben, so dass insbesondere der

695 *H. Klein*, DVBl 1994, 489 (491, 493).
696 *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, 189.
697 Wie zuvor.
698 *BVerfG*, Beschluss v. 29.10.1987 – 2 BvR 624/83, NJW 1988, 1651 (1656 f.), Rn. 133; *H. Klein*, DVBl 1994, 489 (495).
699 Vgl. *Freimuth,* Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, S. 167.
700 Ausführlicher zum Begriff der systemischen bzw. symbolischen Kritikalität einschließlich anderer Begriffsverständnisse bereits in: *Sterz/Werner/Raabe*, RDV 2023, 97 (101).

plötzliche, unerwartete Ausfall der Daseinsvorsorgeleistungen schwerwiegende Grundrechtsverletzungen nach sich ziehen kann.[701]

Weiterhin ist zu berücksichtigen, dass Grundrechtsverletzungen über die *systemische Kritikalität* von kritischen Anlagen auch mittelbar wirken können, d.h. der Ausfall einer kritischen Anlage kann zu Kaskadeneffekten und so zum Ausfall anderer, abhängiger Infrastrukturen führen, die ihrerseits Grundrechtsrelevanz haben[702] (etwa der Ausfall der Strom- hinsichtlich der Gesundheitsversorgung).

Zum Schutz vor möglichen Grundrechtsbeeinträchtigen muss der Staat somit im Rahmen der grundrechtlichen Schutzpflichten tätig werden und die Daseinsvorsorgeleistungen (auch) gegen IT-bedingte Ausfälle absichern.

iii. Gemeinwohlziele

Neben den Grundrechten bestehen außerdem staatliche *Gemeinwohlziele*. Das Gemeinwohl stellt als die Idee eines guten und gedeihlichen Gemeinwesens das übergeordnete Ziel dar, dem sich gesetzte oder noch zu setzende Staatsziele verpflichten müssen, wenn sie legitim sein sollen.[703] Zur Klarstellung dieses Bezugs werden die Staatsziele im weiteren als Gemeinwohlziele bezeichnet.[704] In der Regel dienen Daseinsvorsorgeleistungen, wie sich sogleich zeigen wird, der Erfüllung entsprechender Gemeinwohlziele.[705]

---

701 Diese Vertrauenserwartung wird z.T. durch den Staat selbst eingeschränkt, indem beispielsweise das BBK Empfehlungen zur Bevorratung von Trinkwasser und Lebensmitteln gibt: https://www.bbk.bund.de/DE/Warnung-Vorsorge/Vorsorge/Bevorraten/bevorraten_node.html; zuletzt abgerufen am 14.04.2024.

702 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, S. 5; *Metzger*, in: Wenger, Bulletin 2004 zur schweizerischen Sicherheitspolitik, 73 (77); soweit Infrastrukturen wechselseitig voneinander abhängig sind wird zur Beschreibung der systemischen Kritikalität auch von der „Interdependenz" infrastruktureller Dienste gesprochen: *Folkers*, in: Engels/Nordmann, Was heißt Kritikalität?, 123 (133).

703 *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 3 (4), Rn. 2.

704 Zur Abgrenzung von „hinter der Verfassung stehenden, den Staat selbst „legitimierenden" Staatszwecken; *Calliess*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20a, Rn. 29; zur Abgrenzung von den Staatsstrukturprinzipien/Staatsstrukturnormen (z.B. das Rechtsstaatsprinzip) siehe: *M. Kaufmann*, JZ 1999, 814 (815).

705 Teilweise wird die Daseinsvorsorge im Sinne einer „infrastrukturellen Grundausstattung" sogar als „notwendige Existenzbedingung moderner Staatlichkeit" und da-

Gemeinwohlziele lassen sich in zwei Kategorien unterteilen: Zunächst lassen sich *absolute Gemeinwohlziele* definieren, das heißt solche die allgemein anerkannt oder sogar ausdrücklich verfassungsrechtlich verankert sind (etwa als Staatszielbestimmungen, dazu sogleich) und somit nicht von der jeweiligen Politik des einfachen Gesetzgebers abhängig sind.

Zu ersterem gehören exemplarisch die öffentliche Gesundheit[706], die zumindest in § 2 Nr. 4 RefE KRITIS-DachG auch entsprechend genannt wird.[707] Weiterhin auch die *Sicherstellung der Energie*[708]*- und Wasserversorgung*[709]. Darüber hinaus kann der Erhalt und die Förderung der Volkswirtschaft (nachfolgend nur: *Wirtschaftsförderung*) als Gemeinwohlziel definiert werden; die Verfassung legt zwar keine konkreten Vorgaben für die Gestaltung des Wirtschaftssystems fest,[710] aber das generelle Ziel der Wirtschaftsförderung lässt sich aus einer Gesamtschau der verfassungsrechtlichen Normen[711] herleiten.[712] Auch auf dieses Gemeinwohlziel wird in § 2

---

mit gewissermaßen als übergeordnetes Staatsziel angesehen, *Hermes*, in: Schuppert, Der Gewährleistungsstaat, 111 (113).

706 Damals noch unter dem Begriff „Volksgesundheit" und statt „Gemeinwohlziele" verwendet das BVerfG hier den wohl synonym zu verstehenden Begriff der „Gemeinschaftswerte": *BVerfG*, Beschluss v. 17.07.1961 – 1 BvL 44/55 (erhältlich in juris), Rn. 23.

707 Ebenso in Art. 2 Nr. 5 RKE-RL. Dort wird der wesentliche Dienst definiert, der von kritischen Einrichtungen erbracht wird (Art. 6 Abs. 2 lit a) RKE-RL); eine entsprechende Festlegung als kritische Einrichtung gilt auch in der NIS2-RL (Art. 3 Abs. 1 lit f). Der europäische Gesetzgeber sieht folglich in der öffentlichen Gesundheit ebenfalls ein Schutzgut, dass von kritischen Einrichtungen mit ihren Daseinsvorsorgeleistungen betroffen ist. Siehe im Übrigen zur RKE-Richtlinie auch bereits oben unter: S. 148 ff. Die öffentliche Gesundheit war im RefE BSIG auch noch in der Definition der kritischen Dienstleistung (§ 2 Abs. 1 Nr. 21 RefE BSIG) enthalten, wurde jedoch unverständlicherweise bis zum RegE wieder entfernt.

708 *Papier/Shirvani*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 14, Rn. 680; *BVerfG*, Beschluss v. 20.03.1984 – 1 BvL 28/82 (erhältlich in juris), Rn. 37; *BVerfG*, Urt. v. 17.12.2013 – 1 BvR 3139/08, 1 BvR 3386/08 (erhältlich in juris), Rn 286 f.; *BGH*, Urt. v. 12.03.2015 – III ZR 36/14, NVwZ 2015, 915, Rn. 25.

709 *BVerfG*, Urt. v. 29.07.1959 – 1 BvR 394/58 (erhältlich in juris), Rn. 81; *BVerfG*, Beschluss v. 15.07.1981 – 1 BvL 77/78, BeckRS 2010, 29303, Rn. 129 f.; *Hünnekens*, in: Landmann/Rohmer, Umweltrecht, 102. EL 2023, § 50 WHG, Rn. 6; siehe auch die Gesetzesbegründung zu § 50 WHG in BT-Drs. 16/12275, S. 66.

710 Im Detail umstritten, siehe zum Streitstand: *Stober/Korte*, Öffentliches Wirtschaftsrecht - Allgemeiner Teil, S. 46 f., Rn. 124 f.

711 Eine Liste mit allen Bezügen der Verfassung zum Sachbereich Wirtschaft findet sich bei: *Stober/Korte*, Öffentliches Wirtschaftsrecht - Allgemeiner Teil, S. 46, Rn. 122.

712 Insbesondere kann dies aus Art. 72 Abs. 2 GG mit dem Merkmal der „Wahrung der Wirtschaftseinheit", welches als Anliegen „Beseitigung von Schranken und Hinder-

Nr. 4 RefE KRITIS-DachG mit den „wichtigen wirtschaftlichen Tätigkeiten" explizit Bezug genommen.[713]

Verfassungsrechtlich verankert sind Gemeinwohlziele als „Staatszielbestimmungen", so etwa bei Art. 20a[714], Art. 87e Abs. 4[715] und 87f Abs. 1 GG[716]. Auch in den Kompetenztiteln des Bundes (Art. 73, 74 GG) wie etwa dem Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG) können zumindest mögliche Gemeinwohlziele gesehen werden.[717] Abgesehen von solchen Ausnahmen enthält das Grundgesetz aber keine allgemeine und abschließende Festlegung der Gemeinwohlziele; das Grundgesetz wirkt im Übrigen v.a. umgekehrt, indem es vom Grundgesetz missbilligte Ziele ausschließt.[718]

---

nissen für den wirtschaftlichen Verkehr im Bundesgebiet und damit die Abwehr erheblicher, wirtschaftspolitisch nachteiliger Auswirkungen" verfolgt, *Uhle*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 72, Rn. 151; *BVerfG*, Beschluss v. 27.01.2010 – 2 BvR 2185/04, KommJur 2010, 461 (462) Rn. 57 abgeleitet werden; dies gilt insbesondere i.V.m. dem Kompetenztitel des Rechts der Wirtschaft nach Art. 74 Nr. 11 GG (siehe auch Fn. 717); Darüber hinaus kann man dies auch aus der objektiven Verpflichtung des Staates, auf eine ausreichende Anzahl von Arbeits- und Ausbildungsplätzen hinzuwirken, entnehmen - diese wird aus Art. 12 GG hergeleitet: *Scholz*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 12 Rn. 13 m.w.N.; Die Bedeutung von kritischen Infrastrukturen für die Wirtschaft hebt auch *Emmert*, DuD 2016, 34 (34 f.) hervor.

713 Siehe zuvor entsprechend S. 239, Fn. 707.

714 *Calliess*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20a, Rn. 19 ff., 29 ff. m.w.N.

715 *Möstl*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 87e, Rn. 182, m.w.N.

716 Der in Art. 87f GG liegenden verfassungsrechtlichen Versorgungsgarantie wird für ein Staatsziel ein „ungewöhnlicher Verdichtungsgrad normativer Verbindlichkeit" attestiert, *Cornils*, in: Geppert/Schütz, Beck'scher Kommentar zum TKG, 5. Auflage 2023, Vorb. §§ 156 ff., Rn 16; *Cornils*, AöR 2006, 378-422 (382); kritisch zu einer solchen unbedingten Erfolgsgarantie neben *Cornils*, a.a.O., wohl auch *Danwitz*, DÖV 2004, 977 (984).

717 Vgl. *Korioth*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 30, Rn. 14, 17 der in den Kompetenztiteln zugleich Staatsaufgaben, d.h. Gemeinwohlaufgaben sieht; *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 152 f.; *Schulze-Fielitz*, in: Grimm, Wachsende Staatsaufgaben - sinkende Steuerungsfähigkeit des Rechts, 11 (21).

718 *BVerfG*, Urt. v. 17.12.2013 – 1 BvR 3139/08, 1 BvR 3386/08 (erhältlich in juris), Rn. 172; Insbesondere Enteignungen nach Art. 14 Abs. 3 GG sind ebenfalls nur zulässig, wenn damit ein Gemeinwohlziel verfolgt wird. Als solches können hier neben den vom Grundgesetz missbilligten Zielen insbesondere das ausschließliche Interesse Privater sowie rein fiskalische Interessen des Staates keine Gemeinwohlziele darstellen: *BVerfG*, Beschluss v. 25.01.2017 – 1 BvR 2297/10, NVwZ 2017, 949

Die genannten Staatszielbestimmungen in Art. 87e Abs. 4 und 87f. Abs. 1 GG stellen außerdem spezifische, verfassungsrechtlich normierte, „infrastrukturelle Gewährleistungsaufträge“[719] dar und verpflichten somit den Staat unmittelbar zur Gewährleistung der Daseinsvorsorgeleistungen im Bereich der Eisenbahn (im Regional- und Fernverkehr)[720] sowie der Post und Telekommunikation. Schließlich kann auch das Staatsziel des Art. 20a GG mittelbar auf die Daseinsvorsorgepflichten einwirken; etwa mit Blick auf ein Angebot erneuerbarer Energien oder von (sozial vertretbaren) Alternativen zum fossilen Individualverkehr.

Die zweite Kategorie der Gemeinwohlziele (*relative Gemeinwohlziele*) kann der Gesetzgeber hingegen nach seinen „besonderen wirtschafts-, sozial- und gesellschaftspolitischen Vorstellungen“ bestimmen, diese also „erst selbst in den Rang wichtiger Gemeinschaftsinteressen“ erheben[721] oder ggf. auch wieder aufgeben. Hierbei kommt dem Gesetzgeber ein weiter Gestaltungsspielraum zu.[722] Eine solche flexible Gestaltung ist auch aus tatsächlichen Gründen zwingend, da die für die Gesellschaft besonders wichtigen Ziele im Laufe der Zeit der Veränderung unterliegen.[723] Auch staatsrechtlich bedarf es dieser Möglichkeit, damit dem demokratischen Gesetzgeber jenseits der Verfassung ein hinreichend großer politischer Entscheidungs-

(950), Rn. 35; zur Bestimmung und Abwägung von Staats- bzw. Gemeinwohlzielen im Grundgesetz: *Schuppert*, GewArch 2004, 441 (444 ff.).

719 *Möstl*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 87e, Rn. 182.

720 Der nicht hierunter fallende ÖPNV (*BVerwG*, Urt. v. 16.12.1999 – 3 A 2/99 (erhältlich in juris), Rn 51 ff.) wird ebenfalls zur Gewährleistung der Mobilität der Gesellschaft als von Ländern und Kommunen zu erfüllende Daseinsvorsorgeleistung qualifiziert, siehe hierzu normativ § 8 Abs. 3 S. 1 PBefG („Sicherstellung einer ausreichenden den Grundsätzen des Klimaschutzes und der Nachhaltigkeit entsprechenden Bedienung der Bevölkerung mit Verkehrsleistungen im öffentlichen Personennahverkehr“). In der Literatur wird insofern (z.T. bereits aus der Verfassung) qualitativ zwar keine optimale, aber zumindest eine Mindestversorgung mit Leistungen des ÖPNV gefordert: *D. Zhang*, Bessere Daseinsvorsorge durch Regulierung im Bereich des ÖPNV, S. 156 f.; *Ronellenfitsch*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 89 (91, 94).

721 *BVerfG*, Beschluss v. 17.07.1961 – 1 BvL 44/55 (erhältlich in juris), Rn. 23; ähnlich auch *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 117, S. 141, Rn. 44 f. mit weiteren Verweisen auf die Gegenansicht (statt vieler: *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 116 f.), wonach sich jedes Tätigwerden des Staates auf eine verfassungsrechtliche Grundlage stützen lassen müsste.

722 *BVerfG*, Urt. v. 17.12.2013 – 1 BvR 3139/08, 1 BvR 3386/08 (erhältlich in juris), Rn. 172; und ergänzend angemerkt: Natürlich erst recht bei der Intensität der Verfolgung bzw. dem Ausgleich zwischen Gemeinwohlzielen und ggf. auch Grundrechten.

723 *BVerfG*, Urt. v. 17.12.2013 – 1 BvR 3139/08, 1 BvR 3386/08 (erhältlich in juris), Rn. 171.

spielraum verbleibt. Als ein solches relatives Gemeinwohlziel könnte etwa die Einführung der elektronischen Patientenakte genannt werden, da dies über die Grundversorgung im Gesundheitssektor weit hinausgehen dürfte.

iv. Sozialstaatsprinzip

Schließlich kann ergänzend das in Art. 20 Abs. 1 und Art. 28 Abs. 1 S. 1 verankerte Sozialstaatsprinzip[724] herangezogen werden. Das Sozialstaatsprinzip hat ebenfalls „den Charakter einer Staatszielbestimmung",[725] d.h. es umschreibt zwar die Aufgabe, dass der Staat „für einen Ausgleich der sozialen Gegensätze und damit für eine gerechte Sozialordnung zu sorgen" hat, ohne aber konkret vorzugeben, wie diese zu erfüllen ist.[726]

Im Rahmen der Daseinsvorsorge betrifft das Sozialstaatsprinzip somit zunächst auch nicht die Versorgung an sich,[727] sondern lediglich eine allgemeine Teilhabemöglichkeit in dem Sinne, dass eine „Versorgung zu möglichst für alle tragbaren Bedingungen, was bei zahlreichen Leistungen Ermäßigungen für sozial Schwache einschließt"[728], sichergestellt ist. Einfachgesetzlich ist dies etwa ausdrücklich in § 158 TKG festgeschrieben, wonach Telekommunikationsdienste zu „erschwinglichen Preisen" angeboten werden müssen. Im schon angesprochenen Mobilitätssektor lässt sich außerdem beispielhaft anführen, dass der Staat aus dem Sozialstaatsprinzip heraus zumindest eine für jeden nutz- und bezahlbare Mobilitätsform anbieten muss.[729]

---

724 *Grzeszick*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20, VIII. Sozialstaat, Rn. 1 ff.

725 *Grzeszick*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20, VIII. Sozialstaat, Rn. 18; *H. Maurer/K.-A. Schwarz*, Staatsrecht I, § 9 Rn. 2; es wird aber teilweise zugleich als Staatsstrukturprinzip angesehen, so etwa *K.-A. Schwarz*, in: Stern/Sodan/Möstl, Das Staatsrecht der BRD im europäischen Staatenverbund, § 20, Rn. 10 ff.; dafür, dass Verfassungsnormen generell sowohl Staatsziel-, als auch Staatsstrukturelemente aufweisen können: *M. Kaufmann*, JZ 1999, 814 (815).

726 *BVerfG*, Urt. v. 18.07.1967 – 2 BvF 3/62 (erhältlich in juris), Rn. 74.

727 *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 96; *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, S. 50; *Louis*, Die Besteuerung der öffentlichen Unternehmen und Einrichtungen der Daseinsvorsorge, S. 180.

728 *Henneke*, in: Krautscheid/Waiz/Münch, Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, 17 (19).

729 Vgl. *Ronellenfitsch*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 89 (91, 94).

Auch mit Blick auf die IT-Sicherheitsvorschriften ist das auf die Daseinsvorsorge einwirkende Sozialstaatsprinzip zumindest von mittelbarer Bedeutung. Denn die mit der Gewährleistung der IT-Sicherheit verbundenen Kosten werden von den Betreibern letztlich auf die Verbraucher:innen umgelegt, was ggf. durch entsprechende sozialstaatliche Kompensationsmaßnahmen ausgeglichen werden müsste.

v. Zwischenfazit

Insgesamt lassen sich damit verschiedene Kategorien von Rechtsgütern zusammenfassen, aus welchen der Staat für die Erbringung der Daseinsvorsorge einzustehen hat. Als erstes konnte gezeigt werden, dass spezifische Grundrechte sowohl in ihrer Leistungs- als auch in ihrer Schutzpflichtdimension eine solche Pflicht begründen. Zum zweiten wurde dargestellt, dass die staatlichen Gemeinwohlziele, sowohl soweit sie in der Verfassung verankert sind als auch soweit sie vom einfachen Gesetzgeber nach eigenem politischen Ermessen angestrebt werden mit einer entsprechenden staatlichen Einstandspflicht einhergehen. Drittens wurde gezeigt, dass auch das Sozialstaatsprinzip auf diese Pflicht zumindest mittelbar einwirkt.

Anders als bei den Individualgrundrechten kommt es für die Aspekte des Gemeinwohls insbesondere darauf an, große Ausfälle zu vermeiden, die eine hohe Anzahl von Menschen beträfen.[730] Denn diese bedrohen im Gegensatz zu vereinzelten Fällen, die lediglich Individualgrundrechte beeinträchtigen, Gemeinschaftsrechtsgüter (z.B. die Sicherheit der Energieversorgung und die Wirtschaftsförderung). Dies gilt insbesondere, wenn durch einen Ausfall einer Leistung auch die Versorgung mit anderen Daseinsvorsorgeleistungen beeinträchtigt wird (sog. Kaskadeneffekte, z.B. der Ausfall der Gesundheitsversorgung in Folge eines längerfristigen Stromausfalls).

Die genannten Kategorien (Individualrechtsgüter, Gemeinschaftsrechtsgüter) stehen nicht isoliert nebeneinander, sondern tragen die Erbringungsnotwendigkeit häufig gemeinsam: Je nach Art der Daseinsvorsorgeleistung können die Bedeutungen der jeweiligen Kategorien in ihrer Kritikalität variieren: So hat die kontinuierliche Versorgung mit Strom- und Trinkwasser sowohl ein hohes grundrechtliches als auch gemeinwohlspezifisches

730 Vgl. BNetzA, Katalog von Sicherheitsanforderungen nach § 109 TKG, 29.04.2020, S. 36 f.

Gewicht. Dagegen kann z.B. das Ziel eines funktionierenden Eisenbahnverkehrs zwar auch zu den verpflichtenden Daseinsvorsorgeleistungen gezählt werden, aber eher mit dem Schutzgut des entsprechenden Staatsziels (Art. 87e GG), ggf. i.V.m. mit dem Sozialstaatsprinzip. Hingegen ist selbst bei längeren Ausfällen nicht mit schwerwiegenden individualgrundrechtlichen Auswirkungen zu rechnen, wie es etwa bei der Wasserversorgung der Fall ist.[731]

b. Originäre Wahrnehmung durch den Staat

Der Umstand, dass der Staat aus verfassungsrechtlichen Gründen für die Bereitstellung, d.h. die Verfügbarkeit von Daseinsvorsorgeleistungen einzustehen hat, determiniert noch nicht die Frage, ob und inwieweit der Staat diese Leistungen zur Erfüllung seiner Pflichten auch selbst erbringen muss oder sollte.

Staatsorganisationsrechtlich wird die Erbringung von Daseinsvorsorgeleistungen v.a. als „historisch gewachsene Kernaufgabe" der Gemeinden verstanden.[732] Die eigene Bereitstellung von Daseinsvorsorgeleistungen ist insofern auf kommunaler Ebene auch explizit zulässig (§ 102 Abs. 1 Nr. 3, Abs. 4 Nr. 1, 2 GemO BW) und unterliegt nicht den Einschränkungen kommunaler Wirtschaftstätigkeit.[733] Aber auch der Bund trägt Verantwortung für die Erbringung von Daseinsvorsorgeleistungen wie Teilen des Schienen- und Autoverkehrs, dem Bereich des Postwesens und der Telekommunikation (Art. 90,[734] Art. 87e, Art. 87f GG).

Zur Frage der Erfüllungspflicht ist zunächst festzustellen, dass aus verfassungsrechtlicher Sicht der Staat über die Erfüllung des Existenzminimums hinaus und soweit ebendiese Erfüllung nicht ohnehin durch den Markt

731 *Herzog*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 81 (108), Rn. 71.

732 *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 51; *Waiz*, in: Krautscheid/Waiz/Münch, Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, 41 (42); mit Einzelfällen der Daseinsvorsorge wie der lokalen Energie-, Trinkwasser- und Gesundheitsversorgung: *Mehde*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 28, Rn. 237 f.

733 Vgl. *Lange*, NVwZ 2014, 616 (616), Fn 4 ; für die Trinkwasserversorgung vgl. auch explizit als Aufgabe kommunaler Daseinsvorsorge definierend: § 44 Abs. 1 WasserG BW.

734 Zur „Infrastrukturverantwortung [des Bundes] für ein angemessenes überregionales Fernstraßennetz": *Remmert*, in: BeckOK GG, 57. Edition 2024, Art. 90, Rn. 10 m.w.N.

geleistet wird,[735] nicht verpflichtet ist, selbst Daseinsvorsorgeleistungen anzubieten. Es steht dem Gesetzgeber im Rahmen seiner Gestaltungsfreiheit vielmehr grundsätzlich frei, wie das Ziel der Leistungserbringung erreicht werden soll – ob durch eine eigene Bereitstellung oder durch Private[736] (ggf. in Verbindung mit entsprechender staatlicher Förderung und Aufsicht).

Auch das Sozialstaatsprinzip determiniert die Wahl zwischen staatlicher und privater Erbringung nicht: Zwar lässt sich das Sozialstaatsprinzip prinzipiell einfacher umsetzen, wenn eine Infrastruktur in staatlicher Hand ist. Gleichwohl ist dies auch durch eine Regulierung von privaten Akteuren zu erreichen, man denke exemplarisch an die Vorgabe für private als auch öffentlich-rechtliche Banken zum Angebot eines sog. Basiskontos als „elementare, zur Lebensführung notwendige Finanzdienstleistung".[737]

Allerdings gibt es tatsächliche Gründe, aus denen der Staat im Rahmen seiner wirtschaftlichen Betätigungsfreiheit das Angebot der Daseinsvorsorgeleistungen übernehmen kann. Hier ist zunächst zu beachten, dass viele dieser Leistungen durch Netzinfrastrukturen[738] erbracht werden, was eine Reihe von weiteren Besonderheiten mit sich bringt:

Netzinfrastrukturen bilden zunächst regelmäßig *natürliche Monopole*. Dieser ökonomische Begriff bezeichnet Marktsituationen, bei denen ein einzelner Anbieter die Nachfrage kostengünstiger bedienen kann, als bei

735 So greift exemplarisch der Anspruch auf Bereitstellung des Universaldienstes (Telefonie, Internetzugang) nur, soweit dieser aufgrund von Marktversagen nicht angeboten wird: *Kafka/Wilmes-Horváth*, in: Säcker/Körber, Kommentar TKG - TTDSG, 4. Auflage 2023, § 156 TKG, Rn. 5.

736 *Luch/S. E. Schulz*, MMR 2009, 19 (21); In den einzelnen Sektoren können sich indes Unterschiede ergeben: So wird z.B. in Art. 87f Abs. 2 S. 1 GG für den Bereich des Postwesens und der Telekommunikation als Folge der Privatisierungsreform (Postreform II) ausdrücklich eine Erbringung durch private Akteure vorgegeben; ob dies aber -auch in Fällen des Marktversagens- öffentliche Unternehmen per se von der Erbringung ausschließt, ist umstritten, *Möstl*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art 87f, Rn. 36, 58 m.w.N; dagegen besteht im Bereich des Rundfunks (weiterhin) eine Mischform aus öffentlich- und privatrechtlichem Rundfunk: *Luch/Schulz*, a.a.O.

737 BT-Drs. 18/7204, S. 45; *E. Menges*, in: Ellenberger/Bunte, Bankrechts-Handbuch, Rn. 1 ff.

738 siehe zum Begriff der Netzinfrastruktur: *Schulze*, Liberalisierung und Re-Regulierung von Netzindustrien, S. 3.

einer Aufteilung des Marktes unter mehreren Anbietern.[739] Bei Netzinfrastrukturen wie einem Wasser-, Strom oder Schienennetz ist dies naturgemäß der Fall, da diese Netze unter ökonomischen Gesichtspunkten an einem Ort nur einmal errichtet und betrieben werden können.[740] Ein gleichwohl erfolgendes Angebot mehrerer paralleler Netze durch mehrere Konkurrenten verursacht steigende Kosten pro Leistungseinheit, denen kein adäquater Mehrnutzen gegenübersteht, so dass ein solches Angebot weder volkswirtschaftlich noch individualökonomisch zielführend wäre.[741]

Zweitens wirken die *hohen Kosten* beim Aufbau einer solchen Netzinfrastruktur als starke Markteintrittsschranken, so dass private Anbieter diese Kosten initial möglicherweise nicht aufbringen können oder wollen.[742] Hat sich ein Unternehmen zur Investition entschlossen und ist erfolgreich, wirken diese hohen Kosten als Marktzutrittsschranken für spätere Konkurrenten fort und zementieren so eine ggf. entstandene Monopolstellung.[743]

Drittens ist zu beachten, dass diese Monopole bei Netzinfrastrukturen eine *hohe Abhängigkeit* von der kontinuierlichen Versorgung verursachen, da beim Ausfall des Monopolisten zeitnah keine Alternativen zur Verfügung stehen. Im Unterschied zu frei beweglichen Handelswaren können die Kund:innen nicht jederzeit den Anbieter wechseln und sind somit zwingend auf die kontinuierliche Versorgung durch den jeweiligen Netzanbieter angewiesen.

Insofern spricht bzw. sprach jedenfalls ursprünglich für eine staatliche Erfüllung die Überlegung, dass ein natürliches Monopol tendenziell nicht in privater Hand sein sollte, da dies einen ökonomisch motivierten Miss-

739 *Gersdorf*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage 2019, § 9 TKG [a.F.], Rn 25; *Hermes*, in: Schuppert, Der Gewährleistungsstaat, 111 (113 f.); *Knieps*, Wettbewerbsökonomie, S. 23 ff.

740 *Mühlenkamp*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 65 (68); *Hermes*, in: Schuppert, Der Gewährleistungsstaat, 111 (114).

741 Auch Online-Plattformen wie soziale Netzwerke sind v.a. dann erfolgreich, wenn sie möglichst viele Nutzer:innen aufweisen und tendieren deshalb ebenfalls zu natürlichen Monopolen, *Gabriel*, Die Macht digitaler Plattformen, S. 46.

742 *Schulze*, Liberalisierung und Re-Regulierung von Netzindustrien, S. 3 f; vgl. auch *Mühlenkamp*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 65 (68 f.).

743 Vergleichbar wirken bei monopolistischen Anbietern digitaler, personalisierter Dienste vorhandene, große Anzahl an Nutzern (und somit auch an für die Personalisierung nutzbaren personenbezogenen Daten) als Marktzutrittsschranke gegenüber (potenziellen) Konkurrenten, Vgl. BKartA, Beschluss vom 06.02.2019, Az.: B6-22/16, BeckRS 2019, 4895, Rn. 423 ff.

brauch der Monopolstellung zumindest begünstigt.[744] In Staatshand hingegen steht das Monopol unter demokratischer Kontrolle und auch das Sozialstaatsprinzip kann dadurch direkt umgesetzt werden. Weiterhin kann der Umstand hoher Investitionskosten dazu führen, dass diese für einen privaten Akteur nicht zu stemmen bzw. in absehbarer Zeit nicht amortisationsfähig sind, so dass eine flächendeckende, angemessene Versorgung unterbleibt.

Die hohe Kritikalität der (netzgebundenen) Daseinsvorsorgeleistungen spricht hingegen zunächst nur für eine staatliche Erbringung, soweit man dem Staat generell ein höheres Vertrauen bezüglich der kontinuierlichen Leistungserbringung entgegenbringt. Dies ist indes nicht per se gerechtfertigt; allerdings mag sich der fehlende, ökonomische Kostendruck insofern positiv auswirken. Weiterhin kann die Monopoltendenz zumindest auch dazu führen, dass Investitionen in die IT-Sicherheit unterlassen werden. Ein monopolistisches Unternehmen muss bei Ausfällen, auch soweit sie durch IT-Sicherheitsvorfälle hervorgerufen werden, langfristig weniger mit finanziellen Einbußen rechnen (abgesehen von eventuellen Schadensersatzforderungen), da kein Wettbewerbsdruck und somit auch kaum Risiko eines Verlusts an Kund:innen besteht. Insofern existiert möglicherweise kein hinreichender Marktanreiz zur Investition in die IT-Sicherheit.[745] Auch dies spräche insofern für eine staatliche Leistungserbringung, wenn dem nicht auch anders begegnet werden könnte (dazu sogleich).

c. Heutige Gewährleistungsverantwortung

Heute werden die Leistungen der Daseinsvorsorge in vielen Fällen nicht mehr vom Staat selbst erbracht, sondern diese wurden im Laufe der Zeit privatisiert und die Tendenz setzt sich fort.[746] Gleichwohl ist die Daseinsvorsorge auch heute noch als Staatsaufgabe anzusehen.[747] Insoweit stellte schon *Forsthoff* fest, dass eine solche Verschiebung in der tatsächlichen

744 *Mühlenkamp*, in: Hrbek/Nettesheim, Europäische Union und mitgliedstaatliche Daseinsvorsorge, 65 (68 f.).

745 Vgl. *Merz*, in: Nünlist/Thränert, Bulletin 2018 zur schweizerischen Sicherheitspolitik, 73 (77); außerdem im Produktsicherheitsrecht: *H. Tobias Weiß*, Die rechtliche Gewährleistung der Produktsicherheit, S. 36.

746 *Schiller*, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, S. 77.

747 *Luch/S. E. Schulz*, MMR 2009, 19 (20); *Bull*, Der Staat 2008, 1 (6).

Wahrnehmung lediglich einen Wandel in der Art der Verantwortung des Staates für diese Aufgabe auslöst: Von einer originären Erfüllungsverantwortung als Anbieter der Leistungen hat er dann eine *Gewährleistungsverantwortung*,[748] d.h. er muss im Wege der Aufsicht verbunden mit entsprechenden regulierenden Eingriffen[749] gewährleisten, dass die Daseinsvorsorgeleistungen durch Private sicher und zuverlässig angeboten werden.[750] Man kann, soweit ehemals staatlich erbrachte Leistungen privatisiert wurden, auch von einer *Privatisierungsfolgenverantwortung* sprechen.[751]

Der Staat versucht im Rahmen seiner Gewährleistungspflicht die zuvor skizzierten Risiken einer privaten Leistungserbringung durch diverse regulatorische Maßnahmen zu kompensieren.[752] Dies findet in verschiedenen Formen Ausdruck: So wird versucht den Gefahren der Ausnutzung einer Monopolstellung zu begegnen, indem im Rahmen einer Leistung wie etwa der Stromversorgung der Betrieb der Netze und die Stromerzeugung in unterschiedlichen Märkten unterschiedlichen Adressaten zugewiesen wird, um so ein möglichst hohes Maß an Wettbewerb zu ermöglichen. Gleichzeitig wird die weiterhin bestehende Monopolstellung der Netzbetreiber als Schnittstelle im Strommarkt durch die Bundesnetzagentur streng überwacht.

Was die Kontinuität der Leistungserbringung betrifft, so trifft der Staat nun insbesondere die hier gegenständlichen Vorgaben zur IT-Sicherheit der

748 *G. Kirchhof*, AöR 2007, 215 (251); *Bull*, Der Staat 2008, 1 (9 f.); *Schuppert*, in: Schuppert, Der Gewährleistungsstaat, 11, (14, 16); *Königshofen*, Daseinsvorsorge in Zeiten des demographischen Umbruchs, S. 65 ff., 78 ff., der insofern aber auch kritisch darauf hinweist, dass das Modell des Gewährleistungsstaates nicht für alle Sektoren der Daseinsvorsorge (gleichermaßen) geeignet ist.

749 *Luch/S. E. Schulz*, MMR 2009, 19 (21).

750 *Schiller*, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, S. 78, *Pfannkuch*, KommJur 2023, 245 (245); *Krajewski*, VerwArch 2008, 174 (190); vgl. auch: *BVerwG*, Beschluss v. 02.01.2006 – 6 B 55/05 (erhältlich in juris), Rn. 10; ähnlich auch schon: *Forsthoff*, Rechtsfragen der leistenden Verwaltung, S. 45 f.; Nach dem BVerfG kann bei privaten Unternehmen im Bereich der Daseinsvorsorge auch eine verstärkte Grundrechtsbindung vorliegen (Fraport), *BVerfG*, Urt. v. 22.02.2011 – 1 BvR 699/06, NJW 2011, 1201 (1203 f.), Rn. 59.

751 So für die Informations- und Kommunikationsinfrastruktur: *Hoffmann-Riem*, AöR 1998, 513 (525); in diesem Sinne auch: *Gramlich*, CR 1996, 102 (110); generischer: *Schiller*, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, S. 92; *Bauer*, VVDStRL 1995, 243 (278 f.).

752 Insofern drückt sich die Gewährleistungsverantwortung v.a. in einer „Regulierungsverantwortung" aus, *Schuppert*, in: Schuppert, Der Gewährleistungsstaat, 11 (18).

für die Leistungserbringung notwendigen informationstechnischen Systeme.[753] Dies ist wie beschrieben zum einen notwendig, da es, auch aufgrund einer trotz entsprechender Gegenmaßnahmen möglicherweise bestehenden Monopolstellung, ggf. an einem entsprechenden Marktanreiz zur Gewährleistung der IT-Sicherheit fehlt.[754] Mehr noch lässt aber die überragende Bedeutung der Schutzgüter es darüber hinaus unangemessen erscheinen, das Risiko von Ausfällen durch fehlende IT-Sicherheit bis zum Eintritt entsprechender Marktreaktionen hinzunehmen. Insgesamt erfordert somit die Wahrnehmung der Gewährleistungsverantwortung des Staates die Auferlegung von IT-Sicherheitspflichten für die Betreiber kritischer Anlagen, um eine kontinuierliche Versorgung sicherzustellen.

d. Fazit

Für die Daseinsvorsorge als Begriff bei der Bestimmung der Schutzgüter im Bereich kritischer Anlagen kann somit festgehalten werden, dass die kritischen Anlagen unter den deskriptiven Begriff der Daseinsvorsorge[755] fallende Leistungen anbieten, die nach *Forsthoff* der „Versorgung der Bevölkerung mit den nach dem jeweiligen Stand der Zivilisation für eine normale Lebensführung notwendigen Gütern und Dienstleistungen" dienen.

Die Bedeutung der kontinuierlichen Verfügbarkeit dieser Leistungen konnte unter dem Oberbegriff der Daseinsvorsorge auf zwei spezifische Kategorien von Schutzgütern kondensiert werden: Die erste Kategorie bilden dabei die grundrechtlichen Leistungs- sowie Schutzpflichtdimensionen, die in diesem Kontext auch als *Individualrechtsgüter* bezeichnet werden können. Als zweite Kategorie sind insbesondere Gemeinwohlziele zu nennen, die neben Teilen der öffentlichen Sicherheit (dazu sogleich), zu den *Gemeinschaftsrechtsgütern* zu zählen sind.[756] Auch das Sozialstaatsprinzip wirkt mit Blick auf die allgemeine Erschwinglichkeit der Daseinsvorsorgeleistungen auf dieselben ein.

753 Zur Gewährleistung der physischen Sicherheit greift entsprechend das KritisDachG-E: BMI, Referentenentwurf zum KRITIS-DachG, 21.12.2023.

754 Vgl. im Produktsicherheitsrecht: *H. Tobias Weiß*, Die rechtliche Gewährleistung der Produktsicherheit, S. 35.

755 *Schiller*, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, S. 79 m.w.N.

756 Ähnlich von "kollektiven Rechtsgütern" sprechend: *Wolff*, in: Gusy/Kugelmann/Würtenberger, Rechtshandbuch Zivile Sicherheit, 657 (673).

Weiterhin wurde dargestellt, dass der Staat diese Leistungen außer in Fällen des Marktversagens nicht selbst erbringen muss (Gewährleistungs- statt Erfüllungsverantwortung). Allerdings muss er im Rahmen dieser Gewährleistungsverantwortung die kontinuierliche Erbringung der (z.T. ehemals staatlich bereitgestellten) Daseinsvorsorgeleistungen durch Private sicherstellen, um die betroffenen Schutzgüter bedeutenden Ranges zu sichern.

Insgesamt bedeutet dies: Die an kritische Anlagen gerichteten IT-Sicherheitsvorgaben sichern die kontinuierliche Erbringung ihrer Daseinsvorsorgeleistungen, welche wiederrum für den Schutz der genannten *Individual- und Gemeinschaftsrechtsgüter* entscheidend ist. Das Sozialstaatsprinzip verlangt dabei, dass die Leistungen -auch mit den Mehrkosten für die IT-Sicherheit-[757] allgemein erschwinglich bleiben.

2. Öffentliche Sicherheit

Anders als die Daseinsvorsorge, die einen Teilbereich der Leistungsverwaltung umschreibt,[758] ist die öffentliche Sicherheit ein polizeirechtlicher Begriff, mithin ein solcher der Eingriffsverwaltung.[759]

Diese umfasst als Sammelbegriff ebenfalls sowohl gemeinschafts- als auch individualrechtliche Schutzgüter:[760] Die Unversehrtheit der Rechtsordnung (insbesondere die Vorschriften des Strafrechts), die grundlegenden Einrichtungen und Veranstaltungen des Staates und schließlich die Individualrechtsgüter wie Gesundheit, Freiheit und Eigentum der Bürger:innen.[761] Daraus ließe sich zumindest der Schutz der grundlegenden Einrichtungen und Veranstaltungen des Staates als *Gemeinschaftsrechtsgut* im hier gegenständlichen Kontext qualifizieren. Denn auch staatliche Einrichtungen und Veranstaltungen sind auf die Leistungen von (privaten) kritischen Anlagen (Strom, Wasser, etc.) angewiesen.

Der Schutz der Individualrechtsgüter ergibt sich zunächst wie bereits dargestellt zumindest hinsichtlich der Grundrechte schon aus dem Wesen der Dienstleistungen als Teil der Daseinsvorsorge. Dies schließt eine erneute Erfassung als Teil der öffentlichen Sicherheit nicht per se aus,

757 Und auch für die physische Sicherheit nach dem RefE KRITIS-DachG.
758 *H. Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, § 1, S. 7, Rn. 17.
759 Vgl. *H. Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, § 1, S. 9, Rn. 22.
760 *Spannowsky*, in: BeckOK BauordnungsR BW, 27. Edition 2024, § 3 BWLBO, Rn 23.
761 Statt vieler: *Schirmer*, in: BeckOK InfoMedienR, 43. Edition 2024, § 3 IFG, Rn. 119.

zumindest soweit die Beeinträchtigung Folge eines zielgerichteten, menschlichen Handelns (z.B. ein IT-Angriff) und damit einer polizeirechtlich relevanten Handlung ist. Weiterhin ist eine spezielle Betroffenheit aus polizeirechtlicher Perspektive (auch hinsichtlich des Schutzes der objektiven Rechtsordnung) denkbar, wenn es etwa infolge längerfristiger Ausfälle kritischer Dienstleistungen zu mittelbaren Auswirkungen kommt, wie etwa soziale Unruhen[762] in Folge eines längerfristigen Stromausfalls. Schließlich beschränkt sich der Kreis der Individualrechtsgüter hier nicht wie im Rahmen der Daseinsvorsorge hergeleitet auf die grundrechtlichen Positionen, sondern schließt auch einfachrechtliche Positionen wie staatsbürgerliche Rechte, behördliche Erlaubnisse sowie private Rechte mit ein.[763]

Zusätzlich wird in Art. 2 Abs. 2 lit c) NIS2-RL und § 2 Nr. 4 RefE KRITIS-DachG neben der öffentlichen Sicherheit auch die *öffentliche Ordnung* erfasst.[764] Nach nationalem Verständnis ist die öffentliche Ordnung die „Gesamtheit der ungeschriebenen Regeln, deren Befolgung nach den jeweils herrschenden sozialen und ethischen Anschauungen als unerlässliche Voraussetzung eines geordneten menschlichen Zusammenlebens innerhalb eines bestimmten Gebiets angesehen wird".[765] Dieses Gemeinschaftsrechtsgut scheint wie bereits zuvor nur bei sozialen Unruhen o.ä. betroffen sein zu können; auch insoweit erscheint der regulatorische Mehrwert durch diese zusätzliche Erfassung aber überschaubar.

3. Erhalt der Umwelt

Schließlich hat der europäische und in der Folge auch der nationale Gesetzgeber in § 2 Nr. 4 RefE KRITIS-DachG auch den *Erhalt der Umwelt* als zu schützendes Gemeinwohlziel aufgenommen.[766] Obwohl es kein typisches Gemeinwohlziel der Daseinsvorsorge sein dürfte, erscheint es durchaus

762 Vgl. *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (200), der den Zweck der Sicherung kritischer Infrastrukturen auch in der Absicherung „sozialer und politischer Stabilität" sieht.

763 *Trurnit*, in: BeckOK PolR BW, 31. Edition 2023, § 1 PolG, Rn. 34 f.

764 Ursprünglich auch in § 2 Abs. 1 Nr. 21 RefE BSIG übernommen, aber bis zum RegE wieder entfallen.

765 *Depenheuer*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 8, Rn. 166.

766 im RefE KritisDachG als „ökologischer Funktionen oder der Erhaltung der natürlichen Lebensgrundlagen", siehe im Übrigen entsprechend Fn. 764; als Gemeinwohlbelang bezeichnend: *Schuppert*, GewArch 2004, 441 (446).

sinnvoll dieses national in Art. 20a GG als Staatszielbestimmung niedergelegte Schutzgut[767] in den Katalog aufzunehmen. Viele kritische Anlagen wie z.B. Kraftwerke können bei (IT-bedingten) Zwischenfällen erhebliche Umweltschäden hervorrufen. Insofern dient die Gewähr der IT-Sicherheit in diesen Einrichtungen somit faktisch unstreitig auch diesem Schutzgut.

4. Zusammenfassung

Es konnte gezeigt werden, dass bei kritischen Anlagen mit ihren Dienstleistungen verschiedene Schutzgüter betroffen sind. Ausgehend von den in § 2 Nr. 4 RefE KRITIS-DachG und § 2 Nr. 24 RegE BSIG genannten Definitionsbestandteilen kritischer Dienstleistungen[768] (wichtige Bedeutung für das Funktionieren des Gemeinwesens, bei Ausfall oder Beeinträchtigung langfristige Versorgungsengpässe, Gefährdungen für wirtschaftliche Tätigkeiten, öffentliche Sicherheit oder Ordnung, öffentliche Gesundheit) wurden die von kritischen Anlagen erbrachten Leistungen dem deskriptiven Begriff der *Daseinsvorsorge* zugerechnet.

In einem zweiten Schritt konnten dann die konkreten, korrespondierenden Schutzgüter herausgearbeitet werden. Zunächst ist hier der Zugang zum Existenzminimum als Ausprägung der Menschenwürde (Art. 1 Abs. 1 GG) zu nennen, welches folgerichtig durch den Staat auch im Rahmen der Daseinsvorsorge garantiert werden muss. Weiterhin aktiviert der Schutz vor plötzlichen Ausfällen von Daseinsvorsorgeleistungen auch die staatlichen Schutzpflichten aus den Grundrechten. In beiden Fällen handelt es sich um *Individualrechtsgüter*.

Außerdem sind Daseinsvorsorgeleistungen im Rahmen von *Gemeinschaftsrechtsgütern*, hier namentlich den *staatlichen Gemeinwohlzielen*, wie der Sicherstellung der Energie- und Wasserversorgung, der öffentlichen Gesundheit sowie der Wirtschaftsförderung, kontinuierlich zu erbringen sowie (auch angesichts der Mehrkosten durch die IT-Sicherheit) *sozialstaatskonform* auszugestalten.

Der Aspekt der Daseinsvorsorge wird ergänzt durch die ebenfalls in § 2 Nr. 4 KRITIS-DachG-E und § 2 Nr. 24 RegE BSIG genannte *öffentliche Sicherheit*. Diese umfasst neben den schon im Rahmen der Daseinsvorsorge

767 *Calliess*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20a, Rn. 2 ff., 32 ff.

768 Bzw. wesentlicher Dienste nach RKE-RL.

erfassten Grundrechten auch weitere (einfach-rechtliche) Individualrechtsgüter, sowie als Gemeinschaftsrechtsgut die Funktionsfähigkeit der Veranstaltungen und Einrichtungen des Staates. Schließlich wird zusätzlich auch die objektive Rechtsordnung, möglicherweise auch mit Blick auf soziale Unruhen infolge von langfristigen Ausfällen geschützt. Daneben wird mit dem RefE KRITIS-DachG als neues Schutzgut der Erhalt der Umwelt (Art. 20a GG) ergänzt.

Die Schutzgüter aus dem Bereich der Daseinsvorsorge und der öffentlichen Sicherheit werden in nachfolgender Grafik noch einmal zusammengefasst:

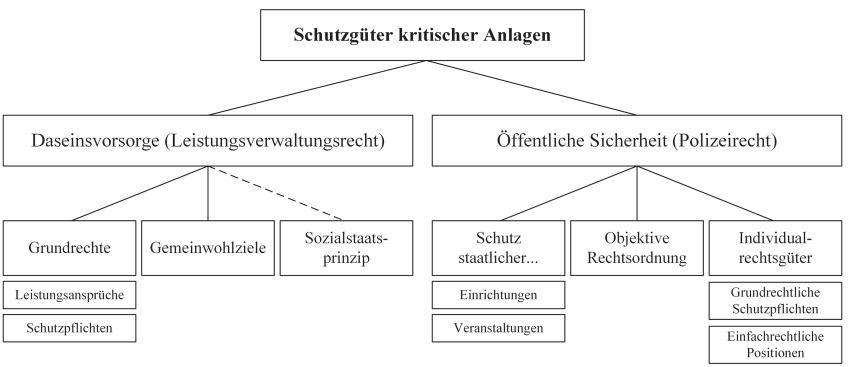

Abbildung 10: Schutzgüter kritischer Anlagen

Ergänzend ist anzumerken, dass auf dieser übergreifenden Ebene des § 30 RegE BSIG, auf der sowohl Unternehmen in kritischen Sektoren (einschl. kritischer Anlagen i.V.m. § 31 Abs. 1 RegE BSIG) als auch in weniger kritischen Sektoren adressiert werden, notwendigerweise Unschärfen hinsichtlich der zu sichernden Schutzgüter entstehen. Im Einzelfall muss deshalb für den jeweiligen Sektor untersucht werden, welche spezifischen Schutzgüter betroffen sind.[769] Teilweise erfolgt dies wie im Energierecht auch durch eine exekutive Konkretisierung (IT-Sicherheitskataloge zu § 11 Abs. 1a bzw. 1b EnWG).[770]

Im Ergebnis legt der Staat den entsprechenden Betreibern kritischer Anlagen mithin Vorgaben zur IT-Sicherheit auf, um durch die Sicherstellung

769 Vgl. in diese Richtung für den Energiesektor: BNetzA, IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG, Aug. 2015, S. 13.

770 Die zugehörigen Regelungen finden sich künftig voraussichtlich in § 5c EnWG.

der kontinuierlichen Erbringung kritischer Dienstleistungen die genannten Schutzgüter[771] zu sichern. Es wurde insofern herausgearbeitet, dass insbesondere bei monopolisierten oder zumindest zu Monopolen neigenden Bereichen der Daseinsvorsorge aufgrund des fehlenden Wettbewerbsdrucks entsprechende Marktanreize zur Investition in die IT-Sicherheit fehlen, so dass eine gesetzliche Vorgabe auch erforderlich ist. Außerdem erlaubt der hohe Rang der betroffenen Schutzgüter kein Zulassen entsprechender Sicherheitsvorfälle, in dessen Folge sich ggf. erst eine marktgetriebene Anpassung entwickeln würde.

III. Schutzgüter digitaler Dienste

Im Folgenden sollen die digitalen Dienste den zuvor beschriebenen Schutzgütern zugeordnet werden. Aus der NIS-RL (EG 48) war dazu nur festzustellen, dass auch die Absicherung digitaler Dienste am Ende der Aufrechterhaltung „wirtschaftlicher und gesellschaftlicher Tätigkeiten" und damit in der Terminologie des (RegE) BSIG der „Funktionsfähigkeit des Gemeinwesens" dient.

Dabei kann zunächst festgehalten werden, dass die tatsächlichen Gründe, die bei klassischen Netzinfrastrukturen für eine Erbringung durch den Staat,[772] zumindest aber für eine durch strenge Regulierung ausgeübte Gewährleistungsverantwortung zur Sicherung der Schutzgüter sprechen, auch bei digitalen Diensten vorliegen: Auch digitale Dienste tendieren insbesondere aufgrund ihrer sehr hohen Zahlen von Nutzer:innen (sowohl auf Kon-

771 Dagegen sollte die IT-Sicherheit nicht selbst als Schutzgut definiert werden (ähnlich auch: *Wischmeyer*, Informationssicherheit, S. 157), da sie wie gezeigt im Kontext des IT-Sicherheitsrechts nur mittelbar notwendig ist, um die Schutzgüter durch die kontinuierliche Erbringung der Daseinsvorsorgeleistungen zu sichern. In diese Richtung als „Staatsaufgabe" definierend aber: *Poscher/Lassahn*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 133 (149), Rn. 48 f.; Eine solches Verständnis übersieht, dass die mit erheblichem Aufwand verbundene Gewährleistung von IT-Sicherheit grundsätzlich Ausdruck der ökonomischen Selbstbestimmung von Unternehmen und Privatpersonen ist, inwieweit sie bereit sind in ihre eigene IT-Sicherheit zu investieren. Nur soweit, wie etwa im hier gegenständlichen Bereich kritischer Anlagen, Individualrechtsgüter Dritter (dies gilt entsprechend für die Datensicherheit) oder Gemeinschaftsrechtsgüter (Schutzgüter) bedroht sind, sind gesetzliche IT-Sicherheitspflichten, die insofern einen erheblichen Eingriff in die Berufs- bzw. unternehmerische Freiheit (Art. 12 GG, Art. 16 GRC) darstellen, zu rechtfertigen.

772 Siehe oben, S. 244 ff.

sumenten- als auch auf Produzentenseite) zu natürlichen Monopolen.[773] Die infolgedessen zu generierende große Menge an personenbezogenen Daten wirkt analog zu den Investitionskosten physischer Netze als Markteintrittsschranke für künftige Mitbewerber.[774] Und schließlich stehen den Nutzer:innen auch bei Ausfall digitaler Dienste kurz- bis mittelfristig keine (gleichwertigen) Alternativen zur Verfügung.

Gleichwohl bestehen auch zwei wesensmäßige, aufeinander aufbauende Unterschiede von digitalen Diensten gegenüber klassischen, kritischen Infrastrukturen (bzw. Anlagen):

Der erste Unterschied besteht darin, dass in klassischen kritischen Infrastrukturen die IT-Systeme der Erbringung einer physischen, kritischen Dienstleistung in einem sog. cyber-physischen System dienen. Der zu schützende Output liegt hier somit in der physischen Leistung (z.B. Strom oder Wasser), nicht in den IT-Systemen und ihren Diensten selbst. Bei digitalen Diensten existiert eine solche physische Leistung hingegen nicht, die kritische Dienstleistung selbst ist hier ebenfalls digitaler Natur.[775] Das bedeutet auch, dass bei den digitalen Diensten eine engere Kopplung zwischen Informationstechnik und den Schutzgütern besteht, da letztere (anders als bei physischen Dienstleistungen) unmittelbar durch informationstechnische Vorfälle beeinträchtigt werden können.

Daraus folgt ein weiterer Unterschied bezüglich der Auslegung der kontinuierlichen Erbringung der kritischen Dienstleistungen. Diese bezieht sich wie bei Strom und Wasser zuvörderst auf das *Ob* der Leistungserbringung; die Qualität, also das *Wie* der Leistung ist eher nachrangig angelegt, stellt sie doch mit Blick auf die Schutzgüter häufig nur ein *Minus* zum völligen Ausfall dar. Anders verhält es sich bei digitalen Diensten, bei denen die Grundrechtsgefährdungen stärker auch durch eine Beeinträchtigung des „Wie" der Leistung, also einer Manipulation des Dienstes entstehen können. Die Qualität der Leistung stellt mithin hier kein *minus* zum Leistungsausfall mehr dar, sondern kann vielmehr zu einer dezidierten Verletzung von Schutzgütern führen.

Beide Beeinträchtigungsformen werden in diesem Abschnitt an den einzelnen Schutzgütern (1. Individualrechtsgüter, 2. Gemeinwohlziele und Sozialstaatsprinzip, 3. Öffentliche Sicherheit) dargestellt.

773 *Gabriel*, Die Macht digitaler Plattformen, S. 46.
774 Siehe S. 246, Fn. 743.
775 Ausführlich dazu später beim Dienstbegriff: S. 279 ff.

1. Individualrechtsgüter

Zunächst ist zu fragen, welche Individualrechtsgüter durch Ausfälle (a.) oder auch Manipulationen (b.) des Dienstes beeinträchtigt sein könnten. Anschließend wird mit Blick auf die Meldepflichten bei Vorfällen noch eine einschränkende Besonderheit beim Schutz der Individualrechtsgüter im RegE BSIG angesprochen (c.).

a. Ausfälle des Dienstes

Grundrechtliche Schutz- oder gar Leistungspflichten lassen sich hinsichtlich der Ausfälle digitaler Dienste auf den ersten Blick weniger eindeutig darstellen als etwa mit Blick auf Leben und Gesundheit bei einem Ausfall der Trinkwasserversorgung.

Selbst mit Blick auf spezifische Informationsgrundrechte sind Verletzungen derselben zumindest durch komplette Ausfälle der digitalen Dienste schwer zu begründen. Exemplarisch sei etwa auf die Informationsfreiheit nach Art. 5 Abs. 1 S. 1 Alt. 2 GG verwiesen: Da dieses Grundrecht nur die „ungehinderte Unterrichtung aus allgemein zugänglichen Quellen" umfasst, nicht aber ein „allgemeines Recht auf Zugang zu Informationen" beinhaltet,[776] ist bei einem kompletten Ausfall einer Online-Suchmaschine oder eines sozialen Netzwerks schon eine Betroffenheit des Schutzbereichs eher fernliegend.[777]

Denkbar sind dagegen Beeinträchtigungen der beruflichen bzw. unternehmerischen Freiheit (Art. 12 GG, Art. 16 GRC) von Unternehmen, die etwa in Suchmaschinen gelistet sind, auf Online-Marktplätzen ihre Produkte anbieten oder auf sozialen Netzwerken auftreten.

b. Manipulationen des Dienstes

Hinsichtlich der Manipulation des Dienstes, mithin dem *Wie* der Diensterbringung, ergibt sich jedoch ein anderes Bild. Insofern ist es für die

776 *Grabenwarter*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 5, Rn 996, 1021.

777 Lediglich ein „Mindestbestand an Informationsquellen" muss sichergestellt werden; *Grabenwarter,* a.a.O., Rn. 1022, dies dürfte aber auch bei Ausfall der genannten Dienste noch der Fall sein.

Schutzgüter weniger entscheidend, dass der Dienst überhaupt verfügbar, d.h. online erreichbar ist, sondern v.a. ob er in der aktiven Erbringung die Rechte der Nutzer:innen hinreichend wahren kann.

Denkbar ist bei allen digitalen Diensten, dass hier insbesondere deren Funktionsweisen unerkannt manipuliert und so Grundrechte wie etwa die Diskriminierungsfreiheit beeinträchtigt werden. Soweit durch IT-Angriffe entweder Inhalte nachträglich gelöscht oder beim Hochladen blockiert werden, könnte außerdem die Meinungsäußerungsfreiheit betroffen sein.[778] Eine Veröffentlichung von Informationen unter falschem Namen (etwa durch Diebstahl der Login-Daten von sozialen Netzwerken) betrifft das Recht auf informationelle Selbstbestimmung bzw. das Datenschutzgrundrecht. Hinsichtlich der Angebotsseite an Informationen bei Online-Suchmaschinen und sozialen Netzwerken kann durch unerkannte Manipulationen (auch mit Blick auf die Personalisierung) die Informationsfreiheit betroffen sein.[779] Möglicherweise noch stärker als durch einen Ausfall beeinträchtigt werden können etwa Unternehmen in ihrer beruflichen bzw. unternehmerischen Freiheit (Art. 12 GG, Art. 16 GRC) durch entsprechende manipulative Benachteiligungen ihrer Einträge in Suchmaschinen, ihrer Produkte auf Online-Marktplätzen oder ihren Seiten in sozialen Netzwerken.

c. Eingeschränkter Schutz von Individualrechtsgütern im IT-Sicherheitsrecht

Diese Individualgrundrechte lassen sich grundsätzlich alle als Schutzgüter digitaler Dienste definieren, da die gesetzlich geforderte Gewährleistung von IT-Sicherheit auch der Sicherung dieser Individualgrundrechte dient. Allerdings ist darauf hinzuweisen, dass eine Verletzung derselben aufgrund

778 Vgl. zur Beeinträchtigung der Meinungsfreiheit durch Nicht-Veröffentlichung bzw. Löschung durch die Plattform: *Raue*, JZ 2018, 961 (964 ff.); diese Schutzpflicht muss, um einen umfassenden Grundrechtsschutz zu gewährleisten, auch dann greifen, wenn die Nicht-Veröffentlichung bzw. Löschung durch einen IT-Angriff auf den digitalen Dienst ausgelöst wird.

779 Anders als der Ausfall eines entsprechenden Dienstes, der insofern nur das Informationsangebot einschränkt führt die Manipulation zu einer „Verzerrung" des Informationsraums, der gegenüber somit eine grundrechtliche Schutzpflicht anzunehmen ist; *Grabenwarter*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 5, Rn. 1028; wohl auch *Schillmöller*, InTer 2020, 150 (152); vgl. außerdem zum Prinzip der Netzneutralität: *Hain*, AfP 2012, 313 (319 f., 325 f.).

des Fokus' des IT-Sicherheitsrechts auf Gemeinwohlziele einfach-rechtlich mitunter nur dann zum Tragen kommt, wenn entweder besonders viele Nutzer:innen oder einzelne Nutzer:innen besonders schwer betroffen sind.

Im Rahmen der Meldepflichten nach § 32 Abs. 1, 3 i.V.m. § 2 Nr. 11, 40 RegE BSIG liegt zunächst generisch (für alle adressierten Einrichtungen) ein erheblicher Sicherheitsvorfall u.a.[780] dann vor, wenn der Sicherheitsvorfall „natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann". Nach Art. 3, 11-13 der zugehörigen DVO[781] insbesondere auch für die hier gegenständlichen digitalen Dienste sind diese Voraussetzungen u.a. dann erfüllt, wenn ein digitaler Dienst einerseits für mehr als 5% oder 1 Million Nutzer:innen (je nach dem was kleiner ist) infolge eines Sicherheitsvorfalls ganz oder teilweise nicht verfügbar ist oder in seiner Verfügbarkeit hätte beeinträchtigt werden können (Art. 11-13, jeweils lit a) und b) DVO), mithin besonders viele Personen betroffen hat bzw. hätte.

Andererseits ist die Erheblichkeit u.a. auch dann zu bejahen, wenn der Sicherheitsvorfall bei einem digitalen Dienst zum Tod oder zu einer schwerwiegenden Gesundheitsbeeinträchtigung einer Person geführt hat oder hätte führen können (Art. 3 lit c), d) DVO), d.h. wenn einzelne Personen besonders schwer betroffen sind.

Unterhalb dieser Schwelle sind Vorfälle aber folglich nicht meldepflichtig und dürften somit nach dem RegE BSIG zumindest keine rechtlichen Konsequenzen auslösen. Allerdings kann und muss die Gewährleistung der IT-Sicherheit natürlich auch bereits unterhalb dieser Schwelle die Risiken für diese Individualgrundrechte reduzieren.

Zusammenfassend offenbart sich mit der Adressierung der digitalen Dienste die schon bei der Entwicklung des BSIG aufgezeigte Tendenz, dass sich dieser europarechtliche Regulierungsansatz weiter vom ursprünglichen Begriff der Daseinsvorsorge im Sinne der Gewährleistung von Leistungen, die für ein normales Leben notwendig sind oder sogar das Existenzminimum darstellen, entfernt. Es bleibt somit nicht mehr bei elementaren Grundrechten wie dem Recht auf Leben und Gesundheit oder mit Blick auf die wirtschaftliche Betätigung der beruflichen bzw. unternehmerischen

780 Alternativ auch dann, wenn er „schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann".

781 Durchführungsverordnung (DVO) 2024/2690 der EU-Kommission vom 17.10.2024 nach Art. 21 Abs. 5, UAbs. 1, Art. 23 Abs. 11 NIS2-RL. Siehe im nationalen Recht §§ 30 Abs. 3, 56 Abs. 5 RegE BSIG.

Freiheit. Vielmehr werden wie dargestellt insbesondere mit den Kommunikationsgrundrechten sowie dem Gleichheitsgrundsatz andere Grundrechte verstärkt in den Blick genommen.

2. Gemeinwohlziele und Sozialstaatsprinzip

Weiterhin ist fraglich welche Gemeinwohlziele von digitalen Diensten betroffen sein können und ob auch hier das Sozialstaatsprinzip Auswirkungen hat.

Bislang dürften der Bereitstellung etwa einer Suchmaschine und eines sozialen Netzwerks noch keine spezifischen, allgemein anerkannten Gewährleistungspflichten gegenüberstehen, wie etwa bei der Sicherstellung der Energieversorgung. Und das obwohl beide Dienste inzwischen möglicherweise bereits als unverzichtbarer Bestandteil der modernen Lebensführung und damit als Teil der Daseinsvorsorge zu qualifizieren sein könnten.[782]

Allerdings kommt das Gemeinwohlziel der *Wirtschaftsförderung*[783] auch bei digitalen Diensten als wichtiges Schutzgut in Betracht. Viele Unternehmen sind wie bereits individualrechtlich beschrieben in erheblicher Weise von der Funktionsfähigkeit der digitalen Dienste wie der Online-Suchmaschinen, der Online-Marktplätze oder der sozialen Netzwerke abhängig, so dass erneut nicht zuletzt aufgrund des Monopolcharakters dieser Dienste eine Beeinträchtigung des Gemeinwohlziels der Wirtschaftsförderung bedeutend erscheint.[784] Dies gilt sowohl für einen vollständigen Ausfall als auch die Manipulation der Dienste.

Mit Blick auf die Manipulation in sozialen Netzwerken als auch in Online-Suchmaschinen kommt als weiteres Gemeinwohlziel auch die *öffentliche Meinungsbildung*[785] in Betracht. Sie wird aus „den verfassungs-

782 In diese Richtung als „eDaseinsvorsorge" u.a. mit Blick auf soziale Netzwerke *Luch/S. E. Schulz*, MMR 2009, 19 (23).

783 Siehe oben S. 238 f.

784 Vgl. EG 48

785 *Mitsch*, DVBl 2019, 811 (811 f.); im Kontext der Pressefreiheit als „öffentliche Meinung": *BVerfG*, Teilurteil v. 05.08.1966 – 1 BvR 586/62, 610/63, 512/64, NJW 1966, 1603 (1604); *Grabenwarter*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 5, Rn. 6; ähnlich mit Blick auf die Informationsfreiheit als Grundlage zur Meinungsbildung: *Koreng*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 245 (247); teilweise auch als „Meinungspluralität": *Müller-Terpitz*, ZUM 2020, 365 (367); *Pille*, Meinungsmacht sozialer Netzwerke, S. 204.

rechtlichen Wertentscheidungen in Art. 5 Abs. 1 GG bzw. Art. 11 GRC" abgeleitet"[786]; Art. 5 Abs. 1 GG enthält insoweit nicht nur individuelle Grundrechte, sondern auch die öffentliche Meinungsbildung als ein „objektives Prinzip der Gesamtrechtsordnung".[787] Dabei ist eine freie Meinungsbildung in einem ungestörten, pluralen Diskurs für eine demokratische Gesellschaft konstitutiv,[788] so dass die öffentliche Meinungsbildung zugleich auch aus dem Demokratieprinzip (Art. 20 Abs. 1, 2 GG, Art. 2 EUV) abgesichert wird.[789]

V.a. die sozialen Netzwerke schaffen einen alle Lebensbereiche umfassenden „öffentlichen Kommunikationsraum",[790] in dem dieser Diskurs auch und gerade mit der „Verbreitung von politischen Programmen und Ideen"[791] zunehmend stattfindet. Gleichzeitig geht die Bedeutung von Rundfunk und Presse in diesem Diskurs zurück,[792] was den Diskurs in sozialen Netzwerken umso gewichtiger erscheinen lässt.

Ebendieser Diskurs und damit das Gemeinwohlziel der öffentlichen Meinungsbildung kann neben den intrinsischen Gefährdungen durch die personalisierten Inhalte (*Filterblasen*)[793] insbesondere auch durch die hier gegenständlichen manipulativen Angriffe auf soziale Netzwerke bedroht werden, wodurch etwa Inhalte einer bestimmten politischen Richtung oder aber auch Falschinformationen („Fakenews") sowie volksverhetzende Inhalte stärker empfohlen werden.[794] Dieses Gefährdungspotential besteht auch bei Online-Suchmaschinen, die mit ihrer Funktion des Filterns und des Rankings von Suchergebnissen den faktisch verfügbaren Informations-

786 *Müller-Terpitz*, ZUM 2020, 365 (367); *Pille*, Meinungsmacht sozialer Netzwerke, S. 204; *Holznagel*, ZUM 2020, 1 (4).

787 *BVerfG*, Urt. v. 16.06.1981 – 1 BvL 89/78, NJW 1981, 1774 (1775); *BVerfG*, Beschluss v. 09.10.1991 – 1 BvR 221/90, NJW 1992, 1442 (1443); *BVerfG*, Urt. v. 15.01.1958 – 1 BvR 400/57, NJW 1958, 257 (258); zur grundrechtliche Schutzpflicht in diesem Zusammenhang: *Grabenwarter*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 5, Rn. 109.

788 *BVerfG*, Urt. v. 15.01.1958 – 1 BvR 400/51, GRUR 1958, 254 (256); ähnlich auch: *Holznagel*, ZUM 2020, 1 (4).

789 Vgl. *Müller-Terpitz*, ZUM 2020, 365 (367).

790 *OLG Dresden*, Beschluss v. 08.08.2018 – 4 W 577/18, MMR 2018, 756 (759), Rn. 19.

791 *BVerfG*, Beschluss v. 22.05.2019 – 1 BvQ 42/19, ZUM-RD 2019, 429 (430 f.), Rn 19.

792 *Mitsch*, DVBl 2019, 811 (814).

793 Zur Definition siehe Fn. 635; *Schillmöller*, InTer 2020, 150 (150 f.); s. außerdem: *G. Wagner/Eidenmüller*, ZfPW 2019, 220 (235); *Paal/Hennemann*, JZ 2017, 641 (641, 644); *Mitsch*, DVBl 2019, 811 (812).

794 Vgl. zu dem verwandten Problem der „Social-Bots": *Milker*, ZUM 2017, 216 (216 f.).

raum bestimmen und somit einen starken Einfluss auf die öffentliche Meinungsbildung ausüben können.[795]

Eine Beeinträchtigung des Sozialstaatsprinzips ist im Rahmen der IT-Sicherheit digitaler Dienste hingegen aufgrund der jedenfalls monetären Kostenlosigkeit derselben nicht ersichtlich. Gleiches gilt für den Erhalt der Umwelt.

3. Öffentliche Sicherheit

Schließlich wurde in Art. 4 Abs. 1 lit. c) der DVO 2018/151[796] auch explizit ein „Risiko für die öffentliche Sicherheit" als Fall einer erheblichen Auswirkung genannt. Zwar erscheint die öffentliche Sicherheit bei einem Ausfall bzw. einer Beeinträchtigung z.B. einer Suchmaschine weitaus weniger gefährdet als etwa bei einem flächendeckenden Stromausfall. Im Einzelnen erscheint aber zumindest die Einschränkung der Funktionsfähigkeit der Einrichtungen des Staates plausibel, da staatliche Einrichtungen (ggf. auch mit sog. e-Government-Leistungen[797]) möglicherweise über Online-Suchmaschinen zugänglich sein müssen. Auch können die zuvor genannten Manipulationsangriffe zur Verbreitung rechtswidriger Inhalte (Fake News, Beleidigungen, Verleumdungen) in sozialen Netzwerken und Online-Suchmaschinen sowohl die objektive Rechtsordnung als auch Individualrechtsgüter verletzen.

4. Fazit

Insgesamt ist mit Blick auf digitale Dienste festzuhalten, dass die Schutzgüter im Vergleich zu kritischen Anlagen hier entweder weniger stark exponiert sind oder z.T. auch gänzlich andere Schutzgüter in Betracht kommen. Ihre Bedeutung als (möglicher) Bestandteil der (digitalen) Daseinsvorsorge

795 Vgl. *Paal/Hennemann*, JZ 2017, 641 (641, 643); von einer insoweit bedenklichen Gatekeeper-Funktion sowohl von Online-Suchmaschinen als auch sozialen Netzwerken ausgehend: *Koreng*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 245 (249).

796 Vorgängervorschrift der DVO 2024/2690 zur NIS-RL. In der neuen DVO zur NIS2-RL ist die öffentliche Sicherheit hingegen nicht mehr genannt.

797 Dies meint die Digitalisierung von Verwaltungsleistungen mit einem entsprechenden Online-Zugang für die Bürger:innen und Bürger, Vgl. *Prell*, NVwZ 2018, 1255 (1255 ff.).

ist zumindest wesentlich geringer, ebenso wie mögliche Verletzungen der öffentlichen Sicherheit. Allerdings nehmen sie ähnlich wie klassische, kritische Netzinfrastrukturen Schlüsselpositionen innerhalb der Gesellschaft ein. Besonders hervorzuheben ist insoweit die Schlüsselfunktion von sozialen Netzwerken und Online-Suchmaschinen als zentrale Informations- und Meinungsplattformen mit in der Folge hohem Beeinträchtigungspotential für entsprechende Gemeinwohlziele (öffentliche Meinungsbildung) und Individualgrundrechte (Informationsfreiheit, Meinungsäußerungsfreiheit). Auch Verletzungen der öffentlichen Sicherheit sind möglich. Gleichzeitig sind viele Unternehmen und damit mittelbar auch Bürger:innen in ökonomischer Hinsicht von allen drei digitalen Diensten abhängig (Wirtschaftsförderung, berufliche und unternehmerische Freiheit).

In den genannten Schlüsselfunktionen unterscheiden sich digitale Dienste auch von anderen wichtigen Einrichtungen (z.B. im Maschinen- und Fahrzeugbau), bei denen im Wesentlichen nur die ökonomische Bedeutung im Vordergrund steht. D.h. bei digitalen Diensten folgt ihre Kritikalität für die Schutzgüter aus ihrem spezifischen Dienstangebot; dagegen kommt es bei den anderen genannten wichtigen Einrichtungen gerade nicht auf ihre spezifische Tätigkeit an, sondern nur noch auf die abstrakte volkswirtschaftliche Bedeutung des Unternehmens.

Digitale Dienste stehen somit hinsichtlich ihrer Kritikalität und der damit verbundenen, erforderlichen Regulierungsintensität *in der Mitte zwischen kritischen Anlagen sowie den genannten anderen wichtigen Einrichtungen.* Sie sind zwar wie beschrieben anders als letztgenannte mit ihrem spezifischen Dienstangebot noch kritisch für ebenfalls spezifische, hochrangige Schutzgüter, aber in etwas weniger ausgeprägtem Maße wie dies bei kritischen Infrastrukturen der Fall ist.[798] Dieser Unterschied zwischen digitalen Diensten und anderen wichtigen Einrichtungen bildet sich indes im RegE BSIG nicht explizit ab, sondern muss folglich über die Angemessenheit der Maßnahmen im Einzelfall (dazu später auf S. 293 ff.) berücksichtigt werden.

B. Systematische Beschreibung der gesetzlichen IT-Sicherheitsvorgaben

Im Nachfolgenden sollen die im RegE BSIG vorzufindenden Sicherheitsvorgaben genauer beleuchtet werden. Sie stellen im Sinne der gegenständ-

798 Vgl. EG 60 NIS-RL, wonach Anbieter digitaler Dienste aufgrund der „Art ihrer Dienste und Tätigkeiten" weniger strikt beaufsichtigt werden sollen.

lichen Untersuchung die Systematik des Gesetzes dar, in die sich die *Resilienz* bei einer Übertragung in den RegE BSIG einfügen müsste.

Dabei wird zunächst auf die IT-Sicherheit und die Schutzziele eingegangen (I.). In einem zweiten Schritt (II.) werden die Bestandteile der Informationstechnik, d.h. v.a. Systeme, Dienste und Daten bzw. Informationen beleuchtet. Schließlich werden unter III. die Begriffe Risiko und Angemessenheit sowie die Risikomethodik beschrieben.

I. IT-Sicherheit und Schutzziele

Aus der Gesamtschau des RegE BSIG sowie aus der Nennung in § 30 Abs. 2 S. 2 Nr. 3 RegE BSIG ist zu entnehmen, dass durch entsprechende Maßnahmen der adressierten Einrichtungen eine (angemessene) *Sicherheit in der Informationstechnik (IT-Sicherheit)* gewährleistet werden soll. Fraglich ist insofern wie die IT-Sicherheit zu definieren ist (1.). Im Weiteren wird dann noch genauer auf die einzelnen Schutzziele aus der Definition eingegangen (2., 3.)

1. IT-Sicherheit

Insgesamt bestehen im einschlägigen Rechtsrahmen drei mögliche Definitionen von IT-Sicherheit, die in Betracht kommen.

Zunächst besteht in § 2 Nr. 39 RegE BSIG eine nationale, unverändert aus § 2 Abs. 2 S. 4 BSIG[799] übernommene Definition der „*Sicherheit in der Informationstechnik*“: „Die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“

Die NIS2-RL verwendet bei den Legaldefinitionen in Art. 6 hingegen den Begriff der *Sicherheit von Netz- und Informationssystemen*, der nach Art. 6

799 § 2 Abs. 2 S. 1-3 BSIG sind kein Teil der Definition, sondern haben lediglich erläuternde Funktion: *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 2 BSIG, Rn. 5.

Nr. 2 NIS2-RL definiert wird als „die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können."

Schließlich definiert § 30 Abs. 1 RegE BSIG implizit selbst die von den besonders wichtigen und wichtigen Einrichtungen zu gewährleistende IT-Sicherheit, wonach diese Einrichtungen technische und organisatorische Maßnahmen ergreifen müssen, um *Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse*, zu vermeiden.[800]

Fraglich ist somit, welches Verständnis von IT-Sicherheit in der Pflichtennorm des § 30 Abs. 1, 2 BSIG zugrunde gelegt werden soll; alle drei genannten Vorschriften definieren die zu gewährleistende IT-Sicherheit mit teilweise unterschiedlichen *Schutzzielen* und insbesondere unterschiedlichen *Schutzobjekten*:

800 Art. 21 Abs. 1 NIS2-RL verweist hingegen an dieser Stelle auf die „Sicherheit der Netz- und Informationssysteme".

<table>
<tr><th>§ 2 Nr. 39 RegE BSIG</th><th>§ 30 Abs. 1 S. 1 RegE BSIG</th></tr>
<tr><td>(2) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen
1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.</td><td rowspan="3">Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen […] zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden […]</td></tr>
<tr><th>Art. 6 Nr. 2 NIS2-RL</th></tr>
<tr><td>„Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können;</td></tr>
</table>

Abbildung 11: IT-Sicherheitsdefinitionen nach RegE BSIG und NIS2-RL

Die Unterschiede im Einzelnen sind:

- In der NIS2-RL wird zusätzlich zu den klassischen Schutzzielen auch die Authentizität genannt.
- Die Definition der NIS2-RL bezieht die Schutzziele auf *Daten* und *Dienste*, jene des § 2 Nr. 39 RegE BSIG nur auf *Informationen* und jene des § 30 Abs. 1. S. 1 RegE BSIG auf *Systeme, Komponenten und Prozesse*. Insbesondere der Unterschied innerhalb des RegE BSIG ist frappierend, da die Systeme, Komponenten und Prozesse zwar auch in der Sicherheitsdefinition des RegE BSIG vorkommen, aber in anderer Funktion: nicht als Schutzobjekt, sondern (nur) als Träger der Sicherheitsvorkehrungen/Maßnahmen.
- Nur die NIS2-RL kennt das zusätzliche Element des „*bestimmten Vertrauensniveaus*“.

Die Frage nach der einschlägigen Definition der IT-Sicherheit ist daher alles andere als trivial und soll wie folgt beantwortet werden:

Schon nach der bisherigen Rechtslage ist die Definition der IT-Sicherheit aufgrund der Unterschiede zwischen BSIG und NIS-RL schwierig.[801] Besonders herausfordernd ist künftig insbesondere, dass der *RegE BSIG in sich nicht (mehr) konsistent ist.* Die Sicherheitsdefinition als prägendes Merkmal des IT-Sicherheitsrechts und insbesondere seiner Pflichtennormen muss eindeutig dahingehend zu bestimmen sein, welche Schutzziele sie adressiert und worauf sich diese Schutzziele beziehen. Nicht nur das die *Authentizität* im RegE BSIG fehlt; es ist insbesondere völlig unklar, ob die Systeme, Komponenten und Prozesse nun wie in § 2 Nr. 39 RegE BSIG nur Maßnahmenträger oder wie in § 30 Abs. 1 S. 1 RegE BSIG auch selbst Schutzobjekt sein sollen. Am Ende sind darüber hinaus beide Definitionen nicht mit jener des Art. 6 Nr. 2 NIS2-RL in Übereinstimmung zu bringen. Weder die in unterschiedlichen Normen jeweils für sich stehenden „Informationen" noch die „Systeme, Komponenten und Prozesse" lassen sich entsprechend der NIS2-RL als „Daten oder Dienste" auslegen.[802]

An dieser Stelle dürfte somit gegenüber der NIS2-RL die Wortlautgrenze erreicht und § 30 Abs. 1 RegE BSIG hinsichtlich der zu gewährleistenden IT-Sicherheit *nicht mehr richtlinienkonform auszulegen*[803] sein. Auch der Erfolg einer richtlinienkonformen Rechtsfortbildung[804] ist zweifelhaft:

Fraglich wäre hier auf der Voraussetzungsebene zunächst, ob der Gesetzgeber bewusst ein von der Richtlinie abweichendes Regelungskonzept

801 In § 8c Abs. 1 BSIG wird auf die Risiken für die „Sicherheit der Netz- und Informationssysteme" abgestellt, gleichzeitig bestand besteht die Definition der Sicherheit in der Informationstechnik in § 2 Abs. 2 BSIG. Auch hier konnte zur Lösung bereits auf den europäischen Sicherheitsbegriff abgestellt und die unpassende nationale Definition außer Acht gelassen werden; zumindest hinsichtlich der Schutzziele ebenso: *Buchberger*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 8c BSIG, Rn 2; *Schallbruch*, CR 2016, 663 (668). Auch die Bestimmung des § 8a BSIG war nicht mit § 2 Abs. 2 BSIG kompatibel.

802 In der Definition des Art. 6 Nr. 2 NIS2-RL steht „Daten oder Dienste", d.h. auch in der nationalen Umsetzung der IT-Sicherheitsdefinition müssten ebenfalls beide Alternativen genannt werden, um den Inhalt der Definition vollständig wiederzugeben.

803 Zum Gebot der richtlinienkonformen Auslegung: *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der europäischen Union, 80. EL 2023, Art. 288 AEUV, Rn. 133 ff.; *Wietfeld*, JZ 2020, 485 (485 ff.).

804 Zur Unterscheidung zwischen Auslegung und Rechtsfortbildung im nationalen Recht: *Wiedemann*, NJW 2014, 2407 (2407 f.) m.w.N.; wobei unter den europarechtlichen Begriff der „richtlinienkonformen Auslegung" nach nationalem Verständnis sowohl die Auslegung als auch die Rechtsfortbildung fallen, *Wietfeld*, JZ 2020, 485 (488 f.); *Roth/Jopen*, in: Riesenhuber, Europäische Methodenlehre, 377 (429), Rn. 51.

verfolgt.[805] Dies verneinend könnte sodann inhaltlich entweder argumentiert werden, dass in einer Analogie neben „Informationen" auch das Angebot der Informationsverarbeitung durch einen Dienst[806] von § 2 Nr. 39 RegE BSIG erfasst sein und außerdem die Authentizität (ggf. als Teil der Integrität)[807] ergänzt werden müsste. In der Folge müsste man dann weiterhin davon ausgehen, dass § 30 Abs. 1 S. 1 RegE BSIG keine eigenständige Definition der IT-Sicherheit begründen, sondern auf die so umgedeutete allgemeine Definition verweisen wollte.[808] Alternativ könnte man (unter Außerachtlassung der Sicherheitsdefinition in § 2 Nr. 39 RegE BSIG) in § 30 Abs. 1 RegE BSIG die „Systeme, Komponenten und Prozesse" als „Daten" (ggf. als teleologisch reduzierter Bestandteil von Systemen) und Dienste (am ehesten dem „Prozess" entsprechend) interpretieren bzw. umdeuten.[809]

Lehnt man auch eine solche Rechtsfortbildung ab, müsste die somit zur NIS2-RL im Widerspruch stehende Regelung im RegE BSIG grundsätzlich entsprechend dem Willen des Gesetzgebers bis auf weiteres angewendet werden.[810] Allerdings muss der Staat auch bei öffentlich-rechtlichen Pflichtennormen wie dem hiesigen § 30 RegE BSIG die Vorgaben der Richtlinie *zugunsten des Normadressaten* (was fraglich sein dürfte)[811] gegen sich gelten

805 Ist dies der Fall, ist eine richtlinienkonforme Rechtsfortbildung ausgeschlossen: *Roth/Jopen*, in: Riesenhuber, Europäische Methodenlehre, 377 (440 f.), Rn. 64, m.w.N. Der Gesetzgeber verfolgt mit seiner Definition der „Sicherheit in der Informationstechnik" bereits seit längerem ein eigenes begriffliches Regelungskonzept (siehe Fn. 801), ohne dass aber eindeutig wäre, ob er hiermit tatsächlich auch eine unterschiedliche Rechtsfolge bewirken will. Daneben darf wohl mit Blick auf § 30 Abs. 1 RegE BSIG eindeutig davon ausgegangen werden, dass Widersprüche zwischen den Definitionen eines Gesetzes und seinen Pflichtennormen schon als innergesetzliche, systematische Brüche stets planwidrig sind.

806 Siehe zur Dienstdefinition sogleich, S. 279 ff.

807 So auch BReg, Entwurf NIS2UmsuCG, 22.07.2024, S. 138; ausführlich sogleich auf S. 271.

808 Dagegen spricht aber, dass diese Divergenz zwischen Definition und Pflichtennorm wie bereits in Fn. 801 beschrieben auch schon in früheren Gesetzesfassungen bestand.

809 Zur Auslegung von Systemen, Komponenten und Prozessen sogleich, S. 273 ff.

810 Vgl. hierzu: *BGH*, Urt. v. 18.11.2020 – VIII ZR 78/20, NJW 2021, 1008 (1010 ff.), Rn. 22 ff., 46; ggf. müsste der Gesetzgeber dann (nach einem Vorabentscheidungsverfahren des EuGHs) die Vorschrift ändern, um ein Vertragsverletzungsverfahren zu vermeiden.

811 Siehe zu dieser Voraussetzung: *Roth/Jopen*, in: Riesenhuber, Europäische Methodenlehre, 377 (394 f.), Rn 14; *EuGH*, Urt. v. 08.10.2020 – C-568/19, BeckRS 2020, 25750, Rn. 34 ff.; *EuGH*, Urt. v. 27.02.2014 – C-351/12, ZUM 2014, 395 (398), Rn. 47; *EuGH*, Urt. v. 24.01.2012 – C-282/10, NZA 2012, 139 (142), Rn. 37; die Frage der

lassen (sog. Direktwirkung), da er sich treuwidrig verhielte, wenn er sich als der zur (widerspruchsfreien) Umsetzung Verpflichtete auf die richtlinienwidrige Fassung berufen würde.[812]

Die mit den genannten Aspekten verbundenen und tiefer in die europäische Rechtsprechung und Methodenlehre eintauchenden Detailfragen sollen hier insbesondere aufgrund des Stadiums der Umsetzung der NIS2-RL (als Regierungsentwurf des NIS2UmsuCG, zu dem auch das BSIG gehört) nicht weiter untersucht werden. Im Ergebnis wird deshalb diese Fragen auslassend vom Ergebnis her gedacht davon ausgegangen, dass innerhalb der Pflichtennorm des § 30 Abs. 1 RegE BSIG ein richtlinienkonformes Verständnis von der IT-Sicherheitsdefinition zugrunde zu legen ist; verbunden mit der Hoffnung, dass der nationale Gesetzgeber den RegE BSIG bis zur Verabschiedung in diesem Punkt noch einmal revidiert.

Als Antwort auf die Frage wie die IT-Sicherheit für die Normadressaten des § 30 Abs. 1 RegE BSIG richtlinienkonform zu definieren ist, gilt somit im Ergebnis:

> Die Normadressaten müssen Störungen der Sicherheit der Netz- und Informationssysteme[813], *d.h. die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden, vermeiden,* indem sie die Netz- und Informationssysteme (durch technische und organisatorische Maßnahmen) befähigen, auf einem be-

Sicherheitsdefinition innerhalb der Pflichtennorm dürfte an sich rechtlich neutral sein, was man ggf. einer Wirkung zugunsten des Normadressaten gleichstellen könnte. Die Anwendung der Richtliniendefinition würde darüber hinaus zumindest faktisch zugunsten des Normadressaten wirken, da so insbesondere die fehlende Kohärenz innerhalb des BSIG überwunden und Rechtssicherheit hergestellt werden würde. Schließlich dürfte aus diesem Ansatz folgen, dass der Staat dem Normadressaten, der die IT-Sicherheit nach der NIS2-RL gewährleistet hat, nicht sein richtlinienwidriges Verständnis von IT-Sicherheit entgegenhalten darf.

812 Vgl. *Gundel*, in: Pechstein/Nowak/Häde, Frankfurter Kommentar zu EUV, GRC und AEUV, 2. Auflage 2023, Art. 288 AEUV, Rn. 39, 48 ff.; *Wank*, Juristische Methodenlehre, S. 274, Rn. 136; *EuGH*, Urt. v. 14.07.1994 – Rs. C-91/92, NJW 1994, 2473 (2474), Rn. 23; grundlegend: *EuGH*, Urt. v. 05.04.1979 – Rs 148/78, NJW 1979, 1764 (1765).

813 Anstelle der „Netz- und Informationssysteme" mag man auch den nationalen Begriff der „informationstechnischen Systeme, Komponenten und Prozesse" verwenden, dazu unter 3.

stimmten Vertrauensniveau[814] alle Ereignisse abzuwehren, die die o.g. Schutzziele beeinträchtigen können.

Nach § 30 Abs. 2 S. 1 RegE BSIG müssen die Sicherheitsmaßnahmen weiterhin auf einem „gefahrenübergreifenden Ansatz" beruhen, d.h. die zu gewährleistende IT-Sicherheit bezieht sich auf alle vorsätzlichen, fahrlässigen und zufälligen Ereignisse, die sowohl intern als auch extern ausgelöst werden können.[815]

2. Verfügbarkeit, Vertraulichkeit und Integrität

Über die spezifische Auslegung der Schutzziele im Kontext der Sicherheitsdefinition des Art. 6 Nr. 2 NIS2-RL (*Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und Diensten*) besteht derzeit noch Unklarheit. Als hilfreich erweisen sich in diesem Kontext die Definitionen der ENISA sowie die technische Literatur. Auch die Definitionen des *Grundschutzkompendiums des BSI* können zumindest indiziell berücksichtigt werden. Es werden auch die Definitionen der Schutzziele mit Blick auf Systeme betrachtet, um diese am Ende des Abschnitts entsprechend Art. 6 Nr. 2 NIS2-RL zur Bestimmung der *Schutzziele an den Diensten* zu nutzen.

Für die IT-Sicherheit im Allgemeinen wird mit Blick auf Daten und Systeme angenommen, dass *Verfügbarkeit* die Nutzbarkeit innerhalb einer definierten Zeitspanne[816] beschreibt oder aber die Anforderung, dass sie „von den Anwendern stets wie vorgesehen" genutzt werden können.[817] Die ENISA definiert Verfügbarkeit als die Tatsache, dass Daten zugänglich sind und Dienste funktionieren.[818] Als Schutzrichtung lässt sich Verfügbarkeit ausdrücken als der Schutz vor Daten-[819] oder Funktionsverlust.

814 Dies dürfte ein Ausdruck dessen sein, dass Sicherheit niemals absolut gewährleistet werden kann. Die konkreten Anforderungen an das „bestimmte Vertrauensniveau" dürften sich aus der Angemessenheit ergeben, siehe zu Letzterem unter S. 293 ff.

815 Vgl. EG 79 NIS2-RL.

816 *Hornung/Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 23 (26), Rn. 13.

817 BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S. 8.

818 The fact that data is accessible and services are operational; ENISA, Glossary Risk Management, 24.07.2009, G6: Data Availability.

819 Zu § 2 Abs. 2 BSIG und dementsprechend auf Informationen abstellend: *Heckmann*, MMR 2006, 280 (281).

Mit der *Vertraulichkeit* wird die Eigenschaft umschrieben, dass Daten und Systeme nur „für autorisierte Benutzer zugänglich" sind.[820] Als Schutzrichtung soll Vertraulichkeit somit den Schutz von gespeicherten Daten gegen das Abhören und Mitlesen durch unbefugte Personen sicherstellen.[821]

Die *Integrität* schließlich beschreibt die Unveränderbarkeit bzw. die Nachvollziehbarkeit jeder Veränderung.[822] Sie enthält die Zusicherung, dass gesendete, empfangene oder gespeicherte Daten vollständig und unverändert sind.[823] Schließlich beschreibt die Integrität demnach sowohl „die Korrektheit (Unversehrtheit) von Daten" als auch „die korrekte Funktionsweise der Systeme."[824]

Insgesamt lassen sich alle Schutzziele in Bezug auf die Daten somit klar definieren. Soweit es die *Verfügbarkeit* betrifft, lässt sich diese Anforderung auch auf den *Dienst* übertragen. Dies ist insofern folgerichtig, als dass für den Rechtsgüterschutz am Ende die Verfügbarkeit des von einem System erbrachten Dienstes erforderlich ist, nicht die Verfügbarkeit eines Systems selbst.

Die *Integrität* lässt sich ebenfalls auf den Dienstbegriff anwenden und kann entsprechend als das manipulationsfreie Informationsangebot eines Systems, also die Erzeugung „korrekter" Ergebnisse, verstanden werden. Hingegen ist die Anforderung der *Vertraulichkeit* an den Dienst losgelöst vom System nicht zielführend. Das Dienstangebot drückt sich in Form von Daten aus, deren Vertraulichkeit aber bereits gesondert erfasst ist. Und die Vertraulichkeit des Dienstes kann sich auch nicht auf das System und seine Komponenten beziehen, da dies gerade die Abgrenzung zwischen System und Dienst verwischen würde.

820 *Hornung/Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 23 (26), Rn. 13.

821 "The protection of [...] stored data against interception and reading by unauthorized persons", ENISA, Glossary Risk Management, 24.07.2009, G7: Data Confidentiality; ähnlich auch das BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S. 8.

822 *Hornung/Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 23 (26), Rn. 13.

823 The confirmation that data which has been sent, received, or stored are complete and unchanged.

824 BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S. 4, 6 „Verfügbarkeit", „Vertraulichkeit" und „Integrität"; *Gadatsch/Mangiapane*, IT-Sicherheit, S. 17 ff.

3. Authentizität

Als weiteres Schutzziel ist in der NIS2-RL anders als in der DSGVO[825] noch die Authentizität genannt. Eine Legaldefinition besteht hingegen nicht. Nach der ENISA ist Authentizität die Eigenschaft, dass eine Entität das ist, was sie vorgibt zu sein.[826] Das BSI definiert die Authentizität ganz ähnlich als die Eigenschaft, „die gewährleistet, dass eine Kommunikationsstelle tatsächlich diejenige ist, der [sic!] sie vorgibt zu sein."[827]

Diese Definition wäre entsprechend für den (digitalen) Dienst anwendbar, über den zwei Parteien kommunizieren. In Abgrenzung zur Bezugnahme auf Daten (dazu sogleich) lässt sich hier ein Vorfeldschutz sicherstellen. Im Rahmen einer Kommunikationsverbindung soll bereits die Authentizität der jeweiligen Entitäten sichergestellt werden, noch bevor es zu einem inhaltlichen Daten- und Informationsaustausch kommt.

Weiterhin führt das BSI aus: "Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden."[828] Allerdings lässt sich gegen diese Definition in Bezug auf Informationen bzw. hier Daten auch gut argumentieren, dass dieser Aspekt der „richtigen, unveränderten Urheberangabe" bereits unter die Integrität von Daten fällt.[829] Auch die Gesetzesbegründung des NIS2UmsuCG geht davon aus, dass die Authentizität im deutschen Recht einen Unterfall der Integrität darstellt.[830] Deshalb nennt der RegE BSIG die Authentizität auch nicht mehr gesondert. Ob dies aber über die Daten hinaus generell überzeugend ist, ist zweifelhaft; außerdem führt es zu einer unnötigen jedenfalls sprachlichen Divergenz zwischen NIS2-RL sowie anderen europäischen IT-Sicherheitsvorschriften (z.B. Art. 2 Nr. 21 EECC-RL) und dem RegE BSIG.

---

825 Teilweise wird ohne weitere Begründung die Authentizität auch zu den Schutzzielen der Datensicherheit gezählt *Forgó*, in: Oppermann/Stender-Vorwachs, Autonomes Fahren, 353 (355). Dafür fehlt es jedoch an einem gesetzlichen Anknüpfungspunkt, da Art. 32 Abs. 1 lit b) DSGVO die Authentizität als Schutzziel gerade nicht nennt.

826 "Property that an entity is what it claims to be", ENISA, Interoperable EU Risk Management Toolbox, 21.02.2023, Anhang I, S. 23.

827 BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S. 1.

828 Wie zuvor; ähnlich auch *Sohr/Kemmerrich*, in: Kipker, Cybersecurity, 49 (54), Rn. 13, wonach Daten echt sein müssten, d.h. es dürfe sich nicht um eine Kopie handeln und der/die Urheberin müsse eindeutig ermittelt werden können.

829 Vgl. *Samonas/Coss*, JISSec, Vol. 10 (2014), Heft 3, 21 (34); *Solms/van Niekerk*, Computers & Security, Vol. 38 (2013), 97 (98).

830 BReg, Entwurf NIS2UmsuCG, 22.07.2024, S. 138.

Im Sinne obiger Argumentation lässt sich die Authentizität zumindest auf den Dienst anwenden.

Die Authentizität ist damit v.a. in *offenen Systemen* ein relevantes Schutzziel, da hier gerade unsicher (bzw. sogar ungewiss) ist, ob die anderen teilnehmenden Entitäten „echt", also authentisch sind.

II. Systeme, Dienste, Daten und Informationen

Nachfolgend sollen die einzelnen Elemente der Informationstechnik, d.h. insbesondere Systeme, Dienste, Daten und Informationen beschrieben werden.

Entscheidend ist bei den *Systemen* zunächst der bereits bei der Definition der IT-Sicherheit genannte Unterschied, dass die NIS2-RL den Begriff der *Netz- und Informationssysteme* verwendet, wohingegen der RegE BSIG an dieser Stelle den alten Terminus der *„informationstechnischen Systeme, Komponenten und Prozesse"* bemüht. Auf diesen (möglichen) Widerspruch im Systembegriff wird unter 1. eingegangen. Zweitens ist fraglich, was unter dem Begriff des *Dienstes* im RegE BSIG zu verstehen ist. Insoweit bestehen dort als auch in der NIS2-RL unterschiedliche Verwendungen des Begriffs und teilweise auch unterschiedliche Legaldefinitionen (2.). Und 3. sind nach der NIS2-RL explizit (digitale) *Daten* und nach dem BSIG (weiterhin) *Informationen* zu schützen, was wiederrum die Frage nach dem einschlägigen Verständnis nach dem RegE BSIG eröffnet.

1. Systeme

Nachfolgend soll der Begriff des *Systems* bestimmt werden. Dabei stehen sich normhierarchisch die Termini „Netz- und Informationssysteme" (NIS2-RL) sowie „informationstechnische Systeme, Komponenten und Prozesse" (RegE BSIG) gegenüber. Es stellt sich somit insbesondere die Frage, ob und inwieweit der nationale Terminus der „Systeme, Komponenten und Prozesse" etwas anderes meint als jener der Netz- und Informationssysteme und in der Folge somit ggf. richtlinienkonform ausgelegt werden müsste oder ob es sich um eine zulässige Konkretisierung handelt.

Hierfür werden zunächst die „Systeme, Komponenten und Prozesse" national ausgelegt (a.). Anschließend werden die Netz- und Informationssysteme der NIS2-RL betrachtet (b.). Schließlich wird in einer Zusammen-

führung untersucht, ob und inwieweit Unterschiede bestehen und ggf. eine richtlinienkonforme Auslegung erforderlich ist (c.). Dabei wird insbesondere auch der Frage nachgegangen, ob Daten rechtlich als Bestandteil des Systems adressiert werden und ob das „System" soziotechnisch zu verstehen ist.

a. Systeme, Komponenten und Prozesse

Die „informationstechnischen Systeme, Komponenten und Prozesse" sind bereits seit 2009 im BSIG vorhanden[831] und wurden nun auch in § 30 Abs. 1 RegE BSIG übernommen.

Allerdings wird diese Begriffstrias der „informationstechnischen Systeme, Komponenten und Prozesse" im RegE BSIG wie auch bislang nicht näher definiert. Nach Wortlaut und Telos dürfte es sich aber hierbei zumindest um technische Mittel zur Verarbeitung von Informationen und damit um Informationstechnik i.S.d. § 2 Nr. 18 RegE BSIG handeln. Dies umfasst jedenfalls alle zur Informationsverarbeitung eingesetzte Hard- und Software.[832]

Nach dem BSI sind *informationstechnische Systeme (IT-Systeme)* „technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls."[833]

Eine *Komponente* ist nach dem BSI (zumindest in der Softwarearchitektur) eine „eigenständig einsetzbare Einheit mit Schnittstellen nach außen, die mit anderen Komponenten verbunden werden kann."[834] Dies dürfte auch über die Softwarearchitektur hinaus als tauglicher Definitionsbestandteil dienen: Insgesamt wird man sagen können, dass IT-Systeme stets aus Soft- und Hardwarekomponenten zusammengesetzt werden.[835] Mit dem Erfordernis einer „eigenständig einsetzbaren Einheit" muss eine Komponente stets eine abgrenzbare (Teil-)Funktion erfüllen. Beispielsweise

831 Zuvor waren es nur Systeme und Komponenten, die Ergänzung der „Prozesse" wurde lediglich als „redaktionelle Anpassung" begründet, BT-Drs. 62/09, S. 13.

832 *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 2 BSIG, Rn. 2; BT-Drs. 11/7029, S. 7.

833 BSI, IT-Grundschutz-Kompendium, 2023, S. 4.

834 BSI, IT-Grundschutz-Kompendium, 2023, S. 5.

835 Vgl. *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 2 BSIG, Rn 9; BT-Drs. 18/4096, S. 26; *Wischmeyer*, Informationssicherheit, S. 192.

besteht ein Smartphone als IT-System (s.o.) aus Hardware-Komponenten wie dem Prozessor, dem Speicher oder den Kameras und aus Softwarekomponenten wie dem Betriebssystem und der jeweiligen Firmware.

Schließlich verbleibt der Begriff des Prozesses: Ein *Prozess* könnte im hiesigen Kontext des IT-Sicherheitsrechts insbesondere für kritische Anlagen entweder ökonomisch (als Produktionsprozess) oder informationstechnisch verstanden werden. Für letztere Betrachtung, spricht zum einen, dass die (informationstechnischen) Schutzziele auch auf die Prozesse bezogen werden. Zum anderen ist nach der Systematik des Rechtssatzes davon auszugehen, dass sich das voranstehende Adjektiv „informationstechnisch" neben Systemen und Komponenten auch auf den Prozess bezieht. Somit ist hier von einem *IT-Prozess* auszugehen.[836] Dieser IT-Prozess ist ebenfalls Teil der IT-Systeme und beschreibt den Vorgang der Informationsverarbeitung.[837]

Diese feingranulare Unterteilung der IT-Systeme in Komponenten und Prozesse dient als rechtlicher Ansatzpunkt dafür, dass die zu treffenden Maßnahmen zielgerichtet an der richtigen Stelle ansetzen.[838] Nach der Gesetzesbegründung sollen etwa besonders kritische IT-Prozesse (z.B. die zentrale Steuerung eines Kraftwerkblocks) abgeschottet werden, so dass sie nicht über das Internet erreichbar sind.[839]

b. Netz- und Informationssysteme

Der Begriff der Netz- und Informationssysteme ist in Art. 6 Nr. 1 NIS2-RL legaldefiniert. Historisch hat sich dieser Begriff erst mit der Zeit im europäischen Recht entwickelt: 2001 sprach die EU-Kommission unter der Überschrift „Sicherheit der Netze und Informationen – Vorschlag für

836 So im Ergebnis auch in der Gesetzesbegründung, BT-Drs. 18/4096, S. 26; Dieser IT-Prozess kann aber wohl nicht mit dem ebenfalls im Gesetz genannten *IKT-Prozess* gleichgesetzt werden, welcher nach § 2 Nr. 16 RegE BSIG i.V.m. Art. 2 Nr. 14 CSA jegliche Tätigkeiten bezeichnet, „mit denen ein ITK-Produkt [sic!] oder -Dienst konzipiert, entwickelt, bereit gestellt oder gepflegt werden soll." Denn der IT-Prozess dient hier teleologisch nicht in erster Linie der Entwicklung, Bereitstellung oder Pflege anderer I(K)T-Produkte und Dienste, sondern der Aufrechterhaltung des Betriebs einer (besonders) wichtigen Einrichtung.

837 BT-Drs. 18/4096, S. 26.

838 Wie zuvor.

839 Wie zuvor.

einen europäischen Politikansatz“ noch von Netzen und Informationssystemen.[840] Diese wurden mit Blick auf die wirtschaftliche und soziale Entwicklung der EU als ein wichtiger Faktor verstanden, denn sie „ermöglichen Dienstleistungen und übertragen Daten in einem Maße, in dem dies noch vor wenigen Jahren unvorstellbar war.“[841] Die heutige Definition der Netz- und Informationssysteme ist in Art. 6 Nr. 1 NIS2-RL in drei (nicht explizit benannte) Teilelemente untergliedert (lit a-c):

i. Netzsystem

Zunächst wird in lit a) auf die Definition eines elektronischen Kommunikationsnetzes nach Art. 2 Nr. 1 RL 2018/1972 verwiesen, wonach ein Netz insbesondere Übertragungssysteme und ggf. Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen zur Übertragung von Signalen erfasst.[842] Aus der Verwendung des Begriffs „elektronisches Kommunikationsnetz“ und dem Begriff „Übertragungssystem“ in der verwiesenen Definition kann geschlossen werden, dass an dieser Stelle das „Netzsystem“ definiert wird. Nach o.g. Mitteilung der EU-Kommission werden Netze als Systeme definiert, „in denen Daten gespeichert oder verarbeitet werden und durch die Daten fließen.“[843] Hierzu gehörten demnach Übertragungs- bzw. Hardwarekomponenten wie z.B. Satelliten, Kabel, Router, Gateways und zugehörige Dienste wie etwa der DNS-Resolver oder Authentifizierungsdienste.[844]

840 EU-Kommission, KOM (2001) 298 endgültig, 06.06.2001.
841 EU-Kommission, a.a.O., S. 2.
842 Vollständige Definition für ein „elektronisches Kommunikationsnetz“: Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen.
843 EU-Kommission, KOM (2001) 298 endgültig, 06.06.2001, S. 9.
844 Wie zuvor.

ii. Informationssystem

Das Informationssystem wird in lit b) definiert als „ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen".

Zwar rekurriert auch dieser Teil der Definition nicht ausdrücklich auf den Begriff des Informationssystems. Allerdings ergibt sich dies zum einen in Gegenüberstellung mit lit a) und zum anderen aus der nahezu gleichlautenden Definition des Informationssystems des Art. 2 lit a) der RL über Angriffe auf Informationssysteme,[845] die sich mit der Strafbarkeit von selbigen befasst und zusammen mit der NIS-RL seinerzeit den „Kern der politischen Antwort der Europäischen Union auf […] sicherheitsbezogenen Herausforderungen im Cyberraum" darstellte,[846] mithin rechtssystematisch eng verwandt ist und deshalb zur Auslegung herangezogen werden kann. Die o.g. Mitteilung der EU-Kommission legt nahe, dass Informationssysteme (an Netze angeschlossene) Anwendungen wie E-Mail und Browser sowie die eigentlichen Endgeräte wie z.B. Server, PCs und Mobiltelefone umfassen.[847]

iii. Digitale Daten

Im letzten Teil (lit c) schließlich werden digitale Daten aufgenommen, die von den Netz- und Informationssystemen „zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden". Trotz dieser eingängigen Definition werden die digitalen Daten aber systematisch („oder") als Alternative zu den Netz- und Informationssystemen definiert. Im Sinne einer teleologischen Auslegung sind aber Daten allenfalls als *Bestandteil eines Systems* der 1. und 2. Variante zu verstehen, da Daten für sich alleine denklogisch noch kein informationstechnisches System darstellen.[848] Zur Definition von Daten ihrerseits sogleich unter (3.).

845 RL 2013/40/EU.
846 EU-Kommission, COM(2016) 410 final, 05.07.2016, S. 2.
847 EU-Kommission, KOM (2001) 298 endgültig, 06.06.2001, S. 8, 9.
848 Kritisch zu dieser Definition nach der NIS-RL bereits ebenso: *Freimuth,* Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, S. 65.

c. Zusammenführung und soziotechnisches Verständnis

Ausgangspunkt war die Frage, was unter den Systemen, Komponenten und Prozessen im RegE BSIG zu verstehen ist und inwieweit unter Beachtung der NIS2-RL (Netz- und Informationssysteme) ggf. eine richtlinienkonforme Auslegung der Begriffe erforderlich ist.

Hinsichtlich des *IT-Systems* ergeben sich keine erheblichen, inhaltlichen Unterschiede. Informationssysteme nach Art. 6 Nr. 2 lit b) der NIS2-RL dürften den „informationstechnischen Systemen" des RegE BSIG entsprechen. Im Detail lassen sich weiterhin die „Komponenten" der „Gruppe miteinander verbundener oder zusammenhängender Geräte" und dem „Prozess" die „automatische Verarbeitung" zuordnen. Insgesamt umfassen IT-Systeme mit ihren Hard- und Softwarekomponenten und ihren den Verarbeitungsprozessen demnach z.B. PCs, Server, Router und Smartphones oder Tablets.

Ob und inwieweit unter den Systembegriff des RegE BSIG auch die *Netzsysteme* der NIS2-RL gefasst werden sollen, ist zweifelhaft. Grundsätzlich besteht mit § 165 TKG eine Sondervorschrift für Anbieter von Telekommunikationsdiensten und Betreiber öffentlicher Telekommunikationsnetze (nachfolgend nur: TK-Anbieter) gilt. Dies gilt nach bisheriger Rechtslage, auch soweit die TK-Anbieter auch als kritische Infrastrukturen anzusehen sind: Die IT-Sicherheitsvorgaben nach § 8a BSIG (§§ 30, 31 RegE BSIG) sind gemäß § 8d Abs. 2 Nr. 1 nicht auf diese anzuwenden. Mit dem RegE BSIG gilt dies nur noch eingeschränkt: Zwar werden diese gemäß § 28 Abs. 4 Nr. 1 RegE BSIG weiterhin nicht den Anforderungen als kritische Anlage nach § 31 RegE BSIG unterworfen, wohl aber den Anforderungen als wichtige Einrichtungen nach § 30 RegE BSIG (§ 28 Abs. 1 Nr. 3 RegE BSIG). Damit könnte der Begriff des „Netzsystems" somit auch im RegE BSIG zunehmend relevant sein, allerdings wurde die Begriffstrias der Systeme, Komponenten und Prozesse nicht verändert. Insofern wäre ggf. auch hier eine richtlinienkonforme Auslegung vorzunehmen, was angesichts des generischen Charakters der Begriffe „Systeme, Komponenten und Prozesse" aber jedenfalls keine Schwierigkeiten auslösen sollte, z.B. indem Satelliten oder Router als Systeme mit ihren jeweiligen Komponenten und Prozessen erfasst werden.[849]

849 Es sei an dieser Stelle (auch für die Informationssysteme) darauf hingewiesen, dass die Begriffe Systeme und Komponenten auch jenseits der genannten Beispiele skaliert werden können: siehe hierzu bereits: S. 114, Fn. 238.

Dass die Daten, wie von der NIS2-RL vorgegeben, rechtlicher Bestandteil des Systems sind, lässt sich nicht ohne weiteres mit der Definition der Informationstechnik „als technische Mittel zur Verarbeitung von Informationen" (§ 2 Nr. 18 RegE BSIG) in Einklang bringen, zu denen wie bereits dargestellt auch die Systeme, Komponenten und Prozesse zählen. Ein *Mittel zur Verarbeitung von* Informationen bzw. nach der Gesetzesbegründung wohl zugleich von Daten,[850] dürfte diese prima facie nicht miteinschließen. Eine Auslegung, die aber ggf. doch teleologisch zwischen Daten und Informationen differenziert und die Daten somit als technische Repräsentation von Informationen den „Mitteln der Verarbeitung von Informationen" und damit auch den Systemen zuordnet entspräche eher dem *Gebot der richtlinienkonformen Auslegung*[851] und ist daher vorzugswürdig. Die Daten sind daher auch nach dem RegE BSIG als Teil des Systems zu verstehen.

Schließlich ergibt sich weder aus dem Systembegriff des RegE BSIG noch der NIS2-RL ein *soziotechnisches Systemverständnis*. Insbesondere kritische Anlagen, aber auch andere regulierte Einrichtungen lassen sich zwar an sich als soziotechnische Systeme verstehen (die dann aber bei holistischer Betrachtung weit über den Regelungsbereich der „IT-Sicherheit" hinausgehen). Aber die Bezeichnung als „informationstechnisches" System in § 2 Nr. 39 RegE BSIG und die Definitionen der Netz- und Informationssysteme in Art. 6 Nr. 1 lit b) NIS2-RL beziehen sich eindeutig auf ein (informations)technisches Verständnis. Gleichwohl wird das IT-Personal in die Gewährleistung der IT-Sicherheit mit einbezogen: So sind nach § 30 Abs. 1 RegE BSIG generell auch das Personal betreffende „organisatorische Maßnahmen" zu treffen und § 30 Abs. 4 Nr. 9 RegE BSIG nennt darüber hinaus auch die Gewährleistung der „Sicherheit des Personals" als spezifische, vorzunehmende Sicherheitsmaßnahme.[852]

850 Das mit Informationsverarbeitung auch die Datenverarbeitung gemeint ist, zeigt sich auch in: BT-Drs. 11/7029, S. 7; ausführlich zur fehlenden Differenzierung zwischen Informationen und Daten im BSIG später auf S. 288.

851 Siehe S. 266, Fn. 803.

852 So auch in Art. 21 Abs. 2 lit i) und EG 79 NIS2-RL; richtigerweise wird man dies allerdings auf jenes Personal beschränken müssen, dass entweder die IT bedient oder zumindest Zugang zu der IT hat, da andernfalls der Anwendungsbereich des IT-Sicherheitsrechts überdehnt werden dürfte.

2. Dienste

Der Dienstbegriff ist im IT-Sicherheitsrecht äußerst vielschichtig und tritt im RegE BSIG bzw. der NIS2-RL insbesondere an drei Stellen auf:

Zunächst ist er in der Pflichtennorm des Art. 21 Abs. 1 NIS2-RL genannt, wonach „Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen *für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen*," von den Normadressaten zu „beherrschen" sind. Zumindest soweit es die „Erbringung ihrer Dienste" betrifft, sieht dies dem Wortlaut nach auch § 30 Abs. 1 RegE BSIG vor, wonach „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden" sind.

Zum zweiten ist der Dienstbegriff in der Definition der „Sicherheit von Netz- und Informationssystemen" (Art. 6 Nr. 2 NIS2-RL) selbst enthalten, wonach diese die Fähigkeit besitzen müssen, „auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten *oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden* bzw. zugänglich sind, beeinträchtigen können." In der entsprechenden (richtlinienwidrigen) Definition der IT-Sicherheit in § 2 Nr. 39 RegE BSIG fehlt der Dienst hingegen.

Schließlich sind der Vollständigkeit halber noch zwei weitere Dienstdefinitionen (IKT-Dienst, digitaler Dienst) in der NIS2-RL bzw. im RegE BSIG zu nennen, die ebenfalls von Relevanz sein könnten.

Nachfolgend werden zunächst die Dienstbegriffe nach der NIS2-RL (a.) und sodann jene nach dem RegE BSIG (b.) dargestellt und an den notwendigen Stellen mit der NIS2-RL gegenübergestellt. Anschließend wird ein Zwischenfazit gezogen (c.).

a. Dienstbegriffe nach der NIS2-RL

Unterschiedliche Dienstbegriffe finden sich zunächst (i.) in Art. 21 Abs. 1 (der ökonomische Dienst) und sodann (ii.) in Art. 6 Nr. 2 (der IT-Dienst). Drittens (iii.) bestehen mit dem „IKT-Dienst" und dem „digitalen Dienst" in Art. 6 Nr. 13 i.V.m. Art. 2 Nr. 12 CSA sowie Art. 6 Nr. 23 NIS2-RL i.V.m. Art. 1 Abs. 1 lit b) RL 2015/1535 noch zwei weitere Dienstbegriffe.

i. Der ökonomische Dienst: Art. 21 Abs. 1 NIS2-RL

Aus o.g. Auszug aus Art. 21 Abs. 1 NIS2-RL, wonach die Sicherheit der Netz- und Informationssysteme gewährleistet werden soll, welche die Einrichtungen für die Erbringung ihrer Dienste (oder ihren Betrieb) nutzen, kann gefolgert werden, dass durch die entsprechenden IT-Sicherheitsmaßnahmen am Ende v.a. die *kontinuierliche Erbringung dieser Dienste* gesichert werden soll. Sofern eine Einrichtung keinen solchen spezifischen Dienst erbringt (z.B. im Maschinen- und Kraftfahrzeugbau) dürfte die 2. Alternative des „Betriebs" greifen.

Historisch ist zu beachten, dass die NIS-RL anders als das BSIG auch kritische Infrastrukturen bzw. deren Leistungen als „wesentliche Dienste" bezeichnete.[853] Nach Art. 14 Abs. 2 NIS-RL sollten die Betreiber u.a. den Auswirkungen von Sicherheitsvorfällen vorbeugen, die „die Sicherheit der von ihnen für *die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme* beeinträchtigen". Dies entspricht im Übrigen zumindest auch der Regelungstechnik nach dem § 8a Abs. 1 BSIG, wonach Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse vermieden werden sollen, die für die *Funktionsfähigkeit der kritischen Infrastrukturen* maßgeblich sind.

Der Dienst bezeichnet hier in *ökonomischer Betrachtung* somit die am Ende *erbrachte Dienstleistung*. Dies können zum einen *physische Dienstleistungen* (z.B. die Versorgung mit Trinkwasser oder Strom) sein:[854] es handelt sich in dem Fall um sog. *cyber-physische Systeme*, bei denen neben der hier adressierten Informationstechnik noch andere Faktoren darüber bestimmen, ob es tatsächlich zu einem Ausfall der kritischen Dienstleistung wie etwa der Strom- oder Wasserversorgung kommt. Zum anderen erbringen

853 Vgl. Art. 4 Nr. 4, Anhang II, EG 19, 20 NIS-RL; weiterhin in Art. 2 Nr. 4, 5 RKE-RL, wonach kritische Infrastrukturen u.a. Anlagen sind, die für die Erbringung wesentlicher Dienste erforderlich sind.

854 Die NIS2-RL (bzw. auch das BSIG) verlangt aber auch bei cyber-physische Systemen ihrem Normzweck entsprechend nur die Sicherheit in der Informationstechnik, die physischen Aspekte (soweit sie sich nicht auf die informationstechnischen Systeme beziehen, siehe hierzu EG 31 NIS2-RL) werden hingegen durch die ECE-RL bzw. den RefE KritisDachG reguliert. Gleichwohl meint der Dienst an dieser Stelle die finale physische Dienstleistung, da diese für die Schutzgüter relevant ist und die zumindest auch durch die Sicherheit in der Informationstechnik beeinträchtigt werden kann.

kritische Anlagen aber im Sektor „digitale Infrastruktur“ oder aber auch die digitalen Dienste[855] wie bereits angesprochen rein *digitale Dienstleistungen*, was hier insbesondere zu einer besonders engen Kopplung zwischen Informationstechnik und den Schutzgütern führt.[856]

ii. Der IT-Dienst: Art. 6 Nr. 2 NIS2-RL

Ein anderes Dienstverständnis findet sich hingegen in Art. 6 Nr. 2 NIS2-RL. Dort wird der Dienst als Teil der Definition der *Sicherheit der Netz- und Informationssysteme* verwendet. Nach dieser Definition sollen an diesem Dienst als Schutzobjekt die Schutzziele Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit sichergestellt werden. Außerdem wird der Dienst demnach „über Netz- und Informationssysteme angeboten“.

Infolgedessen kann der Dienst in dieser Definition zumindest keine physische Dienstleistung wie etwa die Strom- oder Trinkwasserversorgung meinen. Eine solche kann weder den informationstechnischen Schutzzielen zugeordnet werden („vertrauliche Trinkwasserversorgung“) noch wird die Trinkwasserversorgung im Wortsinn „über Netz- und Informationssysteme angeboten“. Auch dass der Dienst hier als Bestandteil der Definition der Sicherheit von Netz- und Informationssystemen genutzt wird, spricht für seinen informationstechnischen Charakter an dieser Stelle.

Für diese unterschiedlichen Verständnisse des Dienstes spricht im Übrigen systematisch auch, dass beim Einsetzen der Sicherheitsdefinition aus Art. 6 Nr. 2 in die zuvor beschriebene Pflichtennorm des Art. 21 Abs. 1 NIS2-RL der Dienst zweimal genannt wird (gekürzte Wiedergabe):

> Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, *d.h. die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der* Dienste, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen.

855 Es handelt sich hierbei um sog. Over-the-Top-Dienste (OTT-Dienste), d.h. solche die der Anwendungsebene zuzuordnen sind und ihre Dienstleistung vollständig in digitaler Form erbringen.

856 Siehe dazu bereits zuvor, S. 254 f.

Insgesamt handelt es sich somit unter Zugrundelegung einer *technischen Betrachtung* an dieser Stelle (also dem hier erstgenannten Dienst) um der eigentlichen Dienstleistung vorgelagerte Dienste. Bei einer physischen Dienstleistung sind diese *vorgelagerten IT-Dienste* etwa Dienste zur elektronischen Ansteuerung einer Pumpe in einem Kraft- oder Wasserwerk. Liegt eine digitale Dienstleistung vor, können entsprechend zu den bisherigen Ausführungen die „Subdienste", d.h. die Dienste, die der eigentlichen digitalen Dienstleistung untergeordnet zuarbeiten, entsprechend als vorgelagerte IT-Dienste erfasst werden. Als Beispiel wäre hier ein Crawler-Dienst (IT-Dienst) einer Suchmaschine (digitale Dienstleistung) zu nennen, der das Internet nach (neuen) Inhalten durchsucht, damit diese später in einen Index aufgenommen und am Ende für die Erzeugung von Suchergebnissen genutzt werden können.[857]

Allerdings könnte bei digitalen Dienstleistungen die Sicherheitsdefinition (über die Subdienste hinaus) auch auf diese ausgedehnt werden. Hierfür spricht v.a. das teleologische Argument, dass auch eine Suchmaschine, ein Online-Marktplatz oder ein soziales Netzwerk natürlich selbst verfügbar, vertraulich, integer und authentisch sein soll. Dass dies im Wortlaut nicht explizit angelegt ist, dürfte insbesondere darauf zurückzuführen sein, dass Art. 21 Abs. 1 NIS-RL mit derselben Norm sowohl die Anbieter solch rein digitaler Dienstleistungen als auch physischer Dienstleistungen regulativ erfassen soll.

iii. Der IKT-Dienst und der digitale Dienst

Daneben bestehen noch zwei weitere Dienstdefinitionen: Zunächst der *IKT-Dienst* nach Art. 6 Nr. 13 NIS2-RL i.V.m. Art. 2 Nr. 13 CSA, „der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht". Die Begriffe des IKT-Dienstes (ebenso wie des IKT-Produktes, Art. 6 Nr. 12 NIS2-RL i.V.m. Art. 2 Nr. 12 CSA) werden in der NIS2-RL und dem RegE BSIG zwar v.a. im abweichenden Regelungskontext von (zertifizierten) IT-Angeboten Dritter verwendet, die von den wesentlichen und wichtigen Einrichtungen genutzt werden (vgl. EG 58, 90 f., Art. 12, Art. 24 NIS2-RL). Soweit es aber hier die soeben dargestellten IT-Dienste betrifft, dürften sich in der gleichsam *technischen Betrachtung* insofern keine we-

857 *Kausar/Dhaka/Singh*, IJCA, Vol. 63 (2013), Heft 2, 31 (31 f.).

sensmäßigen, inhaltlichen Unterschiede ergeben, sondern der IKT-Dienst kann vielmehr als Auslegungshilfe für den IT-Dienst in Art. 6 Nr. 2 NIS2-RL herangezogen werden.

Schließlich gibt es noch die Definition der *digitalen Dienste* nach Art. 6 Nr. 23 NIS2-RL i.V.m. Art. 1 Abs. 1 lit b) RL 2015/1535. Ein „Dienst" ist demnach „eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung."[858] Die einzelnen Bestandteile werden dort noch näher definiert. Die auch im Rahmen dieser Untersuchung so bezeichneten „digitalen Dienste", d.h. Online-Suchmaschinen, Online-Marktplätze und soziale Netzwerke fallen nach Anhang II, Ziff. 6 NIS2-RL exklusiv[859] unter diesen Begriff.[860] Bei diesen digitalen Diensten kommt insoweit wieder eine *ökonomische Betrachtung* mit Blick auf das Marktangebot zur Anwendung.

b. Dienstverständnisse im RegE BSIG

i. Verständnis des nationalen Gesetzgebers

Der nationale Gesetzgeber hat bei der Umsetzung der NIS2-RL in nationales Recht im derzeitigen Entwurfsstand grundlegende Veränderungen vorgenommen, die sich auch auf die zuvor dargestellten Dienstbegriffe auswirken.

858 Dieser Dienstbegriff wird auch in der DSGVO genannt, siehe hierzu S. 119.

859 Daneben werden auch Cloud-Computing-Dienste in Art. 6 Nr. 30 NIS2-RL und § 2 Nr. 4 RegE BSIG als „digitale Dienste" legaldefiniert, sie gehören aber laut Anhang (anders als noch in der NIS-RL) nicht mehr in diesen Sektor, sondern in den (kritischen) Sektor „Digitale Infrastruktur" (Anhang I, Ziff. 8 NIS2-RL) bzw. „Informationstechnik und Telekommunikation" (Anlage 1 Ziff. 6 RegE BSIG). Insgesamt ist somit unklar, ob Cloud-Computing-Dienste nach dem Regelungskonzept weiterhin als „digitale Dienste" zu bezeichnen sind oder ob diese Definition nicht vielmehr ein Relikt aus der alten Rechtslage ist und „digitale Dienste" somit (wie in dieser Untersuchung) exklusiv nur die drei genannten Dienste dieses Sektors erfassen sollen.

860 Die Voraussetzung der Erbringung „in der Regel gegen Entgelt" dürfte trotz fehlender Geldzahlungspflicht der Endnutzer:innen dadurch erfüllt sein, dass die Dienste werbefinanziert sind und die Endnutzer:innen mit ihren Daten „bezahlen"; *Kühling/Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 4 Nr. 25, Rn. 6 f. m.w.N.

Vorbemerkend ist noch einmal hervorzuheben, dass in Art. 21 Abs. 1 NIS2-RL sowohl Einrichtungen, die eine bestimmte (kritische) Dienstleistung erbringen als auch große wirtschaftlich relevante Einrichtungen (z.B. im Maschinen- und Fahrzeugbau) erfasst werden. Insofern verlangt Art. 21 Abs. 1 NIS2-RL von den Einrichtungen, die Sicherheit der Netz- und Informationssysteme zu gewährleisten, die entweder für deren Dienste (i.S.d. kritischen physischen oder digitalen Dienstleistung" oder (sofern eine solche nicht besteht, z.B. Maschinen- und Fahrzeugbau) für deren *Betrieb* erforderlich sind.

Der nationale Gesetzgeber hat nun diese einheitliche Reglung teilweise aufgespalten. Nach § 30 Abs. 1 RegE BSIG müssen die Einrichtungen die Sicherheit für die Systeme, Komponenten und Prozesse gewährleisten, die sie (nur) *für die Erbringung ihrer Dienste* nutzen. In der Entwurfsbegründung zu § 30 Abs. 1 RegE BSIG heißt es insoweit,

> *„der Begriff ‚Erbringung ihrer Dienste' ist hierbei weit gefasst und insbesondere nicht mit der Erbringung (kritischer) Versorgungsdienstleistungen zu verwechseln. Vielmehr sind die hier gemeinten Dienste sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Büro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden."*[861]

Aus dieser Begründung ist zu entnehmen, dass der nationale Gesetzgeber den Begriff des Dienstes hier gerade nicht wie in Art. 21 Abs. 1 NIS2-RL als Dienstleistung, sondern eher *technisch im Sinne eines IT-Dienstes* verstanden wissen will. Die „Dienste" in § 30 Abs. 1 RegE BSIG erfassen somit wohl alle IT-Dienste für den „*Betrieb*" und ersetzen dieses Merkmal insoweit.

Die ökonomische Dienstleistung wird hingegen in der gesonderten Vorschrift für kritische Anlagen (§ 31 Abs. 1 RegE BSIG) adressiert: „Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die *Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen* maßgeblich sind, […] auch aufwändigere Maßnahmen nach § 30 als verhältnismäßig." Nach der Legaldefinition in § 2 1 Nr. 22 RegE BSIG sind kritische Anlagen solche, die eine *kritische Dienstleistung*[862] erbringen; worauf somit durch die „Funktionsfähigkeit der kritischen Anlage" Bezug genommen wird. Damit wird die *physische*

861 BMI, Referentenentwurf zum NIS2UmsuCG, 22.12.2023, S. 124 f.
862 Legaldefiniert in § 2 Nr. 24 BSIG, hierzu auch schon: S. 230.

oder digitale Dienstleistung (als Ausdruck ökonomischer Betrachtung) nur hier erfasst.

ii. Folgen der unionsrechtswidrigen IT-Sicherheitsdefinition

Wie bereits zuvor dargestellt, ist die implizite IT-Sicherheitsdefinition des nationalen Gesetzgebers soweit sie in § 30 Abs. 1 RegE BSIG zum Ausdruck kommt, richtlinienwidrig.

Setzt man nun stattdessen die Sicherheitsdefinition nach Art. 6 Nr. 2 NIS2-RL in § 30 Abs. 1 RegE BSIG ein, kommt es erneut zu einer zweifachen Verwendung des Dienstbegriffs:

> Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der *Sicherheit der Netz- und Informationssysteme (verkürzt definiert als: die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der* Dienste*, die über diese Netz- und Informationssysteme angeboten werden)* die sie für ihre Dienste nutzen, zu vermeiden.

Das schließt indes das o.g. Verständnis des nationalen Gesetzgebers von dem (jetzt zweitgenannten) Dienst in § 30 Abs. 1 RegE BSIG aus, da bei einem technischen Verständnis desselben als IT-Dienst kein sinnstiftender Anwendungsbereich für den erstgenannten, eindeutig informationstechnischen Dienst mehr verbleibt.

Der Regelungsansatz mit dem alternativen Begriff der „kritischen Dienstleistung" (§§ 31 Abs. 1, § 2 Nr. 22, 24 RegE BSIG) ist zwar an sich zu begrüßen, soweit er, wie auch in dieser Untersuchung angestrebt, mehr Rechtsklarheit bei der Unterscheidung von den „IT-Diensten" und den physischen oder digitalen „Dienstleistungen" schafft. Aber dieser Regelungsansatz verträgt sich wie in § 30 RegE BSIG gezeigt mit Blick auf den Dienst nicht mit der Richtliniendefinition der „Sicherheit der Netz- und Informationssysteme", die aufgrund der Unionsrechtswidrigkeit der eigenen IT-Sicherheitsdefinition des § 2 Nr. 39 RegE BSIG angewendet werden muss.

c. Fazit

Die Folgen einer abweichenden Definition der IT-Sicherheit durch den nationalen Gesetzgeber wirken an dieser Stelle fort und es verbleibt erneut die Erwartung, dass der Gesetzgeber dies bis zur finalen Fassung des RegE BSIG noch revidiert. An dieser Stelle sei auch auf den – vom Nationalrat aber nicht angenommenen - österreichischen Umsetzungsentwurf zum NISG 2024 verwiesen, der insoweit sowohl die Sicherheitsdefinition als auch die Pflichtennorm (§§ 3 Nr. 2, § 32 Abs. 1 NISG-E 2024) sehr richtliniennah umgesetzt und derartige Widersprüche somit vermieden hätte.[863] Unter weiterer, konsequenter Annäherung an das Unionsrecht können für den Dienst somit folgende Ergebnisse festgehalten werden:

Der Dienst kann einerseits die physische oder digitale Dienstleistung im Sinne einer ökonomischen Betrachtung meinen. Nach Art. 21 Abs. 1 NIS2-RL dürfte der Dienstbegriff auch weiterhin in diesem *ökonomischen Sinn* zu verstehen sein. Nach dem derzeitigen, aber insoweit richtlinienwidrigen Entwurfsstand des BSIG kommt die *ökonomische Betrachtung* des Dienstes hingegen nur in der „kritischen Dienstleistung" nach § 31 Abs. 1 i.V.m. § 2 Nr. 22, 24 RegE BSIG zum Ausdruck. Gleichzeitig tritt bei diesen ökonomischen Dienstverständnissen in einer *rechtlichen Betrachtung*[864] eine Zuweisungsfunktion hinzu, da die Normadressaten *alle IT-Systeme sichern müssen, die sie für die Erbringung dieser Dienstleistung* nutzen.

Dagegen verwendet die Sicherheitsdefinition in Art. 6 Nr. 2 NIS2-RL (und das insoweit deshalb richtlinienwidrige Verständnis des Dienstes in § 30 Abs. 1 RegE BSIG) eine *technische Betrachtungsweise*: Hier wird nicht die Dienstleistung, sondern ein IT-Dienst beschrieben, an dem die informationstechnischen Schutzziele verwirklicht (und beeinträchtigt) sein können und der die elektronische Informationsverarbeitung hin zu einem

863 Bundeskanzleramt Österreich, Entwurf für ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (NISG-E 2024), 03.04.2024, S. 5, 23, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Begut&Einbringer=&Titel=&DatumBegutachtungsfrist=03.04.2024&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ImRisSeitChangeSet=Undefined&ImRisSeitForRemotion=Undefined&ResultPageSize=100&Suchworte=nis&ResultFunctionToken=536f0746-dbe8-4cde-b86f-022b3f0d32b0&Dokumentnummer=BEGUT_42FD65C8_76B7_40F0_97E3_BB29BDFC0CE9, zuletzt abgerufen am 05.04.2024.

864 Hierzu bereits S. 119.

informationstechnischen Ergebnis beschreibt.[865] Dies erfasst die *IT-Dienste, die für eine physische Dienstleistung erforderlich* sind bzw. die *untergeordneten IT-Dienste einer digitalen Dienstleistung*. Inhaltlich ist dieser Dienstbegriff schließlich wesensmäßig gleich zu jenem der *IKT-Dienste*,[866] der jedoch einen anderen regulatorischen Kontext aufweist, aber gleichwohl zur Auslegung herangezogen werden kann.

Mit Blick auf die *digitalen Dienste*[867], d.h. die Online-Suchmaschine, das soziale Netzwerk und der Online-Marktplatz, ist festzuhalten, dass wie im Sektor „Informationstechnik und Telekommunikation" die erbrachte „kritische Dienstleistung"[868] nur digital erfolgt. Auch mit diesem Dienstbegriff („digitale Dienste") wird somit ähnlich wie in Art. 21 Abs. 1 NIS-RL das ökonomische Angebot beschrieben, nur dass er sich hier als Oberbegriff der genannten Dienste auf *digitale Dienstleistungen* beschränkt.

Diese komplexe Vielfalt an unterschiedlichen Verständnissen des Dienstes soll nachfolgend nochmal tabellarisch zusammengefasst werden, wobei die beiden erstgenannten für diese Untersuchung entscheidend sind:

Tabelle 5: Verständnisse des Dienstes in NIS2-RL und RegE BSIG

Dienstverständnis	Vorkommen im Recht
physische oder digitale Dienstleistung (ökonomisch/rechtlich)	Art. 21 Abs. 1 NIS-RL § 31 Abs. 1, § 2 Nr. 24 RegE BSIG
(untergeordnete) IT-Dienste (technisch)	Art. 6 Nr. 2 NIS2-RL § ~~30 Abs. 1 RegE BSIG~~[869] IKT-Dienst: Art. 6 Nr. 13 NIS2-RL bzw. § 2 Nr. 14 RegE BSIG i.V.m. Art. 2 Nr. 12 CSA
nur digitale Dienstleistung (ökonomisch)	Digitaler Dienst: Art. 6 Nr. 23 NIS2-RL i.V.m. Art. 1 Abs. 1 lit b) RL 2015/1535

865 Insofern steht dieser Dienstbegriff in der nationalen Terminologie eher dem IT-Prozess nach § 2 Nr. 39 RegE BSIG nahe, siehe dazu bereits S. 273 ff.

866 Dieser ist in § 2 Nr. 14 RegE BSIG i.V.m. Art. 2 Nr. 12 CSA identisch zur NIS2-RL definiert.

867 Diese werden im RegE BSIG abweichend von der NIS2-RL nicht legaldefiniert, der Begriff ist daher richtlinienkonform auszulegen.

868 Zu beachten ist, dass es sich aber bei digitalen Diensten nicht um eine kritische Dienstleistung im Sinne des § 2 Nr. 24 RegE BSIG handelt, da die digitalen Dienste hier nicht als kritische Dienstleistung erfasst werden und deren Anbieter somit auch nur § 30 RegE BSIG (und nicht wie Betreiber kritischer Anlagen auch § 31 RegE BSIG) unterfallen.

869 Richtlinienwidrige Auslegung; müsste auch hier ökonomisch (vorangegangene Tabellenzeile) verstanden werden und dann ggf. auch den „Betrieb" umfassen.

3. (Digitale) Daten und Informationen

Fraglich ist schließlich, wie es sich auswirkt, dass in der NIS2-RL auf Daten und im RegE BSIG (zumindest dem Wortlaut nach) auf Informationen abgestellt wird.

Daten werden weder in der NIS2-RL noch im RegE BSIG ausdrücklich definiert. In Art. 2 lit b) der RL 2013/40/EU werden als „‚Computerdaten' jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann" definiert.[870]

In der Definition der Sicherheit in der Informationstechnik werden nach § 2 Nr. 39 RegE BSIG weiterhin „Informationen" als Schutzobjekt genannt. Es ist aber historisch nicht ersichtlich, dass damit aus technischer Sicht zwischen „Daten" und „Informationen" differenziert werden sollte. So heißt es etwa in der Gesetzesbegründung zur Einführung des BSIG mit Blick auf diese Definition der Sicherheit in der Informationstechnik: „Im Gegensatz etwa zum Bundesdatenschutzgesetz, das sich nur auf personenbezogene Daten bezieht, erstreckt sich der vorliegende Gesetzentwurf auf jede Art von Informationen",[871] womit offensichtlich (personenbezogene) „Daten" und Informationen gleichgesetzt werden. Auch die Informationstechnik, die als Oberbegriff die o.g. „Systeme, Komponenten und Prozesse" umfasst, bezieht sich in erster Linie auf Datenverarbeitungsanlagen in Form von Hard- und Software.[872]

Insgesamt ist daher davon auszugehen, dass mit „Informationen" an dieser Stelle letztlich auch in erster Linie die zu sichernden Daten gemeint sind und somit kein Unterschied zur NIS2-RL besteht. In beiden Fällen sind somit die Daten (als Bestandteil des Systems) zu sichern. Eine entsprechende Klarstellung im RegE BSIG wäre gleichwohl vorzugswürdig.

870 Im Übrigen kann auf die Darstellungen auf S. 60 ff. verwiesen werden.
871 BT-Drs. 11/7029, S. 7.
872 *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 2 BSIG, Rn. 2; BT-Drs. 11/7029, S. 7.

III. Risiko und Angemessenheit

Nach § 30 RegE BSIG sind besonders wichtige Einrichtungen und wichtige Einrichtungen verpflichtet, „geeignete, *verhältnismäßige* und wirksame technische und organisatorische Maßnahmen […] zu ergreifen, um *Störungen* der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, *zu vermeiden* […]". Insofern wird in diesem Normauftrag das Risiko nicht genannt; in § 30 Abs. 1 RegE BSIG steht hingegen wie bereits erwähnt statt „Störungen […] zu vermeiden", „*Risiken* für die Sicherheit der Netz- und Informationssysteme […] " *zu beherrschen.* Allerdings stellt sowohl § 30 Abs. 1 S. 2 RegE BSIG als auch die Entwurfsbegründung insoweit explizit auf Risiken ab,[873] so dass die Vermeidung von Störungen entsprechend als Beherrschung von Risiken historisch und richtlinienkonform ausgelegt werden muss.

1. Risiko

Im nachfolgenden sollen zunächst die Definitionen des *Risikos* dargestellt werden, wobei insbesondere auf das beschränkende Merkmal des vernünftigen Aufwands (a.) sowie den Bezugspunkt des Risikos (b.) eingegangen wird.

a. Beschränkung auf den „vernünftigen Aufwand"

Die ursprüngliche NIS-RL definierte Risiko in Art. 4 Nr. 9 noch als „alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben."

Die Begrenzung auf die „*mit vernünftigem Aufwand feststellbaren* Umstände und Ereignisse" brachte eine epistemische Einschränkung in den Risikobegriff ein, d.h. was nicht mit vernünftigem Aufwand feststellbar ist, stellt nach dieser Definition auch kein Risiko dar und wird folglich auch nicht im Rahmen des Risikomanagements behandelt. Diese Einschränkung wurde erst im Laufe des Gesetzgebungsverfahrens zur NIS-RL durch das

873 BReg, Entwurf NIS2UmsuCG, 22.07.2024, S. 160.

europäische Parlament eingebracht;[874] im ursprünglichen Kommissionsentwurf erfasste die Definition des „Sicherheitsrisikos" noch „alle Umstände oder Ereignisse, die potenziell negative Auswirkungen auf die Sicherheit haben".[875]

In der aktuellen NIS2-RL ist diese Einschränkung jedoch entfallen.[876] Das Risiko wird in Art. 6 Nr. 9 nun definiert als „das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird."[877] Diese Definition wird auch in der Begründung zu § 30 RegE BSIG ausdrücklich wiedergegeben.[878]

b. Bezugspunkt des Risikos

In der NIS-RL beschränkte sich außerdem der Bezugspunkt noch auf die „Auswirkungen auf die Sicherheit der Netz- und Informationssysteme". Damit fiel der Risikoeintritt bereits mit dem Sicherheitsvorfall, also einer Schutzzielverletzung zusammen und zwar ohne, dass es auf eine Beeinträchtigung der Schutzgüter ankam. Dies lässt sich anhand nachfolgender Grafik noch einmal darstellen:

874 Ohne Begründung in: EU-Parlament, P7_TA(2014)0244, Legislative Entschließung über Vorschlag zur NIS-RL, 13.03.2014, S. 41, Abänderungsantrag Nr. 47; EU-Parlament, A7-0103/20214 - Bericht über Vorschlag zur NIS-RL, 12.02.2014, S. 36.

875 Art. 3 Nr. 3 in EU-Kommission, KOM(2013) 48, Vorschlag zur NIS-RL, 5.7.2016.

876 In dieser Untersuchung wurde der Begriff allerdings weiterhin genutzt, um eine verhältnismäßige Begrenzung der Risikoidentifikation und -analyse und damit auch des Wissensbegriffs zu beschreiben, siehe dazu S. 166, 170 f.

877 Auch im IT Grundschutzkompendium heißt es insoweit ähnlich, „Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens", BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S 5.

878 BReg, Entwurf NIS2UmsuCG, 22.07.2024, S. 160.

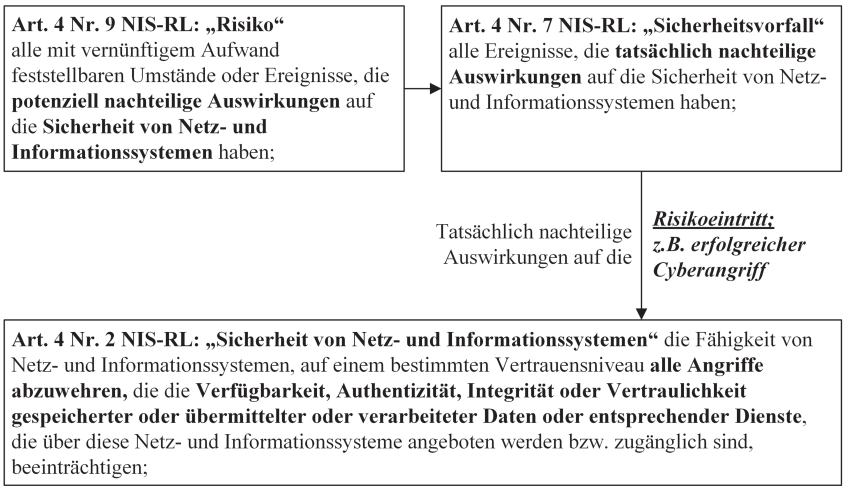

Abbildung 12: Bezugspunkt des Risikos nach NIS-RL

Unter der NIS2-RL wurde dies grundlegend verändert. Mit dem *„Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden“* wird der Bezugspunkt des Risikos verschoben. Dieser bleibt mithin nicht mehr bei dem Sicherheitsvorfall stehen, der nun in Art. 6 Nr. 6 NIS2-RL (vgl. § 2 Nr. 40 RegE BSIG) definiert ist als „ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt“. Vielmehr geht der Begriff über eine solche Schutzzielverletzung hinaus und bezieht sich auf die gerade durch diesen Sicherheitsvorfall verursachten „Verluste oder Störungen“. Aus Art. 23 Abs. 3 NIS2-RL und § 2 Nr. 11 RegE BSIG, welche die Erheblichkeit von Sicherheitsvorfällen definieren, lassen sich die Schutzgüter ableiten, die durch einen Sicherheitsvorfall beeinträchtigt werden. Hervorzuheben sind insoweit insbesondere die *materiellen oder immateriellen Schäden für natürliche oder juristische Personen.*

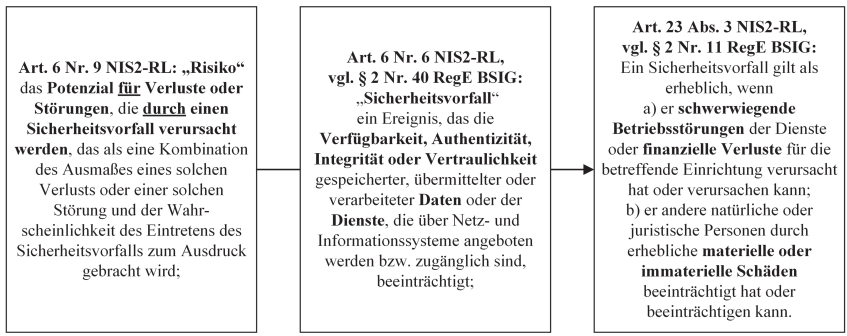

Abbildung 13: Bezugspunkt des Risikos nach NIS2-RL

Tatsächlich werden zwar auch hierdurch die Schutzgüter nur unzureichend abgebildet. Durch die genannten Schadkategorien werden v.a. die *Individualrechtsgüter* erfasst. Die Beeinträchtigung von *Gemeinschaftsrechtsgütern* lässt sich hingegen nur mittelbar aus den „schwerwiegenden Betriebsstörungen der Dienste“ ableiten. Jedenfalls ist aber anders als noch unter der NIS-RL das Risiko nun jedenfalls kategorisch eindeutig auf die *eigentlichen, rechtlich relevanten Schutzgüter* und nicht nur auf die IT-Sicherheit und deren Schutzziele bezogen.

Im RegE BSIG werden diese Änderungen wie dargestellt z.T. auch umgesetzt, indem der „Sicherheitsvorfall“ sowie der „erhebliche Sicherheitsvorfall“ entsprechend der NIS2-RL in § 2 Nr. 11, 40 RegE BSIG definiert wurden. Die fehlende Legaldefinition des Risikos könnte wie bereits beschrieben im Wege richtlinienkonformer und historischer Auslegung ergänzt werden, so dass das neue Risikoverständnis auch im RegE BSIG zum Tragen käme.

In den jeweiligen Pflichtennormen findet sich dies jedoch noch nicht ausdrücklich: Art. 21 NIS2-RL spricht weiterhin von „Risiken für die Sicherheit der Netz- und Informationssysteme“ und auch § 30 Abs. 1 RegE BSIG stellt entsprechend darauf ab, „*Störungen* der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, […] zu vermeiden“.[879] Insofern sind beide Regelungen bzw. Regelungsentwürfe unglücklich, da sie in den Pflichtennormen weiterhin

879 Wie bereits bei der Bestimmung der IT-Sicherheit erwähnt, müsste hier statt auf „Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse“ auf die Sicherheitsdefinition der NIS2-RL verwiesen werden.

auf die Risiken für die IT-Sicherheit mit ihren Schutzzielen abstellen. Es müssten aber entsprechend der DSGVO die *Risiken für Schutzgüter* sein, die durch eine fehlende IT-Sicherheit beeinträchtigt werden können.

Dies dürfte aber durch eine systematische Auslegung zu korrigieren sein, da die Legaldefinition des Risikos nun wie beschrieben explizit auf die Schutzgüter verweist. Zum anderen kommt als teleologisches Argument in Betracht, dass der Normzweck der NIS2-RL (und auch des RegE BSIG) eindeutig auf den Schutz der rechtlich relevanten Schutzgüter (und nicht der IT-Sicherheit als Selbstzweck) zielen muss. Im Ergebnis spricht somit viel dafür, auch die Pflichtennormen in dem Sinne auszulegen, dass die *Risiken für die Schutzgüter* zu beherrschen sind.

2. Methodik, einschließlich Angemessenheit

Nach der Überschrift des § 30 RegE BSIG regelt er „*Risikomanagement-maßnahmen*", was die Notwendigkeit eines „Risikomanagements" im Sinne einer Methodik zum systematischen Umgang mit Risiken verdeutlicht.

Allerdings fehlt es nach wie vor an konkreteren inhaltlichen Ausgestaltungen dieser Methodik. Nach § 30 Abs. 2 Nr. 1 RegE BSIG müssen zumindest Konzepte zur „Risikoanalyse" und zur „Sicherheit für Informationssysteme" erstellt werden. In der Literatur zu den bisherigen Vorschriften (§§ 8a, 8c BSIG) wurde zumindest teilweise vertreten, dass ein Risikomanagement nach ISO/IEC 27005 umgesetzt werden müsste.[880]

Hiernach ist insbesondere eine Risikoidentifikation (7.2), eine Risikoanalyse (7.3), sowie eine Risikobewertung (7.4) vorzunehmen.[881]

Die *Risikoidentifikation* dient zunächst dazu, alle in Betracht kommenden Risiken zu erkennen und zu beschreiben.[882] In der *Risikoanalyse* werden die „Ursachen und Quellen des Risikos, die Wahrscheinlichkeit, dass ein bestimmtes Ereignis eintritt, die Wahrscheinlichkeit, dass dieses Ereig-

880 Explizit wird auf ISO/IEC 27001 verwiesen, es ist aber davon auszugehen, dass damit die gesamte ISO/IEC 2700x-Familie und insbesondere auch die inhaltlich maßgebliche ISO/IEC 27005 gemeint ist; daneben wird auch der BSI IT-Grundschutz als möglicher Standard eines Risikomanagements genannt: *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn. 20.

881 Die Zahlenangaben beziehen sich auf die Abschnitte innerhalb der ISO/IEC 27005:2022.

882 DIN, ISO/IEC 27005:2022 (EN), S. 16.

nis Folgen hat, und die Schwere dieser Folgen berücksichtigt."[883] Nach § 30 Abs. 1 S. 2 RegE BSIG sollen das „Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen" berücksichtigt werden. Bis auf die Umsetzungskosten (dazu sogleich) dürften all diese Faktoren ebenfalls zur Risikoanalyse gehören. Bei der Risikoanalyse nach ISO/IEC 27005 wird außerdem, zwar begrifflich uneindeutig[884] auf Ungewissheit („uncertainty"), im hiesigen Sinne: bekanntes Nicht-Wissen, hingewiesen, die u.a. methodischen Ursprungs, d.h. insbesondere weil Vorgänge vereinfacht modelliert werden, als auch systemischen Ursprungs sein kann, was z.B. bedeutet dass Ereignisse ungewiss sind, weil eine belastbare Beschreibung nicht möglich ist („evidence is limited").[885]

Darauf folgt die Risikobewertung: Hier werden grundsätzlich die Risiken mit vorher festgelegten Risikoakzeptanzkriterien verglichen.[886] Letztere werden inhaltlich insbesondere an der individuellen Risikobereitschaft der Organisation ausgerichtet; die Einhaltung von Gesetzen ist daneben nur ein (weiterer) möglicher Faktor.[887] Dies kann aber im Rahmen des gesetzlichen Auftrags nach § 30 Abs. 1 RegE BSIG nicht zulässig sein.[888] Das maßgebliche Kriterium muss vielmehr im gesetzlich vorgegebenen Ziel eines „*dem Risiko angemessenen* Sicherheitsniveaus" liegen.[889] Dabei sind auch die Umsetzungskosten der Maßnahmen (§ 30 Abs. 1 S. 2 RegE BSIG) zu berücksichtigen.[890]

883 DIN, ISO/IEC 27005:2022 (EN), S. 16.

884 Die DIN, ISO/IEC 27005:2022 (EN) differenziert nicht zwischen „Ungewissheit" und „Unsicherheit"; so wird auf S. 21 als „uncertainty" sowohl die statistische Unsicherheit über den Risikoeintritt als auch das sogleich dargestellte Unwissen aufgrund fehlender Beweise bezeichnet.

885 DIN, ISO/IEC 27005:2022 (EN), S. 21.

886 DIN, ISO/IEC 27005:2022 (EN), S. 22 f.

887 DIN, ISO/IEC 27005:2022 (EN), S. 11 f., Kap. 6.4.2. lit a, e, g.

888 Vgl. *Sterz/Werner/Raabe*, RDV 2022, 291 (294).

889 Vgl. *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn. 20.

890 Daneben soll der „Stand der Technik" eingehalten sowie die einschlägigen „europäischen und internationalen Normen" berücksichtigt werden.

Es ist insoweit das Risiko zunächst der Höhe nach zu bestimmen und dann eine *Kosten-Nutzen-Abwägung*[891] vorzunehmen. Nach EG 81 NIS2-RL sollen die zu ergreifenden Maßnahmen im angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist, um eine „unverhältnismäßige finanzielle und administrative Belastung" (Kosten) zu vermeiden. Der Nutzen hingegen lässt sich nicht durch die Risiken in ihrer absoluten Höhe, sondern nur durch die mit den Maßnahmen zu erreichende *Risikoreduktion* ausdrücken.[892] Unverhältnismäßig sind folglich insbesondere Maßnahmen, die trotz hoher Kosten das Risiko nicht (mehr) signifikant mindern.[893]

Schließlich findet eine *Iteration* statt, die hier als „Monitoring and review" bezeichnet wird.[894] Zum Risikomanagement gehört demnach insbesondere die Entwicklung der Risiken (z.B. durch neu erkannte Schwachstellen und Ereignisse oder neu eingesetzte IT-Komponenten) fortlaufend zu beobachten und sofern sich diese verändern ggf. weitere oder andere Risikomaßnahmen zu treffen.[895] Die Iteration soll sowohl turnusmäßig als auch bei wesentlichen Veränderungen vorgenommen werden.[896]

3. Fazit

Der zentrale Begriff des Risikos wurde durch die NIS2-RL umfassend modifiziert. Hervorzuheben sind insoweit insbesondere der Wegfall der Beschränkung auf den „vernünftigen Aufwand" als auch die Verschiebung des Bezugspunkts des Risikos von den Schutzzielen der IT-Sicherheit hin zu den Schutzgütern. Leider ist dieser neue Bezugspunkt weder in die europäische noch in den Entwurf der nationalen Pflichtennorm (Art. 21

891 So bereits zur bisherigen Rechtslage: *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (165), Rn. 17; *Raabe/Schallbruch/Steinbrück*, CR 2018, 706 (710).

892 So bereits zur bisherigen Rechtslage: *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (169), Rn. 30.

893 *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn. 20; *Gehrmann/Klett*, K&R 2017, 372 (376); Maßnahmen können demnach auch unverhältnismäßig sein, wenn die Kosten der Maßnahmen „unverhältnismäßig höher" sind als die potentiellen Schäden, die durch sie verhindert werden sollen; vgl. auch *Wischmeyer*, Informationssicherheit, S. 254, wonach „Aufwand und Ertrag einer Umsetzungsmaßnahme nicht außer Verhältnis" stehen dürfen.

894 DIN, ISO/IEC 27005:2022 (EN), S. 36 ff.

895 DIN, ISO/IEC 27005:2022 (EN), S. 37.

896 DIN, ISO/IEC 27005:2022 (EN), S. 38.

Abs. 1 NIS2-RL, § 30 Abs. 1 RegE BSIG) im Wortlaut eingearbeitet, sondern er muss jeweils durch Auslegung hineingelesen werden.

Bei der Methodik bzw. der Angemessenheit fiel zunächst auf, dass die ISO/IEC 27005 bei der Risikobewertung auf individuell festzulegende Risikokriterien abstellt, was allerdings der gesetzlichen Vorgabe der „Angemessenheit" widerspricht. Insofern muss hier dem gesetzlichen Verständnis der Angemessenheit als Abwägung zwischen den Kosten der Maßnahmen und der damit zu erreichenden Risikoreduktion Vorrang zukommen. Außerdem wurde festgestellt, dass die Risikomethodik zumindest auf mögliche Ungewissheit (bekanntes Nicht-Wissen) bei Risikoidentifikation und -analyse hinweist.

IV. Zusammenfassung

Im Ergebnis konnten die für die Resilienz relevanten IT-Sicherheitsvorgaben wie folgt beschrieben werden:

Hinsichtlich der *Definition von IT-Sicherheit* erwies sich die nationale Umsetzung in §§ 2 Nr. 36, 30 Abs. 1 RegE BSIG i.E. als nicht mehr europarechtskonform auslegungsfähig und sollte in der Folge somit nicht angewandt werden. Deshalb ist die Definition der „Sicherheit der Netz- und Informationssysteme" nach Art. 6 Nr. 2 NIS2-RL anzuwenden, die im Kern auf die „Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit [Schutzziele] gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über […] Netz- und Informationssysteme angeboten werden" abstellt.

Die Informationstechnik wird nach dem RegE BSIG zunächst in *informationstechnische Systeme, Komponenten und Prozesse* unterteilt. Außerhalb der o.g. Definition der IT-Sicherheit können diese Begriffe auch europarechtskonform den Begriff der „Netz- und Informationssysteme" im Sinne des Art. 6 Nr. 1 NIS2-RL konkretisieren. Die Daten sind in jedem Fall als Teil des Systems zu verstehen.[897]

Die Bestimmung des Dienstbegriffs erwies sich als äußerst komplex und vielschichtig. Auch hier zeigten sich Schwächen im nationalen Umsetzungsentwurf, die nicht mit der NIS2-RL in Übereinstimmung gebracht werden

897 Der entgegenstehende § 2 Nr. 16 BSIG wonach Informationstechnik (zu der auch Systeme, Komponenten und Prozesse) zu verstehen nur die Mittel zur Informationsverarbeitung sind, ist richtlinienkonform auszulegen, siehe: S. 277.

können. Im Ergebnis ist jedenfalls zwischen dem Dienst als kritischer (physischer oder digitaler) Dienstleistung und den (untergeordneten) IT-Diensten der Sicherheitsdefinition zu unterscheiden. Die die IT-Sicherheit maßgeblich beschreibenden Schutzziele beziehen sich insofern auf IT-Dienste und die digitale Dienstleistung.

Das *Risiko* bezieht sich seit der NIS2-RL direkt auf die Schutzgüter. Gleichzeitig ist dies aber sowohl in der nationalen als auch der europäischen Pflichtennorm nicht entsprechend abgebildet. Die *Angemessenheit* beschreibt eine Kosten-Nutzen-Abwägung, was in der ISO/IEC 27005 mit ihren individuellen Risikokriterien jedoch unzureichend abgebildet wird. Bei der Risikoidentifikation und -analyse weist die ISO/IEC 27005 auf mögliche verbleibende Ungewissheiten (bekanntes Nicht-Wissen) hin.

Der Rechtsrahmen an IT-Sicherheitsvorgaben, auf den die Resilienz nach der NIS2-RL und deren Umsetzung in nationales Recht treffen würde, zeigte sich nach aktuellem Entwurfsstand in hohem Maße von Inkonsistenz und Widersprüchen geprägt. Die Schwächen einer solchen nationalen Umsetzung der NIS2-RL sind äußerst kritisch zu betrachten, insbesondere die inkompatiblen Definitionen von IT-Sicherheit und die unklare Verwendung des Dienstbegriffs dürften viele Normadressaten vor große Herausforderungen stellen. Zumindest für diese Untersuchung der Resilienz konnten die relevanten Vorgaben aber für den nächsten Schritt hinreichend genau bestimmt werden.

C. Unterschiede zur DSGVO und Folgen für die Resilienz

Im nachfolgenden Abschnitt werden die inhaltlichen Vorgaben der DSGVO mit jenen des RegE BSIG bzw. der NIS2-RL gegenübergestellt um die relevanten Unterschiede herauszuarbeiten, die ggf. einer Implementierung der Resilienz im RegE BSIG entgegenstehen könnten.

Dabei wird zunächst grundlegend auf die Unterschiede zwischen Daten- und IT-Sicherheit eingegangen (I.). Anschließend werden die Bedeutung der Schutzziele sowie die Bedeutung des Dienstes (II.) und das jeweilige Systemverständnis (III.) beleuchtet. Schließlich werden die jeweiligen Definitionen des Risikos und die Methodiken betrachtet (IV.)

Dabei wird jeweils auch untersucht, inwieweit sich die gefunden Unterschiede auf eine Implementierung der Resilienz auswirken. Alle Ergebnisse werden unter V. zusammengefasst.

I. IT-Sicherheit vs. Datensicherheit

Auf die generelle Unterscheidung zwischen IT-Sicherheitsrecht und Datensicherheitsrecht wurde bereits in der Einleitung hingewiesen.[898] An dieser Stelle soll nun konkret auf die jeweiligen Sicherheitsdefinitionen von NIS2-RL und DSGVO eingegangen werden:

Die *IT-Sicherheit* ist in Art. 6 Nr. 2 NIS2-RL als „Sicherheit von Netz- und Informationssystemen" legaldefiniert als

> *die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können.*

Demgegenüber konnte die *Datensicherheit* (mangels Legaldefinition) in der DSGVO definiert werden als

> *die angemessene Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sowie der Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz der für die Verarbeitung genutzten Systeme und Dienste.*

In beiden Fällen muss durch die *Vornahme technischer und organisatorischer Maßnahmen* ein den jeweiligen Risiken *angemessenes Sicherheitsniveau*[899] (dazu sogleich) gewährleistet werden. Außerdem sind sowohl die IT- als auch die Datensicherheit auf die Abwehr aller widrigen Ereignisse gerichtet, d.h. vorsätzlicher, fahrlässiger und zufälliger Ereignisse mit internen als auch externen Quellen.

Dagegen unterscheiden sich die Sicherheitsdefinitionen insbesondere anhand der Schutzziele sowie der Schutzobjekte. Mit der Authentizität besteht in der IT-Sicherheit nach Art. 6 Nr. 2 NIS2-RL ein weiteres Schutzziel und das System ist nur in der DSGVO auch ein Schutzobjekt, während es der NIS2-RL hingegen nur der Maßnahmenträger ist. Den übrigen Schutzzielen und dem Dienst kommt dabei wie bereits angedeutet außerdem eine andere Bedeutung zu (dazu sogleich). Auf die einzelnen Unterschiede wird im weiteren Verlauf dieses Kapitels noch vertieft eingegangen.

898 Siehe S. 37 f.
899 In Art. 6 Nr. 2 NIS2-RL als das „bestimmte Vertrauensniveau".

II. Bedeutung der Schutzziele und des Dienstes

Ausgehend von den soeben dargestellten Definitionen der IT-Sicherheit und der Datensicherheit wird nun auf die konkreteren Aspekte der unterschiedlichen Bedeutung der Schutzziele (1.) und des Dienstes (2.) eingegangen.

1. Schutzziele

Mit der *Verfügbarkeit, Vertraulichkeit und Integrität* liegen in § 30 Abs. 1 RegE BSIG bzw. Art. 6 Nr. 2 NIS2-RL abgesehen von der *Authentizität* dieselben Schutzziele wie in der DSGVO vor, die sich auch in den Definitionen nicht wesentlich unterscheiden. Allerdings ist zu berücksichtigen, dass diesen im IT-Sicherheitsrecht eine andere Gewichtung zukommt.

Im *IT-Sicherheitsrecht* haben die *Verfügbarkeit und die Integrität* einen besonders hohen Stellenwert, da es hier im Kern stets auf die verlässliche Erbringung einer kritischen Dienstleistung ankommt,[900] für die *die Daten, Systeme und Dienste* benötigt werden. Die Vertraulichkeit der Daten hat hier hingegen eine geringere Bedeutung; sie ist hier aufgrund der Passivität entsprechender Angriffe[901] zumeist nicht unmittelbar für die Erbringung der kritischen Dienstleistung relevant. Allerdings kann etwa die Offenlegung anlagenbezogener Informationen die (IT-)Sicherheit und damit wiederrum die verlässliche Erbringung der kritischen Dienstleistung[902] oder den Betrieb des Unternehmens gefährden. Außerdem können (bekannt gewordene) Vertraulichkeitsdefizite das Vertrauen der Bürger:innen in die kritischen Anlagen und damit die Bereitschaft diese zu nutzen, beeinträchtigen (z.B. im Gesundheits-, Finanz- oder im Telekommunikationssektor), so dass diese ihre gesellschaftsnotwendige Dienstleistung ebenfalls nicht mehr effektiv erfüllen können.[903]

900 *Franck*, RDV 2022, 3 (4); so auch zu Patientendaten mit Blick auf deren sichere Behandlung: *Rajamaki/Nevmerzhitskaya/Virag*, in: Proceedings of 2018 IEEE Global Engineering Education Conference (EDUCON), Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF), 2042 (2042).

901 *Voydock/Kent*, ACM CSUR 1983, 135 (140, 142).

902 *Franck*, RDV 2022, 3 (5).

903 Wie zuvor.

Im *Datensicherheitsrecht* steht hingegen v.a. *die Vertraulichkeit der personenbezogenen Daten* im Vordergrund, da durch diese die Schutzgüter der Rechte und Freiheiten natürlicher Personen in besonderem Maße tangiert werden. Die Verfügbarkeit der Daten selbst ist zumeist nur dann relevant, wenn lediglich eine Teilverfügbarkeit (ggf. Integritätsverletzung) vorliegt und diese ein unvollständiges und somit unrichtiges Abbild der Persönlichkeit schafft. Daneben dürfte im Aufkommen personalisierter Dienste die Integrität von Diensten auch in der DSGVO eine steigende Bedeutung entwickeln (dazu sogleich beim Dienst noch ausführlicher).[904]

Da die Resilienz auch durch die jeweiligen Schutzziele geprägt wird, ist auch insoweit die unterschiedlich gewichtige Bedeutung der Schutzziele und Schutzobjekte in der DSGVO sowie dem RegE BSIG zu beachten. So wird die Resilienz in Art. 32 Abs. 1 lit b) DSGVO typischerweise mehr dazu dienen, ungewisse Ereignisse hinsichtlich der Vertraulichkeit von Daten zu adressieren, während im RegE BSIG der Schwerpunkt eher bei Ereignissen hinsichtlich der Verfügbarkeit und Integrität der Dienste und Daten liegen dürfte.

Ein Hindernis mit Blick auf die rechtliche Integrationsfähigkeit der Resilienz im RegE BSIG erwächst aus der abweichenden Bedeutung bzw. der Erweiterung von Schutzzielen (Authentizität) und der herausgehobenen Bedeutung der Dienste jedoch nicht. Die Resilienz kann auch hinsichtlich der (fehlenden) Authentizität von Entitäten in offenen Systemen eine sinnvolle Ergänzung darstellen, da insoweit oft auch eine hohe Ungewissheit besteht.

2. Dienst

Mit dieser Divergenz in der Bedeutung der Schutzziele korrespondiert auch eine unterschiedliche Bedeutung des Dienstes zwischen dem Datensicherheits- (a.) und dem IT-Sicherheitsrecht (b.).

904 Außerdem entfaltet die Verfügbarkeit der Daten und Dienste Relevanz, soweit es die Wahrnehmung von Betroffenenrechten ermöglicht, siehe dazu bereits: Fn. 256.

a. Im Datensicherheitsrecht

Der Schutzzweck der Datensicherheit wird im Kern durch Schutzzielverletzungen an den personenbezogenen Daten als Passivum betroffen,[905] die Erbringung eines Dienstes als solches ist in der Datensicherheit wie auch im übrigen Datenschutzrecht zunächst kein zentraler Schutzgegenstand.[906]

Eine wichtige Funktion des Dienstes in der DSGVO liegt wie beschrieben darin, dass er als Ergebnis aus personenbezogenen Daten *Wissen* generiert (insbesondere durch Profiling, Art. 4 Nr. 4 DSGVO). Eine Manipulation (Integritätsstörung) des Dienstes erzeugt somit ein falsches Wissen über Personen und ein falsches Persönlichkeitsbild. Am Ende werden auf dieser Basis auch unrichtige Entscheidungen getroffen, die die Persönlichkeitsrechte und andere Rechte und Freiheiten beeinträchtigen können.

Liegen indes keine personalisierten Dienste oder andere persönliches Wissen erzeugende Dienste vor, ist der Dienstbegriff in der DSGVO weniger bedeutsam[907] und der Schwerpunkt der Datensicherheit liegt nach wie vor (nur) in der Sicherung personenbezogener Daten. Insofern zeichnet die DSGVO noch ein eher tradiertes, aber in der Praxis sicher nach wie vor häufig anzutreffendes Bild, wonach personenbezogene Daten z.B. für einen Vertrag oder für eine Online-Bestellung zwar verwendet, aber im Regelfall nicht im o.g. Sinne zu persönlichem Wissen oder gar entsprechenden Entscheidungen weiterverarbeitet werden, so dass dem Dienst tatsächlich keine derart wesentliche Bedeutung zukommt.

b. Im IT-Sicherheitsrecht

Im IT-Sicherheitsrecht ist die Bedeutung des Dienstes hingegen anders zu beurteilen: Hier steht die Funktionalität der IT-Dienste selbst als notwendige Voraussetzung für ein reibungsloses Funktionieren des Betriebs bzw.

905 Vgl. *Kipker*, in: Kipker, Cybersecurity, 1 (3), Rn. 4; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 1b.

906 Vgl. auf das „Funktionieren eines Systems" anstelle des Dienstbegriffs abstellend: *Poscher/Lassahn*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 133 (137), Rn. 12.

907 Abgesehen von seiner Funktion zur Erfüllung der Betroffenenrechte, hierzu bereits unter: S. 120, Fn. 256.

der kritischen Dienstleistung[908] zum Schutz des Gemeinwesens im Vordergrund. Passive Daten müssen hier erst zu einem Dienstergebnis verarbeitet werden und der Dienst kennzeichnet dann die entscheidende Verlinkung zum Schutzgut, da Schutzgüter stets dann gefährdet sind, wenn die hierfür notwendigen IT-Dienste nicht mehr ordnungsgemäß erbracht werden.

Zu diesen Diensten gehören im IT-Sicherheitsrecht zum einen bei den hier gegenständlichen digitalen Diensten auch die jeweiligen, kritischen, digitalen Dienstleistungen (z.B. eine Online-Suchmaschine) und deren (untergeordnete) Dienste. Zum anderen sind es auch die (informationstechnischen) Dienste, die zur Steuerung in kritischen Anlagen notwendig sind, damit diese ihrerseits ihre kritische, physische Dienstleistung (z.B. Stromerzeugung) erbringen können.

c. Fazit und Folgen für die Resilienz

Insgesamt kommt dem Dienst im IT-Sicherheitsrecht tendenziell eine im Vergleich zum Datensicherheitsrecht stärkere Bedeutung zu, da letzteres wie beschrieben (jenseits der Fälle wie den personalisierten Diensten) mehr auf den Schutz der personenbezogenen Daten fokussiert.

Somit dürfte auch die Resilienz sich im IT-Sicherheitsrecht stärker auf den Dienst beziehen. Dies gilt sowohl für die digitale Dienstleistung[909] als auch die untergeordneten IT-Dienste. So können etwa auch die Ergebnisse der *digitalen Dienstleistung* (z.B. Suchergebnisse) überwacht und ggf. Anpassungs- bzw. Erholungsmaßnahmen ergriffen werden. Hingegen kann sich die Resilienz als IT-Sicherheitsrechtliche Anforderung nicht auf die „physische Dienstleistung" beziehen, da hier die Ereignisse und somit auch die Anpassungsmaßnahmen auch außerhalb der IT liegen können.[910]

Mit Blick auf den Ausfall oder die Beeinträchtigung einzelner *IT-Dienste* (sowie der hierfür notwendigen Systeme und Komponenten), die für die Erbringung der digitalen (oder auch einer physischen) Dienstleistung genutzt werden findet die Resilienz hingegen uneingeschränkt Anwendung.

908 Bei kritischen Anlagen also beispielsweise die IT- Dienste wie die Überwachungs- und Steuerungsdienste in einem Kraftwerk, die für die Erbringung der kritischen Dienstleistung (Stromversorgung) erforderlich sind.

909 Bei physikalischen Dienstleistungen kann sich die Resilienz als IT-Anforderung auch hier nur auf die untergeordneten IT-Dienste beziehen.

910 Insoweit wäre dann die „Resilienz" im Rahmen der physischen Sicherheit nach § 2 Nr. 5 RefE KritisDachG gefragt.

Ergänzend sei an dieser Stelle darauf hingewiesen, dass aber nach der Sicherheitsdefinition der Art. 6 Nr. 2 NIS2-RL auch die „*Daten*" geschützt werden müssen, so dass die Resilienz (wie in der DSGVO) auch insoweit bedeutend ist.

III. Verständnis des Systembegriffs

Im nächsten Schritt werden die Unterschiede im Verständnis des Systems in der NIS2-RL bzw. dem RegE BSIG sowie der DSGVO im Kontext der Sicherheitsgewährleistung herausgearbeitet.

Auf den ersten Blick ergeben sich bei der sachlichen Erfassung keine erheblichen Unterschiede. In beiden Fällen werden jedenfalls alle Arten von Computersystemen mit ihrer Hard- und Software erfasst. Auch verwenden beide Systembegriffe zunächst kein soziotechnisches Verständnis. Unterschiede bestehen v.a. in der Regelungsfunktion (1.) sowie der Frage, ob auch die Daten als Systembestandteil verstanden werden (2.). Unter 3. werden diese Unterschiede schließlich mit Blick auf die Resilienz bewertet.

1. Maßnahmenträger oder Schutzobjekt

Hinsichtlich der Regelungsfunktion fällt zunächst auf, dass nach der NIS2-RL das System die Schutzziele der Daten und Dienste sicherstellen soll. Art. 6 Nr. 2 NIS2-RL spricht in der soeben schon genannten Definition der „Sicherheit von Netz- und Informationssystemen" von der „*Fähigkeit von Netz- und Informationssystemen* […] alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit […] [der] Daten oder der Dienste, […] beeinträchtigen können."

Ein ähnlicher Rechtsgedanke als Sicherheit im Sinne *einer Befähigung von Systemen* kann auch für „Systeme, Komponenten und Prozesse" aus dem BSIG entnommen werden: Nach der Definition der „Sicherheit in der Informationstechnik" sollen die Sicherheitsvorkehrungen (Maßnahmen) sowohl in als auch bei der Anwendung von informationstechnischen Systemen, Komponenten und Prozessen zum Einsatz kommen (§ 2 Nr. 39 RegE BSIG). Jedenfalls soweit die *Sicherheitsvorkehrungen „in" den Systemen, Komponenten und Prozessen* selbst implementiert werden, folgt der RegE

BSIG somit demselben Rechtsgedanken der Befähigung des (informationstechnischen) Systems.[911]

Damit unterscheiden sich NIS2-RL und RegE BSIG wesentlich von der DSGVO, bei der die Schutzziele (neben den personenbezogenen Daten) direkt auf die Systeme (und Dienste) bezogen sind. Das System ist in der DSGVO auch selbst ein Schutzobjekt, während es in der NIS2-RL und im RegE BSIG nur der Maßnahmenträger ist, mit dessen Hilfe die Schutzziele an den Schutzobjekten Daten und Diensten bzw. Informationen sichergestellt werden sollen.

Insofern drängt sich die Frage auf, ob gegenüber der DSGVO in der NIS2-RL und im RegE BSIG durch den Umstand, dass die Schutzziele nicht auf das System bezogen werden, eine Schutzlücke entstehen könnte:

Hinsichtlich der Vertraulichkeit des Systems wurde bei der DSGVO in Abgrenzung zu den personenbezogenen Daten auf die *systembezogenen Daten* abgestellt: Diese sind aber durch die explizite Vorgabe der Vertraulichkeit (aller) Daten in der IT-Sicherheitsdefinition bereits erfasst. Hinsichtlich der Integrität des Systems erscheint eine Lücke hingegen naheliegend: Insbesondere die Risiken durch manipulierte IT-Komponenten[912], die Schadsoftware wie Ransomware oder Abhörfunktionen enthalten, könnten mit diesem Schutzziel adressiert werden. Schließlich kommt auch die fehlende Verfügbarkeit des Systems als Lücke in Betracht, welche allerdings über die Verfügbarkeit des von dem System erbrachten Dienstes weitgehend abgedeckt sein dürfte.

2. Systembestandteile

Die DSGVO enthält keine Legaldefinition des Systems und schafft somit auch keine weiteren Unterkategorien; aus der Literatur ließ sich zumindest entnehmen, dass die Systeme aus „Hard- und Softwarekomponenten" bestehen.[913] Im RegE BSIG (§§ 2 Nr. 39, § 30 Abs. 1) wird hingegen konkreter

911 „Bei der Anwendung" adressiert hingegen den organisatorischen Aspekt (und damit nach hiesiger Terminologie das soziotechnische System) sowie bauliche Maßnahmen: BT-Drs. 11/7029, S. 8.

912 *Zhao/X.* an *Wang*, in: Barolli, Advances on Broad-Band Wireless Computing, Communication and Applications, 777 (778 ff.).

913 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 22; siehe im Übrigen S. 114 Fn. 236.

zwischen informationstechnischen *Systemen, Komponenten und Prozessen* differenziert.[914]

Weiterhin sind, wie im Rahmen der DSGVO dargestellt, die personenbezogenen Daten nach Art. 32 Abs. 1 lit b) DSGVO nicht als Bestandteil des Systems zu verstehen. Allerdings wurden bei der Anforderung der Vertraulichkeit von Systemen zumindest *systembezogene Daten* als Systembestandteil definiert. In der NIS(2)-RL werden die Daten wie gezeigt *ausdrücklich als Systembestandteil* definiert. Auch in der nationalen Umsetzung konnte dieses Ergebnis trotz uneindeutigem Wortlauts erreicht werden.[915] Ein möglicher Grund für dieses Vorgehen könnte darin liegen, dass die *Daten*, trotz dass sie auch ausdrücklich von der Sicherheitsdefinition als Schutzobjekt erfasst sind, im IT-Sicherheitsrecht keine derart herausgehobene Bedeutung für die Schutzgüter haben wie in der DSGVO.[916]

3. Fazit und Folgen für die Resilienz

Hinsichtlich des Verständnisses des Systembegriffs ist im Ergebnis festzuhalten, dass nach der DSGVO das System auch als Schutzobjekt definiert ist, während es sowohl im RegE BSIG (als auch in der NIS2-RL) nur den Maßnahmenträger darstellt ohne selbst Schutzobjekt zu sein und dass insofern mit Blick auf die (fehlende) Integrität des Systems auch eine mögliche Schutzlücke besteht.

Zunächst ist für die Resilienz der Aspekt, dass das *System kein Schutzobjekt* ist unkritisch: Die Resilienz stellt eine funktionale Anforderung an Systeme dar, ohne dass diese zwangsweise auch zum Schutz des Systems selbst wirken muss; insofern wird nur der rechtlich geforderte Schutzumfang der Resilienz (gegenüber der DSGVO) reduziert. Rechtssystematisch bringt diese Regelung indes sogar mehr Kohärenz, da die Resilienz somit nicht (wie in der DSGVO) auf einer Ebene neben den andersartigen Schutzzielen zum Schutz des Systems ansetzt.

914 In Art. 6 Nr. 1 lit b) NIS2-RL wie gezeigt zumindest auch als „Geräte oder Gruppe[n] miteinander verbundener oder zusammenhängender Geräte".

915 S. 277 f.

916 Das im RegE BSIG gleichwohl nur die Informationen und Daten (und nicht auch der Dienst) so eine prominente Stellung einnehmen, mag man mit der Gesetzesbegründung erklären, die zumindest bei der Begriffsdefinition der Informationstechnik eine sachlich vielleicht eher unzutreffend starke Inspiration des Gesetzgebers aus dem Datenschutzrecht erkennen lässt.: BT-Drs. 11/7029, S. 7.

Förderlich für eine mögliche Übertragung der Resilienz ist außerdem, dass der Systembegriff in § 2 Nr. 39, § 30 Abs. 1 RegE BSIG mit *Systemen, Komponenten und Prozessen* weiter ausdifferenziert wird. Dies ermöglicht eine spezifischere Anknüpfung, da sowohl einzelne Komponenten resilient sein sollen als auch die Resilienz des Systems angesichts des (ungewissen) Ausfalls bzw. Beeinträchtigung einzelner Komponenten eingreifen kann.

Der Unterschied hinsichtlich der *Daten als Systembestandteil* wirkt sich wie folgt aus: Sowohl in der DSGVO enthält der Systembegriff systembezogene (nicht aber personenbezogene) Daten und nach dem RegE BSIG einheitlich alle Daten, die verarbeitet werden. Eindeutig ist insoweit, dass sich die Resilienz nicht in dem Sinne auf Daten beziehen kann, dass die Daten selbst resilient sein müssten. Dies ist aufgrund des Charakters der Daten als Passivum ausgeschlossen. Der Resilienzbegriff muss sich insofern stets auf das IT-System als Verarbeitungsmittel ohne die darin enthaltenen Daten beziehen; in beiden Fällen muss die Resilienz des Systems aber auch die Daten schützen.

Schließlich setzt die Resilienz ein *soziotechnisches Systemverständnis* voraus, dass nach der expliziten Definition nach Art. 6 Nr. 1 NIS2-RL und auch den Begriffen der „informationstechnischen Systeme, Komponenten und Prozesse" nach § 2 Nr. 39 RegE BSIG im IT-Sicherheitsrecht nicht vorliegt. Eine differenzierende Auslegung wie in der DSGVO, die zumindest auch ein soziotechnisches Systemverständnis ermöglicht, dürfte hier aufgrund dieser expliziten Festlegungen nicht möglich sein. Insgesamt muss somit bei einer Implementierung der Resilienz als Fähigkeit eines soziotechnischen Systems ein eigenständiger System- oder sonstiger Oberbegriff für die informationstechnischen Systeme und das sie bedienende Personal verwendet werden.

Auch ohne einen solchen soziotechnischen Systembegriff kann die Resilienz aber jedenfalls auf Maßnahmenseite implementiert werden. Insofern ist wie dargestellt wurde eindeutig, dass (nach beiden Gesetzen) auch organisatorische Maßnahmen zu treffen sind, welche gerade nicht an den technischen Systemen selbst, sondern an der Organisation und damit dem Personal ansetzen.[917]

917 Siehe hierzu und auch zum Erfordernis der „Sicherheit des Personals", § 30 Abs. 2 S. 2 Nr. 9 BSIG bereits S. 277 f.

IV. Risiko

In diesem Abschnitt soll schließlich noch das Risiko sowohl in seinen Definitionen (1.) als auch in der Risikomethodik einschließlich der Angemessenheit (2.) verglichen werden.

1. Definitionen des Risikos

Das Risiko war bereits in Art. 4 Nr. 9 NIS-RL definiert und wurde in Art. 6 Nr. 9 NIS2-RL maßgeblich verändert. Beide Definitionen werden zunächst mit der Risikodefinition nach der DSGVO verglichen (a.). Anschließend werden die Folgen der Unterschiede für die Resilienz herausgearbeitet (b.)

a. Vergleich

Während die DSGVO mit ihrer weiten Definition des Risikos und der Resilienz einen „naturalistischen Risikobegriff" verfolgt, zeichnete sich die NIS-RL ursprünglich dadurch aus, dass nur mit „vernünftigem Aufwand feststellbare Umstände oder Ereignisse" erfasst sein sollen. Die (mit vernünftigem Aufwand nicht auflösbare) Ungewissheit wurde demnach nicht vom Risikobegriff umfasst. Diese Einschränkung wurde mit der NIS2-RL jedoch entfernt. Außerdem wurde der Bezugspunkt des Risikos durch die NIS2-RL verschoben. Bei der bevorstehenden Umsetzung der NIS2-RL in nationales Recht wurde keine entsprechende Risikodefinition in den RegE BSIG aufgenommen, so dass wie bereits dargestellt in richtlinienkonformer und historischer[918] Auslegung auch hier von der Risikodefinition der NIS2-RL auszugehen ist. Im Ergebnis ist somit ein Vergleich zwischen der Risikodefinition der DSGVO und der NIS(2)-RL vorzunehmen.

---

918 So auch die Entwurfsbegründung zu § 30 RegE BSIG: BReg, Entwurf NIS2UmsuCG, 22.07.2024, S. 160.

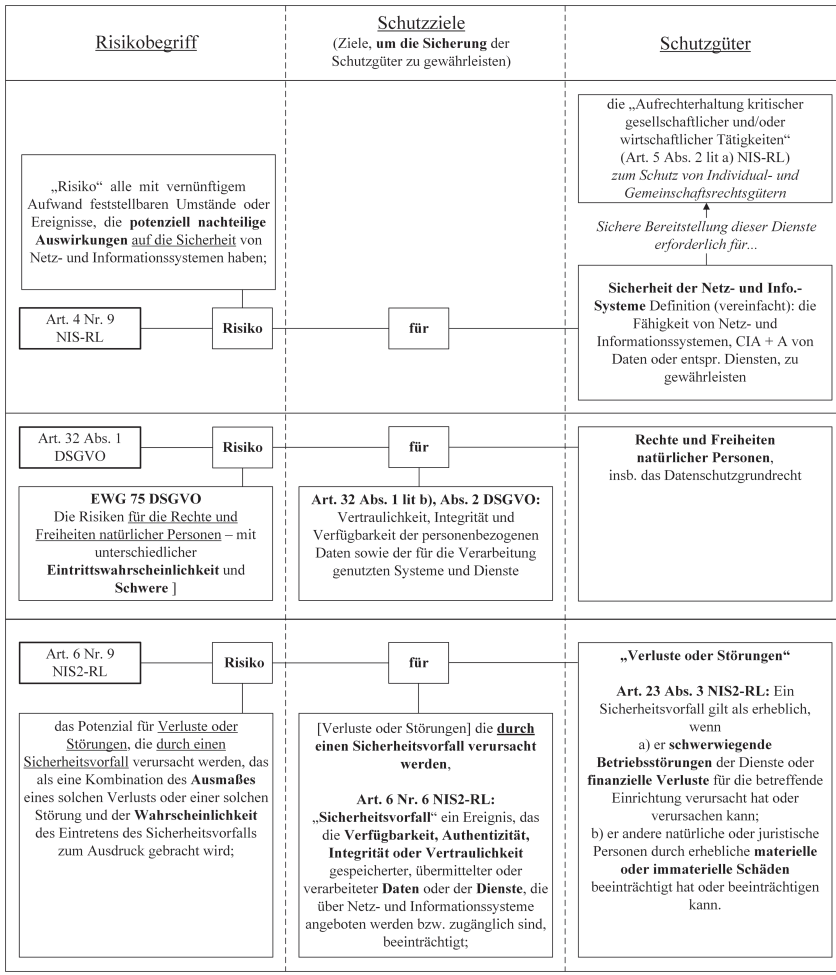

Abbildung 14: Risikobezugspunkte und -definitionen von NIS-RL, DSGVO und NIS2-RL

Die Tabelle gliedert sich in die drei Spalten Risikobegriff, Schutzziele und Schutzgüter. In der zweiten Zeile wird zunächst der historische *Risikobegriff aus der NIS-RL* dargestellt. Wie aus der Definition und der Grafik ersichtlich war der Bezugspunkt des Risikos hier die Sicherheit der Netz- und Informationssysteme. Die bereits im voranstehenden Kapitel herausgearbeiteten Schutzgüter, die beeinträchtigt werden wenn ein digitaler Dienst ausfällt, wurden von dem Risikobegriff der NIS-RL nicht erfasst. Die

Verbindung zwischen den Risiken für die Sicherheit der Netz- und Informationssysteme und den Schutzgütern musste hier vielmehr durch eine teleologische Auslegung hergestellt werden, indem man auf die Notwendigkeit sicher bereitgestellter IT-Dienste für die Funktionalität kritischer Infrastrukturen und die davon abhängigen Schutzgüter abstellt.

Demgegenüber zeigt die Darstellung in der dritten Zeile, dass der *Risikobegriff der DSGVO* sich direkt auf die rechtlich relevanten Schutzgüter in Form der Rechte und Freiheiten natürlicher Personen bezieht. Die Datensicherheit, hier insbesondere ausgedrückt durch die Fähigkeit, die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität an personenbezogenen Daten, Systemen und Diensten sicherzustellen, ist gerade nicht das Schutzgut selbst, sondern beschreibt den Ansatz bzw. die Mittel um die Schutzgüter zu sichern.

Der *Risikobegriff aus der NIS2-RL* nimmt hingegen nun mit den „Verlusten oder Störungen" ebenfalls direkt die Schutzgüter in den Blick, wie sie sich aus der Auslegung des Art. 23 Abs. 3 NIS2-RL (§ 2 Nr. 11 RegE BSIG) ergibt. Die IT-Sicherheit wird hier v.a. durch den Sicherheitsvorfall (Art. 6 Nr. 6 NIS2-RL; § 2 Nr. 40 RegE BSIG[919]) beschrieben, mit dem wie bei der DSGVO verdeutlicht wird, dass die Schutzziele der IT-Sicherheit nur den Zwischenschritt darstellen, durch den die Risiken auf die Schutzgüter wirken. Außerdem ist nun auch in der NIS2-RL von einem naturalistischen Risikobegriff auszugehen.

Damit sind die Risikobegriffe von NIS2-RL und DSGVO nun *weitgehend kohärent*, beide beziehen sich insoweit auf die Schutzgüter. Anzumerken ist allerdings, dass die Pflichtennorm des Art. 21 Abs. 1 NIS2-RL durch die Novellierung offensichtlich nicht an die neue Risikodefinition angepasst wurde – sie spricht weiter von Maßnahmen zur Beherrschung der „Risiken für die Sicherheit der Netz- und Informationssysteme." Auch der umsetzende § 30 Abs. 1 S. 1 RegE BSIG hält nicht nur unverständlicherweise an der Bezeichnung der Vermeidung von „Störungen" anstelle der Beherrschung von „Risiken" fest, sondern bezieht auch diese Störungen nur auf die IT-Sicherheit im Sinne der Schutzziele und Schutzobjekte und nicht auf die eigentlichen Schutzgüter.

919 Anders als die NIS2-RL lautet die Definition im BSIG: „ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über *informationstechnische Systeme, Komponenten und Prozesse* angeboten werden oder zugänglich sind, beeinträchtigt;" Abweichung durch den Autor hervorgehoben; dazu sogleich.

Daneben verfolgte die NIS-RL keinen naturalistischen Ansatz wie in der DSGVO. Während bei letzterem alle Risiken unabhängig von ihrer epistemischen Komponente erfasst werden, handelte es sich nach der NIS-RL nur dann um ein Risiko, wenn dessen Umstände oder damit verbundenen Ereignisse „mit vernünftigem Aufwand" feststellbar waren. Damit wurde hier eine entscheidungstheoretische Differenzierung zwischen Risiko und Ungewissheit ermöglicht, wobei letztere sich gerade nicht vorab als Risiko feststellen lässt.[920] Dieses Element ist allerdings mit der NIS2-RL entfallen, so dass auch hier nun Kohärenz zwischen DSGVO und NIS2-RL besteht.

b. Folgen für die Resilienz

Die Ungewissheit und damit auch die Resilienz wären nach der NIS-RL nicht Teil des Risikos und der Risikomethodik gewesen, sondern die Resilienz hätte mit ihrer Ausrichtung gerade auf ungewisse, nicht mit vernünftigem Aufwand feststellbare Umstände und Ereignisse parallel neben diesen gestanden. Folglich hätte auch kein Konflikt zwischen Risiko und Resilienz existiert, vielmehr hätte die Resilienz kohärent zur Entscheidungstheorie die auch nach der Legaldefinition von dem Risiko (Entscheiden unter Unsicherheit) zu unterscheidende Ungewissheit adressiert, was insoweit positiv zu bewerten gewesen wäre. Auf der Kehrseite der alten Rechtslage steht, dass nach der Definition der NIS-RL nicht das Risiko, sondern im Ergebnis nur die Resilienz direkt auf die Schutzgüter bezogen gewesen wäre.

Hingegen hat sich die Lage unter der NIS2-RL grundlegend gewandelt: Durch den Wegfall der Beschränkung auf den *vernünftigen Aufwand* und die Neuausrichtung des Bezugspunkts auf die Schutzgüter ist der Risikobegriff der NIS2-RL nun zunächst inhaltlich deutlich näher an jenen der DSGVO herangerückt. Diese stärkere Einheitlichkeit erleichtert zunächst die Übertragung der Resilienz. Auf der anderen Seite folgt nun aber auch der Risikobegriff der NIS2-RL (entgegen der Entscheidungstheorie) einem naturalistischen Verständnis, welches auch die Ungewissheit und damit auch den Ansatzpunkt für die Resilienz zwangsläufig mitbeinhalten muss. Eine wie oben dargestellte klare Trennung zwischen Risiko und Ungewissheit bzw. Resilienz ist somit nicht mehr möglich. Die Verschiebung

920 Siehe hierzu S. 171, Fn. 474.

des Bezugspunkts der Risikodefinition in der NIS2-RL (entsprechend der DSGVO) auf die Schutzgüter ist hingegen uneingeschränkt positiv zu bewerten. Folglich haben Resilienz und Risiko nun auch in der NIS2-RL denselben Bezugspunkt.

2. Methodik, einschließlich Angemessenheit

Weder die DSGVO noch der RegE BSIG geben ein gesetzliches Risikomanagement vor.[921] In der jeweiligen privaten Normung, auf die z.T. in der Literatur bzw. von EDBP verwiesen wird finden sich trotz grundsätzlich übereinstimmenden Aufbaus (Risikoidentifikation, -analyse und -bewertung; Iteration) Unterschiede.

Die ISO/IEC 27005 ist im Vergleich zur ISO/IEC 29134 in höherem Maße auf privates Risikomanagement von Unternehmen zugeschnitten. Sie nimmt die Risikobewertung anhand von Risikokriterien vor, die nach der individuellen Risikobereitschaft festzusetzen sind. Dies ist jedoch für die Erfüllung des gesetzlichen Normauftrags ungeeignet. Insofern wird die *Angemessenheit* in der ISO/IEC 27005 unzutreffend konkretisiert, es muss wie bei ISO/IEC 29134 eine auf rechtliche Angemessenheit zielende *Kosten-Nutzen-Abwägung* bei der Maßnahmenwahl vorgenommen werden. Da in beiden Fällen somit nur ein (dann übereinstimmender) methodischer Ansatz der Risikoangemessenheit besteht, existiert umgekehrt sowohl im RegE BSIG als auch in der DSGVO kein Anknüpfungspunkt für die Resilienz im Sinne einer *abstrakten Angemessenheit*.

Schließlich ist noch hervorzuheben, dass die ISO/IEC 27005 anders als die ISO/IEC 29134 bei der Risikoanalyse (und Risikoidentifikation) die verbleibende Ungewissheit (bekanntes Nicht-Wissen) anspricht, was zwar noch keinen klaren methodischen Ansatzpunkt für die Resilienz, aber zumindest doch einen starken Hinweis schafft.

V. Zusammenfassung

Insgesamt erweist sich der Rechtsrahmen des IT-Sicherheitsrechts trotz einiger Hürden für die Übertragung und Einführung des Resilienzbegriffs,

921 Für ein solches mit einem Vorschlag bereits: *Werner/Brinker/Raabe*, CR 2022, 817 (817 ff.).

wie er bereits im Rahmen der Auslegung nach Art. 32 Abs. 1 lit b) DSGVO definiert wurde, als geeignet, da entweder keine Unterschiede bestehen oder diese aber der Implementierung der Resilienz nicht entgegenstehen.

Die größten Unterschiede zwischen DSGVO und NIS2-RL bzw. RegE BSIG bestehen hinsichtlich folgender Aspekte:

- Die *Definitionen von Daten- und IT-Sicherheit* unterscheiden sich zunächst v.a. in der Authentizität als weiterem Schutzziel des IT-Sicherheitsrechts (in der NIS2-RL) und den abweichenden Schutzobjekten (DSGVO: personenbezogene Daten, Systeme und Dienste; RegE BSIG/NIS2-RL: Daten und Dienste).
- Die Datensicherheit nach Art. 32 DSGVO ist (jenseits personalisierter Dienste) teleologisch stärker auf die Vertraulichkeit personenbezogener Daten und die IT-Sicherheit im RegE BSIG stärker auf die Verfügbarkeit und Integrität von Diensten (IT-Dienste und digitale Dienstleistungen) gerichtet. Diese Ausrichtung wirkt sich ebenso wie das zusätzliche Schutzziel der Authentizität prägend auf die Schutzrichtung der Resilienz aus.
- Das *System* ist im RegE BSIG nicht wie in der DSGVO auch ein Schutzobjekt, sondern nur der Maßnahmenträger. Dadurch wurde zumindest hinsichtlich der Integrität des Systems auch eine mögliche Schutzlücke identifiziert. Für die Resilienz führt das abweichende Systemverständnis aber im Vergleich zur DSGVO zu mehr Kohärenz, da die Resilienz dadurch nicht als funktionale Anforderung „neben" den kategorisch andersartigen Schutzzielen (Sollzustände) am System ansetzen müsste.
- Der RegE BSIG differenziert neben dem „System" auch noch zwischen „Komponenten" und „Prozessen". Diese Differenzierung ist für die Resilienz besonders wichtig, da sie als Anforderung insbesondere auch den ungewissen Ausfall oder die Beeinträchtigung einzelner Komponenten und Prozesse im System adressieren kann.
- Der Systembegriff im IT-Sicherheitsrecht ist eindeutig technischer Natur; aufgrund der Definitionen v.a. in Art. 6 Nr. 1 NIS2-RL ist es anders als in der DSGVO hier kaum mehr möglich durch Auslegung ein soziotechnisches Verständnis zu ermitteln. Für die Resilienz als Eigenschaft soziotechnischer Systeme ist somit zumindest auch ein anderer Anknüpfungspunkt, der auch die soziale Komponente (also das IT-Personal) mit einbezieht, erforderlich.

Keine oder zumindest deutlich weniger gewichtige Unterschiede konnten im Übrigen bei den folgenden Aspekten festgestellt werden:

- Bei dem Verständnis von Daten bzw. Informationen gibt es abgesehen vom Erfordernis des Personenbezugs bei der DSGVO im Ergebnis keine Unterschiede.
- Hinsichtlich der Risikodefinition wurden ursprünglich bestehende Unterschiede zwischen der DSGVO und der NIS-RL mit der NIS2-RL weitgehend beseitigt. Allerdings stellen die zugehörigen Pflichtennormen weiterhin auf die Risiken für die IT-Sicherheit und nicht (wie zutreffend in der DSGVO) auf die Risiken für die rechtlich relevanten Schutzgüter ab.
- Das Risikomanagement ist in beiden Fällen nicht klar gesetzlich vorgegeben. Die ISO/IEC 27005 ist in ihrer grundlegenden Struktur (Identifikation, Analyse, Bewertung, Behandlung, Iteration) ähnlich zu jener der ISO/IEC 29134. Insbesondere bestehen keine rechtlich durchgreifenden inhaltlichen Unterschiede bezüglich der im Rahmen der Risikobewertung herzustellenden Risikoangemessenheit. In beiden Fällen ist hier (anders als die ISO/IEC 27005 zunächst nahelegt) eine Kosten-Nutzen-Abwägung vorzunehmen und für die Resilienz fehlt es insoweit an dem methodischen Ansatz einer abstrakten Angemessenheit. Schließlich ist aber bemerkenswert, dass die ISO/IEC 27005 auf die Ungewissheit bei der Risikoanalyse (bekanntes Nicht-Wissen) hinweist.

D. Übertragung der Resilienz in den RegE BSIG

Im vorangegangenen Abschnitt konnte dargestellt werden, dass der Rechtsrahmen des IT-Sicherheitsrechts auch für die Resilienz geeignet ist.

Jenseits dieser rechtssystematischen Möglichkeit der Übertragung wird nun noch konkretisierend untersucht, ob und inwieweit bereits funktionale Elemente der Resilienz im IT-Sicherheitsrecht bestehen (I.) und welche teleologischen Gründe für die Einführung der Resilienz im IT-Sicherheitsrecht sprechen (II.).

I. Bestehende, funktionale Resilienz-Elemente

In verschiedenen Regelungen des IT-Sicherheitsrechts ist die Resilienz bzw. sind einzelne Bestandteile derselben bereits funktional angelegt.

Die NIS-RL enthielt bereits in EG 46 unter dem Oberbegriff „Risikomanagement" die Elemente „Aufdeckung und Bewältigung von Sicherheits-

vorfällen sowie [die] Minderung ihrer Folgen." Bei den Sicherheitsvorfällen kann es sich insbesondere um ungewisse Ereignisse handeln, die deshalb eintreten, weil sie sich nicht vorher antizipieren und durch risikobezogene Maßnahmen ausschließen lassen. Damit weist dieser Umgang mit Sicherheitsvorfällen im Sinne der Erkennung derselben bzw. der folgenmindernden Anpassung an solche bereits auf die Resilienz hin.

Auch nach der neuen Rechtslage sollen nach dem auch für digitale Dienste relevanten § 30 Abs 1, Abs. 2 Nr. 2 RegE BSIG[922] Sicherheitsvorfälle bewältigt und insbesondere deren Auswirkung auf die eigenen Dienste oder Dienste von Dritten so gering wie möglich gehalten werden. Nach Art. 6 Nr. 8 NIS2-RL gehören zur „Bewältigung von Sicherheitsvorfällen" alle Maßnahmen und Verfahren zur „Verhütung"[923] sowie im Sinne der Resilienz zur „Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon".[924]

Zusätzlich werden in § 30 Abs. 2 Nr. 3 RegE BSIG[925] als Maßnahmen außerdem auch die „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement," gefordert. Die Aufrechterhaltung des Betriebs kann v.a. durch Anpassung erreicht werden. Die „Wiederherstellung nach einem Notfall" betrifft (allerdings ohne den Aspekt der lernenden Verbesserung) erneut die Phase der Erholung.

Von Betreibern kritischer Anlagen wird nach § 31 Abs. 2 RegE BSIG zusätzlich zu den Anforderungen nach § 30 Abs. 1 RegE BSIG auch der Betrieb von Angriffserkennungssystemen verlangt. Mithilfe dieser sollen

922 Art. 21 Abs. 1, Abs. 2 lit b) NIS2-RL.

923 Der Aspekt der Verhütung passt allerdings nicht zur Resilienz und ist hier auch innersystematisch wenig überzeugend, da ein infolge einer erfolgreichen Verhütung gar nicht eingetretener Sicherheitsvorfall auch nicht „bewältigt" werden muss.

924 Die Definition der NIS2-RL wird nach dem RegE BSIG nicht explizit in nationales Recht umgesetzt, so dass eine richtlinienkonforme Auslegung erforderlich wäre. Dagegen ist in § 8c Abs. 2 S. 2 Nr. 2 BSIG in Umsetzung des Art. 14 Abs. 1 lit b) i.V.m. Art. 4 Nr. 8 NIS-RL noch unmittelbar festgelegt, dass Anbieter digitaler Dienste bei der Gewährleistung eines risikoangemessenen Sicherheitsniveaus den Aspekten „der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen" Rechnung tragen müssen. Dies wurde auch in Art. 2 Abs. 2 der DVO 2018/151 konkretisiert, wonach u.a. Prozesse zur Erkennung ungewöhnlicher Ereignisse eingerichtet werden müssen, Reaktionen nach festgelegten Verfahren vorgesehen und schließlich eine nachgelagerte Vorfallsanalyse durchgeführt werden soll, um einen „kontinuierlichen Verbesserungsprozess [zu] fördern".

925 Art. 21 Abs. 2 lit c) NIS2-RL.

durch tradierte als auch KI-gestützte Muster- und Anomalieerkennung sowie (andere) heuristische Methoden Angriffe frühzeitig detektiert werden.[926] Auch insoweit besteht somit ein Ansatz zur Erkennung von Ereignissen.

Weiterhin ist der untergesetzliche *Leitfaden zum Schutz kritischer Infrastrukturen*[927] zu nennen. Dort wird die Einführung eines Krisenmanagements gefordert, um für den Fall, dass es trotz vorbeugender (risikobezogener) Maßnahmen zu einer Krise kommt, „möglichst ohne Zeitverzögerung adäquat auf eine Situation reagieren zu können. Hierdurch können die Auswirkungen einer Krise reduziert und die Zeitspanne zur Wiederherstellung des Normalzustandes verkürzt werden."[928] Damit werden insbesondere die Elemente der Anpassung an ein schädigendes Ereignis um Folgen/Auswirkungen zu minimieren und der Wiederherstellung nach einem solchen Ereignis aufgenommen.

Ausdrückliche Nennungen der Resilienz im IT-Sicherheitsrecht wurden bereits in der Wortlautauslegung berücksichtigt[929] und sollen deshalb hier nur kurz wiedergegeben werden:

Mit der Entwicklung der „EU's Cybersecurity Strategy for the Digital Decade"[930] wurde der Begriff der Resilienz deutlich prominenter platziert, was z.T. auch in der NIS2-RL und in der RKE-RL bzw. dem RefE KritisDachG fortwirkt. In der genannten EU-Cybersicherheitsstrategie heißt es zunächst: „Cybersicherheit ist daher eine wesentliche Voraussetzung für den Aufbau eines resilienten, grünen und digitalen Europas"[931] und zeigt erneut den Schlagwortcharakter dieses Begriffs in der Politik und am Ende auch im IT-Sicherheitsrecht. Auch die NIS2-RL spricht in EG 2 davon, dass seit In-

926 *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn 23 f.; BT-Drs. 18/4096, S. 25; weitergehend im Sinne der Resilienz, dass mit Angriffserkennungssystemen Angriffe „erkannt und verhindert werden, sowie entstandene Schäden durch (automatische) Beseitigungsmaßnahmen mitigiert werden" sollen: *Kohpeiß/Schaller*, CR 2024, 22 (22).

927 BMI, Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Mai 2011.

928 BMI, Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Mai 2011, S. 6.

929 Siehe S. 145 ff.

930 EU-Kommission, JOIN(2020) 18 final, The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020.

931 en: Cybersecurity is therefore essential for building a resilient, green and digital Europe; weiterhin sollen demnach auch Lieferketten vernetzter Geräte und Infrastrukturen resilient sein: EU-Kommission, JOIN(2020) 18 final, The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020, S. 1, 5.

krafttreten der NIS-RL „erhebliche Fortschritte bei der Stärkung der *Cyberresilienz* der Union erzielt worden" seien. Weiterhin enthält § 2 Nr. 5 RefE Kritis-DachG eine Resilienzdefinition, die aber wie bereits beschrieben[932] zwar auch Resilienzelemente (Anpassung: Reaktion auf Vorfälle, Begrenzung der Folgen eines Vorfalls; Erholung von einem Vorfall) enthält, aber darüber hinaus v.a. tradierte, risikobasierte Sicherheitsaspekte umschreibt. Insgesamt bildet die Resilienz hier eher als übergreifender Ausdruck physischer Sicherheitsgewährleistung das Gegenstück zur IT-Sicherheit. Ganz ähnlich verhält es sich mit der „digitalen operationalen Resilienz" nach der DORA die wie ebenfalls bereits dargestellt[933] inhaltlich zu weit gefasst ist, aber ebenfalls auch wesentliche Resilienzelemente (Erkennung, Reaktion und Wiederherstellung sowie das Lernen aus Vorfällen) umfasst.

Insgesamt finden sich damit im RegE BSIG sowie der NIS2-RL selbst als auch in verwandten Rechtsakten sowie untergesetzlichen Konkretisierungen bereits einige Elemente, die hinreichend konkret zumindest Teilaspekte der Resilienz abdecken und somit eine Implementierung der Resilienz als Oberbegriff für diese Teilaspekte nahelegen.

II. Teleologische Gründe

Teleologisch ist davon auszugehen, dass sich das IT-Sicherheitsrecht mit Blick auf neue Ungewissheitssituationen ähnlichen Herausforderungen ausgesetzt sieht wie das Datensicherheitsrecht. Dies betrifft insbesondere den Wandel von geschlossenen zu offenen Systemen, bei denen Ereignisse nicht mehr antizipiert werden können, mithin ungewiss sind.[934] Auch die steigende Komplexität der informationstechnischen Systeme sowie die zunehmende Integration von KI-Anwendungen schaffen parallel neue Ungewissheitssituationen.

Diese werden aber bislang auch im IT-Sicherheitsrecht nicht hinreichend erfasst. Zwar existieren bereits funktionale Resilienzelemente (Angriffserkennung, Bewältigung von und Erholung nach Sicherheitsvorfällen) und auch in der ISO/IEC 27005 finden sich stärkere Ansätze für die Beachtung der Ungewissheit. Aber die Resilienz als übergeordnete funktionale Anforderung an soziotechnische Systeme zur Adressierung von Ungewiss-

932 Siehe S. 148, 152 f.
933 Siehe S. 149, 152 f.
934 So bereits zuvor, S. 209.

heit ist trotz dieser Ansätze nach wie vor rechtlich nicht vorgegeben und das Fehlen dieser Anforderung vermag insofern eine Lücke in der rechtlich geforderten und damit auch der faktischen Sicherheitsgewährleistung zu eröffnen.

III. Gesamtergebnis

Das IT-Sicherheitsrecht enthält bereits eine große Anzahl an Ansatzpunkten, die auf die Resilienz hinweisen. Auch teleologisch liegen zur DSGVO parallele Ungewissheitssituationen vor, für die die Resilienz eine Antwort geben kann.

Nach einer intensiven Beschreibung der gesetzlichen IT-Sicherheitsvorgaben (B.) konnte im voranstehenden Abschnitt C.[935] außerdem gezeigt werden, dass hier keine derart gravierenden Unterschiede zum Datensicherheitsrecht bestehen, die einer Implementierung der Resilienz im Wege stehen würden. Als Gesamtergebnis sprechen daher viele rechtliche Argumente für die Übertragung der Resilienz in das IT-Sicherheitsrecht, hier in Gestalt des § 30 Abs. 1 RegE BSIG.

Die Resilienz ist somit auch hier als die Fähigkeit eines soziotechnischen Systems zu verstehen, wofür es jedoch noch an einem entsprechenden rechtlichen Anknüpfungspunkt fehlt. Die ungewissen Ereignisse sind entsprechend der (von der Datensicherheit abweichenden) Definition der IT-Sicherheit (Art 6 Nr. 2 NIS2-RL) mit Blick auf Daten sowie insbesondere auf die Dienste zu bewältigen. Bei den Diensten ist insoweit wie beschrieben zwischen den IT-Diensten und ggf. der erbrachten digitalen Dienstleistung zu unterscheiden, auf die sich die Resilienz beziehen kann.

Bezüglich der Inhalte der Resilienz, unmittelbar bevorstehende oder bereits eingetretene ungewisse Ereignisse zu erkennen und sich an diese anzupassen sowie sich unter lernender Verbesserung davon zu erholen, kann die zu Art. 32 Abs. 1 lit b) DSGVO entwickelte Definition uneingeschränkt Anwendung finden. Die gleichwohl z.T. abweichende Umsetzung der Resilienz im IT-Sicherheitsrecht soll nun noch einmal anhand der personalisierten Dienste für das IT-Sicherheitsrecht demonstriert werden.

935 Siehe hier die Zusammenfassung, S. 311 f.

E. Demonstration anhand des Szenarios

Der für den RegE BSIG relevante Angriffsvektor liegt hier nicht in der singulären, sondern in der pluralen Informationsmanipulation des personalisierten Dienstes, d.h. durch viele übernommene oder künstlich erzeugte Accounts wird ein (ML-gestütztes)[936] Empfehlungssystem[937] angegriffen, um das *Lernwissen*, also das abstrakte Wissen über Präferenzen und deren Zusammenhänge, zu verändern. Damit können beispielsweise bestimmte einseitige oder unwahre Inhalte in sozialen Netzwerken stärker empfohlen[938] und so die öffentliche Meinungsbildung beeinträchtigt werden.[939]

I. Ungewissheit

Bezüglich der Ungewissheit liegt wie im für die DSGVO demonstrierten Angriffsvektor ein Fall des *bekannten Nicht-Wissens* in einem offenen System vor. Allerdings besteht die Ungewissheit hier nicht nur bezüglich der Manipulationsfreiheit der Daten in einem spezifisch einer Person zugeord-

936 Es ist zum Zeitpunkt dieser Untersuchung unklar, wie das Verhältnis der kommenden KI-VO zur NIS2-RL und dem BSIG ist. Jedenfalls für den Bereich der digitalen Dienste dürfte hier keine Kollision bestehen, da die hierfür eingesetzten KI-Systeme keine Hoch-Risiko-KI-Systeme i.S.d. Anhang III der KI-VO-E sein dürften. Insbesondere fallen sie nicht unter den Begriff „kritische Infrastruktur", da dies nur auf wesentliche Einrichtungen im Sinne der NIS2-RL verweist; digitale Dienste sind hingegen nun wichtige Einrichtungen, Art. 3 Abs. 2 i.V.m. Anhang II, Ziff. 6, NIS2-RL.

937 Zu Vergiftungsangriffen auf regelbasierte Empfehlungssysteme (ohne ML) siehe statt vieler: *Chen et al.*, Trans Emerging Tel Tech 2021, AS-Nr. e3872.

938 Vgl. unter anderem zu YouTube und LinkedIn: *G. Yang/Gong/Cai*, in: Proceedings 2017 Network and Distributed System Security Symposium, Fake Co-visitation Injection Attacks to Recommender Systems, S. 10 ff.

939 Darüber hinaus sind in digitalen Diensten auch andere Angriffe auf die öffentliche Meinungsbildung möglich, die jedoch nicht wie in diesem Szenario auf die Personalisierungsfunktion gerichtet sind: Hierzu gehören insbesondere die großflächige Verbreitung von Falschinformationen („Fake News") in sozialen Netzwerken, siehe *Milker*, ZUM 2017, 216 (216 f.); zum Wahlkampf in den USA 2016 außerdem: *Badawy/Ferrara/Lerman*, in: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign, 258 (258 f., 264). Da auch hier sowohl von realen Menschen als auch von Bots unerwünschte Informationen eingebracht werden, kann somit die Resilienz auch hier mit entsprechenden Gegenmaßnahmen (Anomalieerkennung, CAPTCHAs, Löschung) greifen.

neten Account, sondern insbesondere auch hinsichtlich der Authentizität von vielen Accounts, die (möglicherweise) manipulierte Daten senden. Weiterhin kann eine Ungewissheit darüber bestehen, wie ggf. eingesetzte ML-Systeme auf solche Angriffe reagieren.

II. Resilienzmaßnahmen

Um den genannten Angriffen zu begegnen, kommen somit zum Teil auch andere Maßnahmen in Betracht als für den nach der DSGVO relevanten Angriffsvektor der singulären Informationsmanipulation. Wie bereits im entsprechenden Abschnitt zur DSGVO sind die aufgezählten Maßnahmen nur exemplarischer Natur.

1. Ereigniserkennung

Der Eintritt bzw. das unmittelbare Bevorstehen des ungewissen Ereignisses muss zunächst erkannt werden. Hierfür kann insbesondere wieder eine Anomalieerkennung eingesetzt werden, z.B. eine statistische Anomalieerkennung an den Elementen (also etwa starke Ausschläge bei den positiven oder negativen Bewertungen an einem Produkt auf einem Online-Marktplatz).[940]

Auch können bestimmte Attribute in den Accounts oder Profilen der Nutzer:innen auf ein Angriffsverhalten hindeuten; diese Attribute können zuvor (ggf. in einer vorangegangen Erholungsphase) mit einem überwachten Klassifizierungsverfahren aus den Accounts bzw. den Profilen von nachweislich feindlich agierenden Nutzer:innen abgeleitet werden.[941]

Auch können menschliche Expert:innen hinzugezogen werden, um zu prüfen ob sich sowohl die Ergebnisse der Erkennungssysteme[942] als auch

940 *Gunes et al.*, AIR 2014, 767 (779 ff.); *G. Yang/Gong/Cai*, in: Proceedings 2017 Network and Distributed System Security Symposium, Fake Co-visitation Injection Attacks to Recommender Systems, S. 13.

941 Vgl. *Gunes et al.*, AIR 2014, 767 (779); *Burke et al.*, in: Proceedings of the 12th ACM SIGKDD, Classification features for attack detection in collaborative recommender systems, 542 (542 ff.).

942 *Biggio/Roli*, Pattern Recognition, Vol. 84 (2018), 317 (327).

die Ergebnisse der eigentlichen personalisierten Dienste (digitale Dienstleistung) noch im gewünschten Rahmen bewegen.[943]

2. Anpassungsfähigkeit

Um den erkannten oder ggf. zumindest vermuteten Angriff zu unterbinden, können (wie bereits bei der singulären Informationsmanipulation) CAPTCHAs eingesetzt werden, um zumindest nicht-menschliche Angreifer mit einer gewissen Sicherheit auszuschließen.[944] Dabei gilt: je stärker die Anomalien ausfallen, desto eher ist von einem Angriff auszugehen und desto eher sollten folglich solche Zugangserschwernisse eingesetzt werden.

Bezüglich der bereits eingegangenen, manipulierten Daten gilt: Werden Empfehlungssysteme ohne ML eingesetzt, sind die als manipuliert erkannten Daten zu deaktivieren und somit ihre Wirkung auszuschließen. Beim Einsatz von ML gilt entsprechend, dass diese zum weiteren Training zu nutzenden Daten vorher von den als „Vergiftungsangriffe" erkannten Anomalien bereinigt werden müssen.[945]

Um auch auf Fälle der Nicht-Erkennung reagieren zu können, können z.B. mehrere unterschiedliche ML-Systeme parallel verwendet werden: Sofern diese divers sind, d.h. in ihren Lernalgorithmen variieren oder mit unterschiedlichen Trainingsdaten trainiert wurden, werden sie bei einem Angriff zu unterschiedlichen Ergebnissen kommen bzw. der Angriff wirkt sich in den unterschiedlichen Modellen weniger stark auf die Ergebnisse aus.[946] Somit kann als Anpassung im Ereignisfall (welcher etwa durch unerwartete Abweichungen der Ergebnisse festgestellt werden kann) nach dem Mehrheitsprinzip für die häufigere Ergebnisvariation entschieden und

943 Damit könnten im Übrigen auch weitere (nicht manipulationsbedingte) Ereignisse festgestellt werden, z.B. Abweichungen in Folge eines mit ungenauen Daten trainierten ML-System

944 Siehe S. 218, Fn. 630.

945 Man spricht in diesem Zusammenhang auch vom Kuratieren der Trainingsdaten: Dies umfasst neben der hier angesprochenen Bereinigung von Anomalien auch andere wichtige Schritte wie die Prüfung der Datenqualität, der Integration von verschiedenen Datensätzen oder auch der Beschriftung von Daten, *Heinemeyer/Herpig*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 65 (73 f.).

946 Vgl. *Machida*, in: IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), On the Diversity of Machine Learning Models for System Reliability, 276 (276 f., 285), der diesen Ansatz zur Fehlerkorrektur einsetzt.

so eine Auswirkung des Angriffs auf die finalen Entscheidungen des personalisierten Dienstes verhindert werden.[947]

3. Erholung

Sofern die Daten bereits für das weitere Training verwendet wurden müssen die nun fehlerhaften ML-Systeme in einen manipulationsfreien Zustand zurückversetzt werden. Letzteres kann durch das Zurücksetzen des Modells in einen früheren Zustand und ggf. ein erneutes Training mit sauberen Trainingsdaten erreicht werden.

Langfristig muss das Wissen aus den Ereignissen genutzt werden, um künftige Angriffe besser zu erkennen und insbesondere die ML-Systeme in ihrer Angriffssicherheit gegenüber solchen Manipulationen weiter zu verbessern. Denkbar ist hier auch, dass die Gewichtung der genutzten Features (Inhaltsinformationen) basierend auf zurückliegenden Angriffen verändert werden,[948] so dass häufig oder leicht zu manipulierende Features künftig weniger stark berücksichtigt werden.

III. Abstrakte Angemessenheit

Die abstrakte Angemessenheit ist für die Resilienz als besonderer Bestandteil der Methodik wie auch in der DSGVO erforderlich, da bislang nur auf die Risikoangemessenheit abgestellt wird. Die abstrakte Angemessenheit richtet sich auch hier nach der abstrakten Bedrohung der Schutzgüter, d.h. welches Gewicht diese Schutzgüter aufweisen und welche Schäden an diesen drohen. Insoweit kann wie § 30 Abs. 1 S. 2 RegE BSIG bereits klarstellt

947 Außerdem existieren sog. „Resilience-by-Design"-Ansätze (dazu auch nochmal im Ausblick, S. 335 ff.), mit denen ML-Systeme so gestaltet werden können, dass sie allgemein weniger anfällig für manipulierte Daten sind und hieraus möglichst kein falsches Sachwissen erzeugen: *Jagielski et al.*, in: 2018 IEEE Symposium on Security and Privacy (SP), Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning, 19 (20 ff.). Da dies jedoch kein adaptives Verhalten nach Erkennung eines ungewissen Ereignisses, sondern eher eine klassische Härtungsmaßnahme darstellt, wird diese Maßnahme hier nicht unter die Resilienz gefasst.

948 Vgl. *Sreevallabh Chivukula et al.*, Adversarial Deep Learning in Cybersecurity, S. 50 f.; *Xue et al.*, IEEE Access, Vol. 8 (2020), 74720 (74733); *Kolcz/Teo,* Feature weighting for improved classifier robustness, 2009, S. 1 ff.

zum einen auf die Größe der Einrichtung und damit den Kreis der potenziell betroffenen Personen abgestellt werden. Weiterhin verlangt § 30 Abs. 1 S. 2 RegE BSIG die „gesellschaftlichen und wirtschaftlichen Auswirkungen" zu berücksichtigen. Bei digitalen Diensten könnte man exemplarisch wie folgt differenzieren:[949]

Während dies bei Online-Marktplätzen vor allem Wohlfahrtsverluste und damit Beeinträchtigungen des Gemeinwohlziels *Wirtschaftsförderung* durch Manipulationen umfasst (etwa durch Fake-Bewertungen), sind bei der Online-Suchmaschine und den sozialen Netzwerken insbesondere Beeinträchtigungen der *öffentlichen Meinungsbildung* in die Bewertung einzubeziehen. Gleichzeitig sind jeweils auch die entsprechenden Individualgrundrechte (Berufsfreiheit bzw. unternehmerische Freiheit sowie Informations- und Meinungsäußerungsfreiheit) der möglicherweise großen Anzahl betroffener Personen zu berücksichtigen.

Da es sich hierbei um äußerst bedeutende Schutzgüter handelt, die, nicht zuletzt aufgrund der Monopolstellung der Online-Suchmaschinen wie auch der sozialen Netzwerke, bei fehlender IT-Sicherheit durch eine Manipulation dieser Dienste massiv beeinträchtigt werden, dürften auch Resilienzmaßnahmen noch im großen Umfang angemessen sein.

949 Ausführlich zu den Schutzgütern bei digitalen Diensten bereits: S. 254 ff.